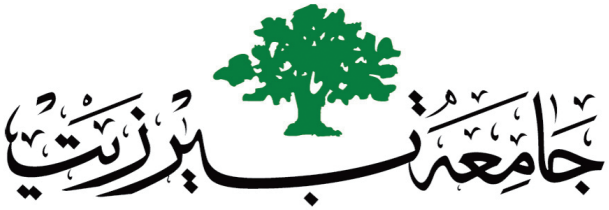


BIRZEIT UNIVERSITY

Faculty Of Graduate Studies
Mathematics Program

Chaos In Topological Spaces

Prepared by
Tasneem Hamza

Supervised by
Prof. Mohammad Saleh

M. Sc. Thesis
Birzeit University
Palestine

2014

Chaos In Topological Spaces

Prepared By

Tasneem Hamza

Master in Mathematics, Birzeit University, 2014

Supervised By

Prof.Mohammad Saleh

Mathematics Department, Birzeit University
Palestine
2014

This thesis was submitted in fulfillment of the requirements for the Master's Degree in Mathematics from the Faculty of Graduate Studies at Birzeit University, Palestine.

Chaos In Topological Spaces

Prepared By

Tasneem Hamza

This thesis was defended successfully on June 11, 2014. And approved by:

Committee Members		**Signature**
1. Prof. Mohammad Saleh	Head Of Committee	.....
2. Dr. Reema Sbeih	Internal Examiner	.....
3. Dr. Marwan Aloqeili	Internal Examiner	.....

Dedication

First of all, my enormous debt of gratitude goes to my thesis Supervisor and mentor, Professor Mohammad Saleh. I am especially thankfull to him for his mentorship and guidance throughout the period of my thesis. I would like also to thank my thesis defense committee members for their valuable comments and suggestions.

I would like to express my sincere gratitude to my family for their support and patience, I especially dedicate this Thesis to the soul of my loving Uncle, Mr. Yaser Hamza for inspiring me to pursue my graduate studies. His devotion to his teaching work and students was a distinguished example influenced me through my life and university studies. I would like to express my special feeling of gratitude for my husband, Dr. Muhsen Owaida, for his unwavering encouragement and valuable counsel through my thesis work.

Declaration

I certify that this thesis, submitted for the degree of Master of Mathematics to the Department of Mathematics at Birzeit University, is of my own research except where otherwise acknowledged, and that this thesis (or any part of it) has not been submitted for a higher degree to any other university or institution.

Tasneem Hamza Signature .....

June 30, 2014

Abstract

Chaos theory has been at the forefront of research in the last few decades. In this research, we study chaos theory and various definitions of chaos, especially Devaney's definition of chaos. We propose a generalization of Devaney's chaos in metric spaces onto topological spaces. We also propose a relaxation on Devaney's definition conditions and study the effect of such relaxation on chaos definition. At last, we study the application of chaotic maps in hash functions and propose a new method for hash function construction using the Double chaotic map.

ملخص

برزت نظرية الفوضى في طليعة البحوث في العقود القليلة الماضية. في هذا البحث، ندرس نظرية الفوضى وتعريفات مختلفة لها، وخاصة تعريف **ديفاني** لنظرية الفوضى.في هذا البحث نقترح تعميما لتعريف **ديفاني** لنظرية الفوضى في الفضاءات المترية على الفضاءات الطوبوغرافية. نحن أيضا قمنا بعمل بعض التعديلات تعريف **ديفاني** وقمنا بدراسة تأثير هذه التعديلات على تعريف نظرية الفوضى. في النهاية، قمنا بدراسة تطبيقات الدالات الفوضوية في تطبيقات أمن الحاسوب والمعلومات، وخصوصا نستخدم الدالة الفوضوية المزدوجة.

Contents

1 Introduction

1.1 History of Chaos Theory

Chaos theory is the science of describing the behavior of dynamical systems, it has been of significant interest in the last few decades. Applications of chaos theory span several fields of science like astronomy, biology, metrology, population, and economics. First encounters of chaotic behavior were mentioned in the work of Henri Poincaré in his study of the **n-body problem** in the 1880s. According to Poincaré, long-term unpredictability makes determinism and randomness somewhat harmonious. Poincaré found that if we have the exact laws governing the universe state, and we know the accurate initial state of the universe, then we can predict precisely the future state of the universe. But, even a very small error in approximating the initial state, will lead to random phenomenon and make the future state of the universe unpredictable, this was the first encounter of sensitivity to initial conditions.

Edward Lorentz is considered the official discoverer of chaotic behavior and chaos theory. In 1961, he first encountered the phenomenon during his experiments and calculations on predicting weather forcasts using nonlinear dynamical models. During his time, it was known among mathematicians that small variations in calculations produce small difference in results. What happened is that during the first trial of experiments he used 6-digit numbers, and during a second trial of experiments, he used 3-digit numbers which did not provide the same solutions. The work of Lorentz coined the term "Butterfly effect", which means flapping of a butterfly wings today may produce a storm after a period of time [22].

The term chaos was first introduced in the paper of the mathematician James A. Yorke titled "Period Three Implies Chaos". Yorke defined the chaotic function and proved that for continuous map f on a closed interval I, if there exists periodic point in I of period 3 then f is a chaotic function.

In 1976, the biologist Robert M. May introduced the logistic map as a simple equation with complex dynamics. Mitchell Jay Feigenbaum used the logistic map to demonstrate the transition between regular dynamics and chaos.

During the last few decades, research in chaotic dynamical systems flourished and has gotten a lot of interest. At the close of the eighties, Robert L. Devaney published his popular book "An Introduction to Chaotic Dynamical Systems", making chaos theory popular that it entered universities as a course in dynamical systems. In 1989, Devaney published his definition of chaotic functions in metric spaces laying the basis for future definitions of chaos.

1.2 Basic Definitions

In this section we quote some definitions that will be used in the following chapters.

Definition. 1.2.1. *Let $f : X \to X$ be a function. A point $x \in X$ is called a* ***periodic point*** *of f if there exists a natural number n such that $f^n(x) = x$. We denote the set of periodic points of the function f by $P(f)$.*

Definition. 1.2.2. *Let $f : X \to X$ be a function. A point $x \in X$ is called a* ***recurrent point*** *of f if there exists a sequence n_k such that $f^{n_k}(x)$ converges to x.*
We denote the set of recurrent points of the function f by $R(f)$.

Definition. 1.2.3. *Let $f : X \to X$ be a function. The* ***orbit*** *of x denoted by $O(x)$, is defined to be $O(x) = \{f^n(x) | n \geq 0\}$.*

Definition. 1.2.4. *A G_δ-**set** is a subset of a topological space that is a countable intersection of open sets.*

Definition. 1.2.5. *A point $x \in X$ is called a* ***transitive point*** *if $\overline{O(x)} = X$. We denote the set of all transitive points by Tr_f.*

Definition. 1.2.6. *A subset S of X is called a* ***residual set*** *if it contains a dense G_δ-set.*

Definition. 1.2.7. *The ω-**limit set** of $x \in X$, denoted by $\omega(x)$, is the set of cluster points of the orbit $\{f^n(x)\}_{n\in\mathbb{N}}$.*

Definition. 1.2.8. *Let X be a metric space and let $f : X \to X$ be a continuous map. Then:*

1. *If for every pair of nonempty open subsets U and V in X, there is a positive integer n such that $f^n(U) \cap V \neq \phi$ then f is called UV-**topologically transitive**.*

2. *If there is a point $x_0 \in X$ such that the orbit of x_0 is dense in X, then f is called OX-**topologically transitive**.*

Throughout the text when we say a function f is *transitive* we mean UV-topologically transitive.

Definition. 1.2.9. *Let X be a metric space with metric d and let $f : X \to X$ be a continuous map. We say that f has* ***sensitive dependence on initial conditions*** *if there exists $\delta > 0$ such that for any $x \in X$ and for any open neighborhood $B_\epsilon(x)$ of x where $\epsilon > 0$, there exists $y \in B_\epsilon(x)$ and $n \geq 0$ such that*

$$d(f^n(x), f^n(y)) \geq \delta.$$

Definition. 1.2.10. *A subset A of a topological space X is called a* ***dense set*** *in X if for all $x \in X$ either $x \in A$ or it is a limit point of A. Equivalently, a subset A of a topological space X is called a* ***dense set*** *in X if for all $x \in X$ and any neighborhood U of x, $U \cap A \neq \phi$.*

Definition. 1.2.11. *A* ***nowhere dense set*** *in a topological space is a set whose closure has empty interior.*

Definition. 1.2.12. *A function $f \colon X \to Y$ between two topological spaces (X, τ_X) and (Y, τ_Y) is callled a* ***homeomorphism*** *if it has the following properties :*

1. *f is a bijection (one to one and onto).*
2. *f is continuous.*
3. *The inverse function f^{-1} is continuous.*

Definition. 1.2.13. *We say that X is* ***isomorphic*** *to Y if there exists a function $f : X \to Y$ such that*

1. *f is a homeomorphism.*
2. *f is onto.*
3. *f is one to one.*

Definition. 1.2.14. *A topological space X is* ***compact*** *if any open cover of X has a finite subcover.*

Definition. 1.2.15. *A topological space X is* ***perfect*** *if it has no isolated points.*

Definition. 1.2.16. *A topological space X is* ***seperable*** *if it contains a countable dense subset.*

Definition. 1.2.17. *A metric space is called* ***complete*** *if every Cauchy sequence in X converges in X.*

Definition. 1.2.18. *A* ***Baire Space*** *is a topological space such that the intersection of any countable collection of open dense sets in the space is also dense.*

Definition. 1.2.19. *Consider the continuous and differentiable map $f : \mathbb{R} \to \mathbb{R}$. Then the map f is said to be expanding if $|f'(x)| > 1$; for all $x \in \mathbb{R}$.*

Definition. 1.2.20. *A metric space (X, d) is **totally bounded** if and only if for every real number $\epsilon > 0$, there exists a finite collection of open balls in X of radius ϵ whose union contains X.*

Definition. 1.2.21. *Let X and Y be topological spaces, and let $f\colon X \to X$ and $g\colon Y \to Y$ be continuous functions. We say that f is topologically **conjugate** to g if there exists a homeomorphism $h\colon Y \to X$ such that $f \circ h = h \circ g$.*

Definition. 1.2.22. ***Hausdorff space** or T_2 space is a topological space in which distinct points have disjoint neighbourhoods.*

Definition. 1.2.23. *A metric on a set X is a function $d : X \times X \to \mathbb{R}$ that satisfies the following properties:*

1. *$d(x, y) > 0$ for all $x, y \in X$.*
2. *$d(x, y) = 0$ if and only if $x = y$.*
3. *$d(x, y) = d(y, x)$ for all $x, y \in X$.*
4. *$d(x, y) \leq d(x, z) + d(z, y)$ for all $x, y, z \in X$.*

Definition. 1.2.24. *Let X be a metric space. If $S \subseteq X$ and $d \in [0, \infty)$, the d-dimensional **Hausdorff content** of S is defined by*

$$C_H^d(S) := \inf\Big\{\sum_i r_i^d : \text{ there is a cover of } S \text{ by balls with radius } r_i > 0\Big\}.$$

Definition. 1.2.25. *The **Hausdorff dimension** of X is defined by*

$$\dim_{\mathrm{H}}(X) := \inf\{d \geq 0 : C_H^d(X) = 0\}.$$

For example, the Hausdorff dimension of the circle S^1 is 1 and the Hausdorff dimension of the Euclidean space $\mathbb{R}^n$ is n.

Note that, the metric dimension that used in this research refers to Hausdorff dimension.

1.3 Research Objectives and Contributions

Devaney's definition of chaos has been a major step in defining chaos in metric spaces. Many definitions have been introduced for chaos in metric spaces. On the other hand, chaos in topological spaces attracted very few researchers. In this thesis, our contribution is threefold:

1. We look into developing new definition of chaos in topological spaces. We provided a generalization of Devaney's definition of chaos in metric spaces onto topological spaces.

2. We proposed some modifications on Devaney's definition conditions by weakening them and testing if the definition is still valid.

3. At last, we proposed a new method for building hash functions using the Double chaotic map.

We currently working on submitting our contribution in this thesis as a journal paper [16].

1.4 Thesis Structure

The structure of the thesis is as follows:

Chapter2 introduces Devaney's definition and study its conditions. Then it presents D-Chaos definition.

Chapter3 studies transitivity and discusses some crosslinks, and properties that could imply transitivity.

Chapter 4 introduces our main contribution in this thesis; generalization of Devaney's definition on topological spaces and relaxation of Devaney's definition conditions.

Finally, in **Chapter 5** we study hash functions as an application for chaotic maps and propose a new method for building hash functions using the Double chaotic map.

2 Chaos in Metric Spaces

We first talk about Devaney's definition of chaos in metric spaces and consider the redundancies in the definition.

2.1 Devaney's Definition of Chaos

Let X be a metric space. A map $f : X \to X$ is said to be chaotic on X if :

1. f is transitive.
2. The set of periodic points is dense.
3. f has sensitive dependence on initial conditions.

Banks et al. proved that for a continuous map in any metric space X, conditions(1) and (2) imply (3) as they proved in [4, Theorem 1].

Theorem. 2.1.1. *[4, Theorem 1] Let X be a metric space and let $f : X \to X$ be a continuous map. If f is transitive and the periodic points are dense in X then f has sensitive dependence on initial conditions.*

Proof. Notice that there exists $\delta_0 > 0$ such that we can find two periodic points p_1 and p_2 where their orbits are disjoint with distance more than δ_0. Let t, s be any positive numbers such that:

$$d(f^t(p_1), x) + d(f^s(p_2), x) \geq d(f^t(p_1), f^s(p_2)) \geq \delta_0$$

If $d(f^t(p_1), x) \leq \dfrac{\delta_0}{2}$ then $d(f^s(p_2), x) \geq \dfrac{\delta_0}{2}$ and If $d(f^s(p_2), x) \leq \dfrac{\delta_0}{2}$ then $d(f^t(p_1), x) \geq \dfrac{\delta_0}{2}$.

So there exists a periodic point say p_3 such that the distance between the orbit of p_3 and any point $x \in X$ is at least $\dfrac{\delta_0}{2}$.

$$\text{That is} \qquad d(x, f^t(p_3)) \geq \frac{\delta_0}{2}, \quad \text{for all } t \in \mathbb{Z}^+$$

Now, suppose $\delta = \dfrac{\delta_0}{8}$ and let $x \in X$ and N be any neighborhood of X. Suppose $U = N \cap B_\delta(x)$ where $B_\delta(x) = \{y \in X \mid d(y, x) < \delta\}$.

So U is a nonempty open set since it is the intersection of two open sets and there exists $p \in U$ where p is a periodic point of order n. Set

$$V = \bigcap_{i=0}^{n} f^{-i}(B_\delta(f^i(p_3)))$$

So V is a nonempty open set since it is the intersection of a finite collection of open sets and $p_3 \in V$. But f is transitive so for any two nonempty open sets U and V there exists $y \in U$ such that $f^k(y) \in V$ where k is a nonnegative integer.

Now, let $m \in \mathbb{Z}^+$ such that $\frac{1}{n} + \frac{k}{n} \leq m \leq 1 + \frac{k}{n}$. Then $1 \leq mn - k \leq n$ and $f^{mn}(p) = p$. Also,

$$f^{mn}(y) = f^{mn-k}(f^k(y)) \ \in f^{mn-k}(V) \subseteq B_\delta(f^{mn-k}(p_3))$$

This implies that

$$d(x, f^{mn-k}(p_3)) \leq d(x,p) + d(p, f^{mn}(y)) + d(f^{mn}(y), f^{mn-k}(p_3))$$

Notice that:

1. $d(x,p) < \delta$, since $p \in B_\delta(x)$ and $p \in U$.
2. $d(f^{mn}(y), f^{mn-k}(p_3)) \leq \delta$, since $f^{mn}(y) \in B_\delta(f^{mn-k}(p_3))$
3. $d(x, f^{mn-k}(p_3)) \leq \frac{\delta_0}{2} = 4\delta$

It follows that

$$4\delta \leq d(p, f^{mn}(y)) + 2\delta \Longrightarrow d(p, f^{mn}(y)) > 2\delta$$

This means

$$2\delta < d(p, f^{mn}(y)) < d(p, f^{mn}(x)) + d(f^{mn}(x), f^{mn}(y))$$

Then, $d(p, f^{mn}(x)) + d(f^{mn}(x), f^{mn}(y)) > 2\delta$

So $d(p, f^{mn}(x)) > \delta$ or $d(f^{mn}(x), f^{mn}(y)) > \delta$

In either of these cases we can find points p and y in N such that $d(p, f^{mn}(x)) > \delta$ or $d(f^{mn}(x), f^{mn}(y)) > \delta$, so f has sensitive dependence on initial conditions. □

In [27], Vellekoop and Berglund proved that on intervals, transitivity implies chaos in the sense of Devaney. Before we give the proof of this theorem, consider the following lemma that we need for the proof.

Lemma. 2.1.1. *[27, Lemma 1] Suppose that I is an interval and $f : I \to I$ is a continuous map. If $J \subset I$ is an interval which contains no periodic points of f and $z, f^m(z)$, and $f^n(z) \in J$ with $0 < m < n$, then either $z < f^m(z) < f^n(z)$ or $z > f^m(z) > f^n(z)$.*

Proof. Suppose not, i.e there exists $z \in J$ such that $z < f^m(z)$ and $f^m(z) > f^n(z)$ where $0 < m < n$, and J is an interval that has no periodic points.

Consider the function $h(x) = f^m(x)$ this means that $z < h(z)$ and we claim that $z < h(z) < h^{r+1}(z)$ for all $r \in \mathbb{Z}^+$ and then the assumption is not true, so the lemma holds. We prove the claim above by induction, assume $z < h(z) < h^r(z)$ to show that $z < h(z) < h^{r+1}(z)$, suppose it is not true i.e $h(z) > h^{r+1}(z)$ for some $r \in \mathbb{Z}^+$, let $g(x) = h^r(x) - x$ on the interval $[z, h(z)]$ then by induction hypothesis $g(z) = h^r(z) - z > 0$ and

$$\begin{aligned} g(h(z)) &= h^r(h(z)) - h(z) \\ &= h^{r+1}(z) - h(z) < 0 \end{aligned}$$

Now, by the Intermediate Value Theorem there exists $c \in (z, h(z))$ such that $g(c) = 0$ so $h^r(c) = c$ and then $f^{rm}(c) = c$ is a periodic point in J.

On the other hand let $r = n - m > 0$ then $z < h^{(n-m)m}(z) < f^m(z)$ since $f^{n-m}(f^m(z)) < f^m(z)$.

Now, consider the function $k(x) = f^{(n-m)m}(x) - x$ on the interval $[z, f^m(z)]$ then $k(z) > 0$ and $k(f^m(z)) < 0$. Again by the Intermediate Value Theorem there exists $t \in (z, f^m(z))$ such that $f^{(n-m)m}(t) = t$, this means that there is a periodic point t in J which contradicts the assumption. □

Now we give the theorem and its proof.

Theorem. 2.1.2. *[27, Theorem 1] Let I be an interval and let $f : I \to I$ be a continuous map. If f is transitive then the periodic points of f are dense in I and f has sensitive dependence on initial conditions.*

Proof. Suppose that f is transitive. So by Theorem 2.1.1 it suffices to show that the periodic points of f are dense in X.

Assume not, there exists an open interval $J \subseteq I$ such that J has no periodic points. Let $x \in J$ be any point in J.

Let N be a neighborhood of x such that $N \subset J$ and let E be an open set in J/N. Now, by the transitivity of f, for any two nonempty sets J and E, there exists $y \in J$ such that $f^m(y) \in E$, where m is a nonnegative integer. J has no periodic points so $y \neq f^m(y)$.

Let $\epsilon = d(y, f^m(y))$ and let $U' = \{x | d(x, y) < \epsilon/3\}$ be a neighborhood of y, $V = \{z | d(z, f^m(y)) < \epsilon/3\}$ be a neighborhood of $f^m(y)$ then $U' \bigcap V = \phi$. Now, f is continuous then f^m is also continuous and so for any neighborhood V of $f^m(y)$ in I there exists a neighborhood U of y in I such that $f^m(U) \subseteq V$. Consider two cases

Case 1: If $U \subseteq U'$.

Then $U \bigcap f^m(U) = \phi$. Again, f is transitive, so there exists $z \in U$ such that $f^n(z) \in U$, where $n > m$. Finally, there exists $0 < m < n$ and $z, f^n(z) \in U$, but $f^m(z) \notin U$, so this contradicts the Lemma 2.1.1.

Case 2: If $U' \subseteq U$.

Then $U' \bigcap f^m(U) = \phi$. Again, f is transitive, so there exists $z \in U'$ such that $f^n(z) \in U'$, where $n > m$. Finally, there exists $0 < m < n$ and $z, f^n(z) \in U'$, but since $z \in U$ so $f^m(z) \in f^m(U)$ and $U' \bigcap f^m(U) = \phi$ so $f^m(z) \notin U'$, and this contradicts Lemma 2.1.1. □

In the next proposition, we will see another look to sensitive dependence on initial conditions as mentioned in [1, Proposition 2.1.16].

Proposition. 2.1.1. *[1, Proposition 2.1.17] Let $f : I \to I$ be a differentiable map if f is an expanding map then it possess a sensitive dependence on initial conditions.*

Proof. Consider the Lyapunov exponent $\lambda(x)$ for a map f as follows

$$\lambda(x) = \lim_{n\to\infty} \frac{1}{n} \sum_{i}^{n-1} \log |f'(x_i)|, \text{ for all } x_i \in I.$$

Now, take two points x_0, x_1 and let $\delta = |x_0 - x_1|$. Then after n iterations we have

$$\delta x_n = |x_n - x_{n-1}| = |f^n(x_1) - f^n(x_0)| = \delta e^{n\lambda(x_0)}$$

Take the limit of both sides and solve

$$\begin{aligned}\lambda(x_0) &= \lim_{n\to\infty}\lim_{\delta\to 0}\frac{1}{n}\log\Big|\frac{f^n(x_0+\delta)-f^n(x_0)}{\delta}\Big| = \lim_{n\to\infty}\frac{1}{n}\Big|\frac{df^n(x_0)}{dx}\Big| \\ &= \lim_{n\to\infty}\frac{1}{n}\log\Big|\prod_{i=0}^{n-1}f'(x_i)\Big| = \lim_{n\to\infty}\sum_{i=0}^{n-1}\log|f'(x_i)|.\end{aligned}$$

Now, if $m, n \in \mathbb{Z}^+$ then after $m > n$ iterations we get

$$\begin{aligned}|f^m(x_1)-f^m(x_0)| &= \delta x_0 e^{m\lambda(x_0)} \\ &= \delta x_0 e^{(m-n)\lambda(x_0)}e^{n\lambda(x_0)} \\ &= \delta e^{(m-n)\lambda(x_0)} > \delta.\end{aligned}$$

Now, if

$$f'(x_i) > 1$$

then

$$\log|f'(x_i)| > \log 1 = 0$$

this implies that

$$\sum_{i=0}^{n-1}|f'(x_i)| > 0$$

and so

$$\lim_{n\to\infty}\sum_{i=0}^{n-1}|f'(x_i)| > 0$$

then $\lambda(x) > 0$ and so f has a sensitive dependence on initial conditions. □

Examples [2, Example 1], [27, Example 1]

(i) In [2], D. Assaf, and S.Gadbois proved that (1) and (3) do not imply (2). We consider an example

Let $X = \{S^1 \backslash \{e^{(i2\pi p)/q} | p, q \in \mathbb{Z}, q \neq 0\}$, where the metric is the usual arc length i.e $d(e^{i\theta}, e^{i\phi}) = |\theta - \phi|$. Let $f : X \to X$ be a map defined by $f(e^{i\theta}) = e^{i2\theta}$, then

(a) f is transitive. Take any two nonempty open sets U, V of X, then there exists $y \in U$ such that $f^k(y) \in V$ for some k nonnegative integer, since $f^k(V)$ expands to cover all X.

(b) f contains no periodic points. x is a periodic point of f if and only if there exists $k \in \mathbb{Z}^+$ such that $f^k(x) = x$ i.e. if $f^k(e^{i\theta}) = e^{i\theta}$ then

$$\begin{aligned} & e^{i\theta 2^k} &=& e^{i\theta} \\ so, \quad & e^{i\theta(2^k-1)} &=& 1 \\ and, \quad & i\theta(2^k-1) &=& 0 \\ then, \quad & \theta &=& 2n\pi \end{aligned}$$

We remove the periodic points from the set X . So there are no periodic points.

(c) f has sensitive dependence on initial conditions. Let $\delta = \dfrac{\pi}{2} > 0$, and take any point $e^{i\theta} \in X$. This implies that there exists $e^{i\phi} \in X$ such that $0 < |\theta - \phi| < \pi$. Now, choose $n \in \mathbb{Z}^+$.

$$\begin{aligned} so, \quad & 2^n|\theta-\phi| < \pi < 2^{n+1}|\theta-\phi| \\ then, \quad & d(f^n(e^{i\theta}), f^n(i\phi)) = d(e^{i2^n\theta}, e^{i2^n\phi}) > \frac{\pi}{2}. \end{aligned}$$

(ii) In [27], Vellekoop and Berglund give a counter example that shows conditions (2) and (3) don not imply (1). Let

$$f(x) = \begin{cases} 3x, & 0 \le x < \frac{1}{3}; \\ -3x+2, & \frac{1}{3} \le x < \frac{2}{3}; \\ 3x-2, & \frac{2}{3} \le x < 1; \\ f(x-1), & x \ge 1. \end{cases}$$

(a) f is not transitive. Notice that $f([0,1]) = [0,1]$ and any open set in $(1,\infty)$ does not intersect $f^k(U)$, where U is open set in $(0,1)$.

(b) The periodic points are dense in X. Consider $f^n(x)$ as follow.

$$f^n(x) = \begin{cases} 3^n x - i, & \frac{i}{3^n} \le x < \frac{i+1}{3^n}; \quad \text{if } i \text{ is even} \\ -3^n x + (i+1), & \frac{i}{3^n} \le x < \frac{i+1}{3^n}; \quad \text{if } i \text{ is odd} \\ f^n(x-1), & x \ge 1. \end{cases}$$

Where $i = 0, 1, 2, \cdots, 3^n - 1$. Notice that the fixed points of $f^n(x)$ are

1. $x = \dfrac{i}{3^{n-1}}$, if i is even except at $i = 3^{n-1}$.
2. $x = \dfrac{i+1}{3^{n+1}}$, if i is odd.

So the distance between any two fixed points is less than $(\frac{1}{3})^{n-1}$. So the periodic points are dense in X.

(c) f has sensitive dependence on initial conditions. Since $|f'(x)| = 3$, for all $x \in [0, \infty)$. By Proposition 2.1.1 we get that f has sensitive dependence on initial conditions.

2.2 D-Chaos

Aullbach establishes in [3, Definition 3.3] the D-chaos definition that we present here, which gives us a generalization of the Devaney's definition of chaos in a compact metric space.

Definition. 2.2.1. *[3, Definition 3.3] A continuous map $f : X \to X$ where X is a compact metric space is called D-chaotic if there exists a compact invariant subset Y of X such that:*

1. *$f|_Y$ is transitive.*
2. *$\overline{(P(f)|_Y)} = Y$.*
3. *$f|_Y$ has sensitive dependence on initial conditions.*

if $Y = X$ in the D-chaos definition, then (X, f) is a chaos in the sense of Devaney.

Lemma. 2.2.1. *A function is invertible if and only if it is bijective.*

Proof. The first direction. Suppose that a function $f : X \to Y$ is invertible and let f^{-1} be its inverse. First we show that f is injective, so let $a, b \in X$ such that

$$\begin{aligned} & f(a) = f(b), \\ so, \quad & f^{-1}(f(a)) = f^{-1}(f(b)), \\ then, \quad & id(a) = id(b), \\ and, \quad & a = b \end{aligned}$$

To show f is surjective, let $y \in Y$ and let $f^{-1}(y) = x$ for some $x \in X$. This implies that $f(x) = f(f^{-1}(y)) = id(y) = y$, so f is bijective.

The opposite direction. Suppose that f is bijective and let $y \in Y$. Since f is surjective so there exists $x \in X$ such that $f(x) = y$. Also, f is injective so x is unique.

Now, define $g : Y \to X$ such that $g(y) = x$. So g is well defined. And

$$g(y) = x$$

then,

$$f(g(y)) = f(x) = y = id(y)$$

and,

$$g(y) = x$$

then,

$$g(f(x)) = g(y) = x = id(x)$$

We conclude that g is the inverse of f, and f is invertible. □

Consider the next proposition as mentioned in [3, Proposition 3.1].

Proposition. 2.2.1. *[3, Proposition 3.1] Let (X, d_X) and (Y, d_Y) be compact metric spaces and suppose that a continuous map $f : X \to X$ is conjugate to continuous map $g : Y \to Y$. Then f is D-chaotic if and only if g is D-chaotic.*

Proof. Let f be D-chaotic and suppose that f is conjugate to g, so there exist a homeomorphism (continuous and an invertible map with continuous inverse) $h : X \to Y$ such that $h \circ f = g \circ h$. We want to show that g is D-chaotic.

Let $G = h(F) \subseteq Y$, where F is a compact invariant subset of X. We know that the image of a continuous compact set is compact. So G is a compact subset of Y and invariant

$$\begin{aligned} g(G) &= g(h(F)) \\ &= h(f(F)) \\ &\subseteq h(F) = G \end{aligned}$$

We want to show the following three conditions:

1. $g|_G$ is transitive. Suppose not, so there exists two nonempty open subsets $U, V \subseteq G \subseteq Y$ of G such that

$$g^k(U) \cap V = \phi, \qquad \text{for all } k \in \mathbb{Z}^+.$$

But, h is surjective, so there exists $N \subseteq F \subseteq X$ an open set in F such that $h(N) = U$, note that we restrict $h : F \to G$. Also, $h \circ f = g \circ h$ and h is invertible. Note that

$$\begin{aligned} & g = h \circ f \circ h^{-1} \\ \textit{so}, \quad & g^k = h \circ f \circ h^{-1} \circ h \circ f \circ h^{-1} \cdots \circ h \circ f \circ h^{-1} \quad \text{k-times} \\ \textit{and}, \quad & g^k = h \circ f^k \circ h^{-1} \\ \textit{then}, \quad & g^k \circ h = h \circ f^k \end{aligned}$$

$$\begin{aligned} \text{Now,} \quad g^k(h(N)) \cap V &= \phi \\ h(f^k(N)) \cap V &= \phi \\ h^{-1}(h(f^k(N) \cap V)) &= \phi \\ h^{-1}h(f^k(N)) \cap h^{-1}(V) &= \phi \qquad (\text{ since } h \text{ is } 1-1) \\ f^k(N) \cap h^{-1}(V) &= h^{-1}h(f^k(N)) \cap h^{-1}(V) = \phi \\ f^k(N) \cap h^{-1}(V) &= \phi \qquad \text{for all } k \in \mathbb{Z}^+ \end{aligned}$$

Which is a contradiction since N and $h^{-1}(V)$ are open subsets in F and X is chaotic. So $g|_G$ is transitive.

2. $\overline{(P(g)|_G)} = G$.
Observe that x is a periodic point of $f|_F$ of order n if and only if $y = h(x)$ is a periodic point of $g|_G$ of order n.
The first direction. Suppose that x is a periodic point of $f|_F$ of order n. i.e. $f^n(x) = x$

$$\begin{aligned} g^n(y) &= g^n(h(x)) \\ &= h(f^n(x)) \\ &= h(x) = y \end{aligned}$$

The opposite direction. Suppose that y is a periodic point $g|_G$ of order n, i.e. $g^n(y) = y$

$$\begin{aligned} \textit{then}, \quad g^n(h(x)) &= h(x) \\ \textit{and}, \quad h(f^n(x)) &= h(x) \qquad (h \text{ is } 1-1) \\ \textit{so}, \quad f^n(x) &= x \end{aligned}$$

Now, assume $\overline{(P(g)|_G)} \neq G$, so there exists an open set V in G such that $(P(g)|_G) \bigcap V = \phi$. This means that $y \notin V$, for all periodic points in G. But, a periodic point x in F such that $h(x) = y$ of the same period.

$$\begin{array}{rrcll} & h(x) & \notin & V, & \\ \textit{then}, & h^{-1}(h(x)) & \notin & h^{-1}(V) & \\ \textit{and}, & x & \notin & h^{-1}(V), & \text{for all } x \text{ periodic point in } F. \end{array}$$

But $h^{-1}(V)$ is an open set in F and $\overline{P(f)|_F}$ is dense in F. So we get a contradiction , which means that $\overline{(P(g)|_G)} = G$.

3. $g|_G$ does not have sensitive dependence on initial conditions. We have that $f|_F$ has sensitive dependence on initial conditions. So there exists $\delta_0 > 0$, such that for all $x \in F$ and for any $\epsilon_0 > 0$, there exists $z \in F$ such that $d(x, z) < \epsilon_0$ and $d(f^n(x), f^n(z)) > \delta_0$.

   Now, let $y \in G$ and $\delta > 0$, so there exists $\epsilon > 0$ and $w \in G$ such that $d(g^n(y), g^n(w)) < \delta$. Also, we know that h is surjective so there exists $x, z \in F$ such that $h(x) = y$ and $h(z) = w$. Then

$$\begin{aligned} d(g^n(y), g^n(w)) &= d(g^n(h(x)), g^n(h(z))) \\ &= d(h(f^n(x)), h(f^n(z))) < \delta \end{aligned}$$

   But, h^{-1} is continuous. And

$$d(h^{-1}(h(f^n(x))), h^{-1}(h(f^n(z)))) < \delta_0$$

   So,

$$d(f^n(x), f^n(z)) < \delta_0$$

   Which contradicts the assumption. So $g|_G$ has sensitive dependence on initial conditions.

□

3 Cross Links of Transitivity

We begin with a section of topological transitivity and consider two definitions of it and then state some theorems. Next, we will see if the map has only one discontinuity, under what condition the transitivity implies the existence of dense orbit? Finally, we consider the indecomposability definition and the relation between it and the transitivity and with other definitions.

3.1 Topological Transitivity

In this section we consider the two definitions of topological transitivity mentioned in Definition 1.2.8 and Definition 1.2.9, then we consider some theorems related to those definitions.

The two definitions of transitivity are equivalent under some conditions. Consider the following theorem as in [12, Proposition 1, Proposition 2].

Proposition. 3.1.1. *[12, Proposition 1, Proposition 2] Let X be a complete metric space with a countable base and $f : X \to X$ a continuous function, also X has no nonempty open subset U that has a finite subset dense on it. Then f is UV-topologically transitive if and only if it is OX-topologically transitive.*

Proof. The first direction. Consider the countable base $\{V_i\}_{i\in I}$ and let

$$W_i = \bigcup_{n=0}^{\infty} f^{-n}(V_i)$$

Since f is continuous, so for every open subset V_i, $f^{-n}(V_i)$ is open, then W_i is open in X. By the transitivity of f, for every nonempty open subset U of X, there exists $n \in \mathbb{Z}^+$ such that

$$\begin{aligned} f^n(U) \cap V_i \neq \phi \quad \textit{implies} \qquad & f^{-n}(f^n(U) \cap V_i) \neq \phi \\ \textit{then}, \qquad & U \cap f^{-n}(V_i) \neq \phi \\ & U \cap \bigcup_{n=0}^{\infty} f^{-n}(V_i) \neq \phi \\ & U \cap W_i \neq \phi \end{aligned}$$

So W_i is dense in X, and this true is for all $i \in I$.

By Baire Category theorem, every completely metrizable topological space is a Baire space. So $\bigcap_{i\in I} W_i$ is dense in X. Let $x \in \bigcap_{i\in I} W_i$ and given any nonempty open subset U of X, then there exists $V_i \subseteq U$ for some $i \in I$ (since $\{V_i\}_{i\in I}$ is a base of X). We showed above that there exists $n \in \mathbb{Z}^+$ such that $x \in f^{-n}(V_i)$, so $f^n(x) \in V_i \subset U$, this implies that $f^n(x) \in U$, for some $n \in \mathbb{Z}^+$. This means the orbit of x is dense in X, for every $x \in \bigcap_{i\in I} W_i$.

The opposite direction. Suppose that X has a dense orbit at $x \in X$ and let U, V be two nonempty open subsets of X. there exists $m, n \in \mathbb{Z}^+$ such that $f^m(x) \in U$, $f^n(x) \in V$ (suppose m, n are the least positive integer). Consider two cases :

Case 1: If $m \geq n$.

This means that $f^m(x)$ get in V then $f^n(x)$ get in U. So there exists points $\{f^{k_1}(x), f^{k_2}(x), \cdots, f^{k_s}(x)\}$. Where $n \leq k_i \leq m$, for all $i = 1, 2, \cdots, s$. By assumption that V has no finite dense subset, so there is an open set $W \subseteq V$ such that W does not have any element of these set. On the other hand, there exists $r \in \mathbb{Z}^+$ with $f^r(x) \in W$ (since we assume that the orbit of x is dense). Set $j = r - m > 0$ so $f^j(U) \cap V \neq \phi$.

Case 2: If $m < n$.

Let $j = n - m > 0$. Then $f^j(U) \cap V \neq \phi$.
We conclude from the two cases that f is UV-topologically transitive. □

Now, we consider the following proposition that gives another condition for the function f to be UV-topologically transitive if f is OX-topologically transitive, see [24, Proposition 1.1].

Proposition. 3.1.2. *[24, Proposition 1.1] Let X be a prefect space (i.e has no isolated points) then if f is OX-topologically transitive then f is UV-topologically transitive.*

Proof. Suppose X is a perfect space which has a dense orbit say $O(x)$. Now, let U, V be two nonempty open subsets of X.

$f^k(x) \in U$ and $f^m(x) \in V$ for some $k < m \in \mathbb{Z}^+$ this follows since the orbit of x is dense. Now, X has no isolated point so $f^m(x) \in V \backslash \{x, f(x), \ldots, f^k(x)\}$ where $V \backslash \{x, f(x), \ldots, f^k(x)\}$ is nonempty open subset of X.

So we conclude that $f^{m-k}(U) \cap V \neq \phi$ and this implies that f is UV-topologically transitive. □

In general, UV-definition and OX-definition not equivalent. We consider two examples as in [12, Example1, Example 2].

Example. 3.1. *[12, Example 1] Let $X = \{1, 2\}$, and give the discrete topology τ, i.e $\tau = \{\phi, X, \{1\}, \{2\}\}$. Let $f : X \to X$ be a continuous map such that $f(x) = 2$.*

$O(1) = \{1, f(1)\} = \{1, 2\} = X$ is dense in X. So OX-definition is satisfied.

But f does not satisfy the UV-definition, Let $U = \{2\}, V = \{1\}$, then $f^k(U) = \{2\} \cap V = \phi$ for all $k \in \mathbb{Z}^+$.

Example. 3.2. *[12, Example 2] Let $X = \{\theta \in S^1 | \theta = \frac{2k\pi}{2^n-1}, n \in \mathbb{Z}^+, 0 \leq k \leq 2^n - 1\}$ and define $f : X \to X$ a continuous map such that $f(\theta) = 2\theta$, and let $g : S^1 \to S^1$ be defined as $g(\theta) = 2\theta$. Let U, V be two nonempty open subsets in X, so $U = \acute{U} \cap X$, $V = \acute{V} \cap X$, where $\acute{U}, \acute{V}$ are open sets in S^1. Also, $g^k(\acute{U}) = S^1$ for some $k \in \mathbb{Z}^+$. So $g^k(\acute{U}) \cap \acute{V} \neq \phi$.*

The periodic points of g are

$$\begin{aligned} g^n(\theta) = \theta \quad & implies \quad 2^n\theta = \theta + 2k\pi \\ & then, \quad 2^n\theta - \theta = 2k\pi \\ & \theta = \frac{2k\pi}{2^n - 1} \end{aligned}$$

We get that the elements of X are periodic points of the function g.

Now, there exists a periodic point $p \in \acute{U}$ and $g^k(p) \in \acute{V}$, (since the periodic points of g are dense in S^1). But, $p \in X$ this implies $p \in U = X \cap \acute{U}$, $f^k(p) = g^k(p) \in V = \acute{V} \cap X$, so $f^k(U) \cap V \neq \phi$. This means that f is UV-topologically transitive.

On the other hand, f is not OX-topologically transitive since any orbit in X is periodic orbit and so there is no dense orbit on X.

Let us consider the following theorems.

Theorem. 3.1.1. *Every compact metric space is seperable.*

Theorem. 3.1.2. *A metric space is compact if and only if it is complete and totally bounded.*

Theorem. 3.1.3. *Every seperable metric space has countable basis.*

Lemma. 3.1.1. *Let X be a metric space. Then*

1. *The union of finitely many nowhere dense sets is nowhere dense.*
2. *If X has no isolated points then every finite subset of X is nowhere dense.*

Theorem. 3.1.4. *[17],[9],[28],[13], [12] Let $f : X \to X$ be a continuous map, X be a compact perfect metric space, and $f(X) = X$, then the following are equivalent:*

1. *f is UV-topologically transitive.*
2. *f is OX-topologically transitive.*
3. *Whenever E is a closed subset of X and $f(E) \subseteq E$, then either $E = X$ or E is nowhere dense.*
4. *Whenever U is an open subset of X and $f^{-1}(U) \subseteq U$, then $U = \phi$ or U is dense in X.*
5. *For every nonempty open subset U in X, $\bigcup_{n=1}^{\infty} f^{-n}(U)$ is dense in X.*
6. *For every nonempty open subset U and V in X, there exists $n \in \mathbb{Z}^+$ such that $f^{-n}(U) \cap V \neq \phi$.*
7. *The set of points $\{x|\overline{O_f(x)} = X\}$ is a dense G_δ-set.*
8. *For every nonempty open subset U in X, $\bigcup_{n=1}^{\infty} f^n(U)$ is dense in X.*

Proof. (1) and (2) are equivalent

Since X is compact so we conclude by Theorem 3.1.1, Theorem 3.1.2 and Theorem 3.1.3 that X is complete and has countable bases. Also, X is perfect so it has no isolated points then by Lemma 3.1.1 every finite subset of X is nowhere dense, this implies that X has no nonempty open subset U that has a finite subset dense on it.

We get by Proposition 3.1.1 that f is UV-topologically transitive if and only if f is OX-topologically transitive.

(2) implies (3)

Let $x \in X$ such that $\overline{O_f(x)} = X$, and let E be a closed subset where $f(E) \subseteq E$.
Now, if E is not nowhere dense i.e. $Int(\overline{E}) = Int(E) \neq \phi$, then $Int(E) \subseteq E$ and open, so by denseness of the orbit of x, there exists $f^k(x) \in Int(E)$ for some $k \in \mathbb{Z}^+$ so $f^k(x) \in E$.
Consider the set $\{f^m(x) | m \geq k\} \subseteq E$ since $f(E) \subseteq E$. This implies that

$$\{x, f(x), \cdots, f^{k-1}(x)\} \cup E = X$$

Take f for both sides

$$\{f(x), \cdots, f^{k-1}(x)\} \cup f(E) = f(X) = X$$

By repeating this we get $f(E) = X \subseteq E$ so $E = X$.

(3) implies (4)

Suppose (3) holds and let U be a nonempty open subset in X where $f^{-1}(U) \subseteq U$. Consider $E = X|U$ is a closed subset. Now,

$$\begin{array}{rcll} f(E) = f(X|U) & \subseteq & f(X|f^{-1}(U)) & (since f^{-1}(U) \subseteq U) \\ & = & f(f^{-1}(X|U)) & \\ & \subseteq & X|U = E & \end{array}$$

This implies that $f(E) \subseteq E$, by (3) either $E = X$ or E is nowhere dense.
If $E = X$ then $U = \phi$.
If E is nowhere dense, i.e. $Int(E) = \phi$ then

$$\begin{array}{rcl} \overline{U} = \overline{X|E} & = & X|Int(E) \\ & = & X|\phi \\ & = & X \end{array}$$

So U is dense in X.

(4) implies (5)

Let U be any nonempty open subset in X. Then

$$\begin{aligned} f^{-1}(\bigcup_1^\infty f^{-n}(U)) &= \bigcup_1^\infty f^{-1}(f^{-n}(U)) \\ &= \bigcup_1^\infty f^{-n-1}(U) \subseteq \bigcup_1^\infty f^{-n}(U) \end{aligned}$$

So $\bigcup_1^\infty f^{-n}(U)$ is open, $f^{-1}(\bigcup_1^\infty f^{-n}(U)) \subseteq \bigcup_1^\infty f^{-n}(U)$ and $\bigcup_1^\infty f^{-n}(U) \neq \phi$, by (4) we get $\bigcup_1^\infty f^{-n}(U)$ is dense in X.

(5) implies (6)

Suppose U, V be two nonempty open subset in X. So $\bigcup_1^\infty f^{-n}(U)$ is dense in X.

$$\bigcup_1^\infty f^{-n}(U) \cap V \neq \phi$$

This is equivalent to $f^{-n}(U) \cap V \neq \phi$ for some $n \in \mathbb{Z}^+$.

(6) implies (7)

Let $\{U_n\}_1^\infty$ be a topological basis. So we get that

$$\{x|\overline{O_f(x)}\} = \bigcap_{n=1}^\infty \bigcup_{k=1}^\infty f^{-k}(U_n) \neq \phi$$

Since for every U_n open subset in X, there exists $f^k(x) \in U_n$ for some $k \in \mathbb{Z}^+$, this implies that $x \in f^{-k}(U_n)$.
Now, by (6) $\bigcup_{k=1}^\infty f^{-k}(U_n)$ is dense for all $n \in \mathbb{Z}^+$. But X is compact then it is complete, so by Baire Category theorem, $\bigcap_{n=1}^\infty \bigcup_{k=1}^\infty f^{-k}(U_n)$ is a dense G_δ-set.

(7) implies (2)

If (7) holds then it is clear that (2) holds.

(1) equivalent to (8)

Let U, V be two nonempty open subsets in X. Then
$f^n(U) \cap V \neq \phi$, for some $n \in \mathbb{Z}^+$
This is equivalent to $\bigcup_1^\infty f^n(U) \cap V \neq \phi$. Then $\bigcup_1^\infty f^n(U)$ is dense in X. $\square$

3.2 Discontinuity and Transitivity

In [1, Proposition 1], it has been proved that if $f : X \to X$ is a continuous map where X is a complete metric space with a countable base and if f is UV-topologically transitive then it has a dense orbit. But, in [13] they showed that in a Baire seperable metric space, if f has a discontinuity at most one point then UV-topological transitivity implies OX-topological transitivity.

Proposition. 3.2.1. *[1, Proposition 1] Let $f : X \to X$ be a UV-topologically transitive map on a Baire seperable metric space X. Then if f has only one point of discontinuity then f has a dense orbit.*

Proof. Let z be a point of discontinuity and suppose f is UV-topologically transitive of a Baire seperable metric space X. If $\overline{O(z)} = X$ then we are done.
If $\overline{O(z)} \neq X$, so there exists an open subset V such that $V \cap \overline{O(z)} = \phi$. We claim that $O(z)$ is nowhere dense.

Suppose $O(z)$ is not nowhere dense, this means that $Int(\overline{O(z)}) \neq \phi$, let $U = Int(\overline{O(z)}) \subseteq \overline{O(z)}$. By the transitivity of f, there exists $q \in U$ such that $f^m(q) \in V$, for some $m \in \mathbb{Z}^+$. We conclude that $f^m(q) \neq f^n(z)$, for every $n \in \mathbb{Z}^+$, this implies that f^m is continuous at q (Since f is continuous). That means there exists an open neighborhood W of q such that $f^m(W) \subseteq V$.

On the other hand, there exists $k \in \mathbb{Z}^+$ such that $f^k(z) = q$ (Since $q \in U$), then we have $f^{k+m}(z) \in V$ and this yields to a contradiction.

Now, consider the countable basis $\{U_n\}_{n \in \mathbb{Z}^+}$ of $X/\overline{O(z)}$ and let

$$T_n = \{x \in X | f^k(x) \in U_n, \text{ for some } n \in \mathbb{Z}^+\}.$$

Let $x \in T_n$ then there exists $k \in \mathbb{Z}^+$ such that $f^k(x) \in U_n$, and we know that f^k continuous at x and this means that $f^k(U) \subseteq U_n$, for some open neighborhood U of x, thus T_n is open.

Take any nonempty open subset V in X, by transitivity of f there exists $y \in V$ such that $f^k(y) \in U_n$ for some $k \in \mathbb{Z}^+$, hence $y \in T_n$ and T_n is dense in X, and this is true for all T_n's. Now, since X is a Baire space so $\bigcap_{n\in\mathbb{Z}^+} T_n$ is also dense in X and it follows that $\overline{O(x)} = X$, for all $x \in \bigcap_{n\in\mathbb{Z}^+} T_n$.

□

In the following example A. Peris [23] gives a function that is discontinuous at two points and shows that the previous proposition does not hold.

Example. 3.3. *[23, Example 1] Consider the tent map.*

$$T(x) = \begin{cases} 2x; & 0 \le x \le 1/2 \\ 2(1-x) & 1/2 < x \le 1 \end{cases}$$

It is clear that $T(x)$ is a continuous function and $T(x)$ is a UV-topologically transitive map. So, by Theorem 3.1.1 the tent map has a dense orbit.

Now, let $y_1 \in (0,1)$ such that $O_T(y_1)$ is dense in $[0,1]$ and take $y_0 = y_1 + 1$. Define $f(x)$ as:

$$f(x) = \begin{cases} T(x) & 0 \le x < 1 \\ y_0 & x = 1 \\ 1 + T(x-1) & 1 < x < 2 \\ y_1 & x = 2 \end{cases}$$

At first we will show that $f(x)$ does not have a dense orbit.

Notice that $O_T(y_1) = O_f(y_1)$ so it is dense in $(0,1)$. It follows that, $1 + O_T(y_0 - 1) = \{x_n\}_{n\in\mathbb{Z}^+}$ is dense in $(1,2)$. Then

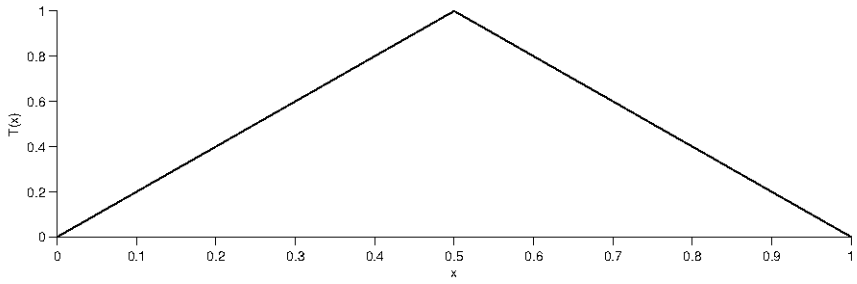
$$f(y_0) = 1 + T(y_0 - 1) \quad \textit{and} \quad f(x_1) = 1 + T(x_1 - 1) = 1 + T^2(y_0 - 1) = x_2.$$

Inductively, we have $x_{n+1} = f(x_n)$ and hence $O_f(y_0)$ is dense in $(1,2)$.

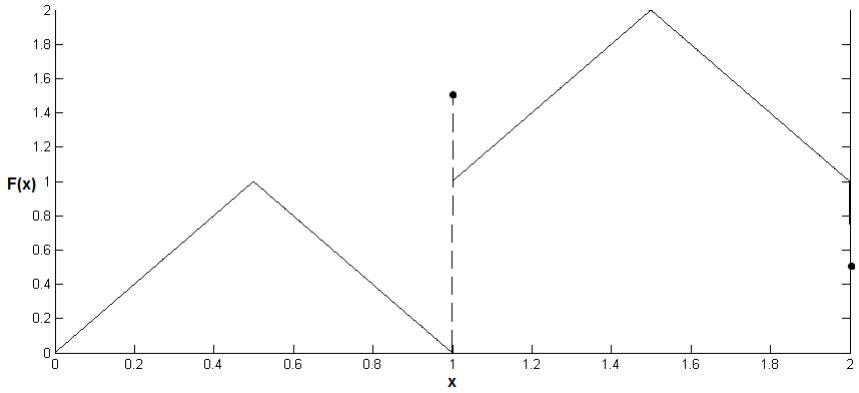
We conclude that $O_f(y_1)$ is dense in $(0,1)$ and $O_f(y_0)$ is dense in $(1,2)$

Now, suppose $x = \frac{k}{2^n}$, where $k, n \in \mathbb{Z}^+$ we have shown that $O_f(y_1)$ is dense in $(0,1)$ and $O_f(y_0)$ is dense in $(1,2)$. Then $f^m(x) = y_1$ if $x \in (0,1)$ or $f^m(x) = y_0$ if $x \in (1,2)$. Moreover,

$$T(\frac{1}{2}) = 1, T^2(\frac{1}{4}) = T^2(\frac{3}{4}) = 1, \ldots T^n(\frac{k}{2^n}) = 1.$$



(a) Tent Map T(x).



(b) Modified Tent Map f(x)

Figure 1: Plots of T(x) and f(x)

This is true if $x = \frac{k}{2^n} \in (0,1)$ *and in irreducible form. This implies that*

$$y_0 = f^m(x) = f(f^{m-1}(x)) = f(T^{m-1}(x)) = f(1)$$

For $x \in (1,2)$ *and* $f(x) > 1$ *then if* $f(x) = 2$ *we get* $f^2(x) = f(2) = y_1$, *or if* $1 < f(x) < 2$ *we iterate the map* f *until we find* $k \in \mathbb{Z}^+$ *such that* $T^k(x-1) = 1$, *and since* $f^t(x) = 1 + T^t(x-1) = f(1) = y_0$, *where* $1 \leq t \leq m$, *then we get* $f^{m+1}(x) = y_1$.

Finally, let $x \in [0,2]$ *then consider two cases.*

Case 1 : $x \in [0,1]$.

Either $x = \frac{k}{2^n}$ *then* $f^m(x) = y_0$ *for some* $m \in \mathbb{Z}^+$ *so for all* $t \geq m, f^t(x) \in (1,2)$. *Or* $x \neq \frac{k}{2^n}$ *then* $f^n(x) = T^n(x) \in [0,1)$.

Case 2 : $x \in (1,2]$.

Either $x = \frac{k}{2^n}$ *then* $f^m(x) = y_1$ *for some* $m \in \mathbb{Z}^+$ *so for all* $l \geq m, f^l(x) \in (0,1)$. *Or* $x \neq \frac{k}{2^n}$ *then* $f^n(x) = T^n(x) \in (1,2)$.

So we conclude that f *does not have a dense orbit.*
Then we will show that f *is UV-topologically transitive. Let* U, V *be two nonempty open subset in* $(0,2)$. *There are four cases :*

Case1: *If* $U, V \subseteq (0,1)$ *and we know that* $O(y_1)$ *is dense in* $(0,1)$ *then there exists* $n, m \in \mathbb{Z}^+$ *such that* $f^n(y_1) \in U$, $f^m(y_2) \in V$ *and suppose* $n < m$, *if we let* $k = n - m$ *then we get* $f^k(f^n(y_1)) \in f^k(U) \cap V$, *so* $f^k(U) \cap V \neq \phi$.

Case2: *If* $U, V \subseteq (1,2)$ *and we know that* $O(y_0)$ *is dense in* $(1,2)$ *so as in* ***Case1****, it follows that* $f^k(U) \cap V \neq \phi$.

Case3: *If* $U \subseteq (0,1)$ *and* $V \subseteq (1,2)$, *we can choose* n, k, m *such that* $f^m(\frac{k}{2n}) = y_0$ *this implies that* $f^t(y_0) \in V$, *for some* $t > m$ *where* $t \in \mathbb{Z}^+$. *Then* $f^t(U) \cap V \neq \phi$.

Case4: *If* $U \subseteq (1,2)$ *and* $V \subseteq (0,1)$, *as in* ***Case3*** *we can find* $n, k, m \in \mathbb{Z}^+$ *such that* $f^m(\frac{k}{2n}) = y_1 \in U$, *so* $f^t(y_1) \in V$, *for some* $t > m$ *where* $t \in \mathbb{Z}^+$.

Finally, we conclude that f *is UV-topologically transitive but* f *does not have a dense orbit.*

3.3 Indecomposability and Transitivity

In this section we introduce the concept of indecomposability of f and show the relation between transitivity and indecomposability.

Consider the definitions of indecomposability, strongly indecomposable and weakly indecomposable as mentiond in [14, Definition 2.1].

Definition. 3.3.1. *[14, Definition 2.1] Let $f : X \to X$ be a continuous map on the metric space X. Then f is called:*

1. Strongly Indecomposable *if for any sequence of f-invariant closed subsets $\{A_n\}_{n\in\mathbb{Z}^+}$ of X with $Int(A_n) \neq \phi$ then $Int(\bigcap_{n\in\mathbb{Z}^+} A_n) \neq \phi$.*

2. Indecomposable *if for any two f-invariant closed subsets $A, B \subseteq X$ with $Int(A) \neq \phi$ and $Int(B) \neq \phi$ then $Int(A \cap B) \neq \phi$.*

3. Weakly Indecomposable *if there exists a residual subset $S \subseteq X$ such that for any two points $x, y \in S$, $w(x) = w(y) \neq \phi$.*

In [14], they used the theorem that states that f is transitive if and only if the only f-invariant closed subset that have nonempty interior is X itself. But, in the following example we will show that this statement is not true in general.

Example. 3.4. *Let $X = \{1, 2\}$, $\tau = \{\phi, X, \{2\}\}$ and define the function*

$$f : X \to X \text{ by } f(x) = 1.$$

The only closed proper subset it is the set $\{1\}$ and it is f-invariant, since $f(1) = 1$ but $int(\{1\}) = \phi$. So we conclude that the only f-invariant closed subset with nonempty interior is X itself.

On the other hand, f is not transitive. Take $U = V = \{2\}$ are nonempty open subset of X then $f^k(U) = \{2\}$, for all $k \in \mathbb{Z}^+$, so $f^k(U) \cap V = \phi$.

However, we found that the statement would be true if X is a compact perfect metric space and $f(X) = X$, and we clarified this in next theorem.

Theorem. 3.3.1. *Let $f : X \to X$ be a continuous map, where X is a compact perfect metric space and $f(X) = X$, then f is transitive if and only if the only f-invariant closed subset that have nonempty interior is X itself.*

Proof. From statement 1 and 3 in Theorem 3.1.4 the proof holds. □

Now, we consider the following Lemma.

Lemma. 3.3.1. *Let $f : X \to X$ be a continuous map where X is a compact perfect metric space, $f(X) = X$ and $\overline{R(f)} = X$. Then the following are equivalent:-*

1. *f is transitive.*
2. *f is strongly indecomposable.*
3. *f is indecomposable.*
4. *f is weakly indecomposable.*

Proof. 1 implies 2 implies 3

Suppose that f is transitive then by Theorem 3.1.5 the only f-invariant closed subset that have nonempty interior is X itself, so f is indecomposable and this implies that f is strongly indecomposable.

3 implies 1

Suppose that f is indecomposable and let A be a nonempty closed f-invariant set with nonempty interior, we will show that $A = X$.

Now, let U be a nonempty open subset in X and let $U' = \overline{\bigcup_{n\in\mathbb{Z}^+} f^n(U)}$, so U' is a nonempty closed f-invariant subset with nonempty interior.

$$\begin{aligned} f(U') &= f(\overline{\bigcup_{n\in\mathbb{Z}^+} f^n(U)}) \\ &\subseteq \overline{f(\bigcup_{n\in\mathbb{Z}^+} f^n(U))} \\ &\subseteq \overline{\bigcup_{n\in\mathbb{Z}^+} f^{n+1}(U)} \\ &\subseteq \overline{\bigcup_{n\in\mathbb{Z}^+} f^n(U)} = U' \end{aligned} \tag{1}$$

Also,

$$int(\overline{\bigcup_{n\in\mathbb{Z}^+} f^n(U)}) = \bigcup_{n\in\mathbb{Z}^+} f^n(U) \neq \phi$$

Now, f is indecomposable so we get

$$\begin{aligned} & int(U' \cap A) && \neq && \phi \\ then, \quad & int(U') \cap int(A) && \neq && \phi \\ and, \quad & \bigcup_{n \in \mathbb{Z}^+} f^n(U) \cap int(A) && \neq && \phi \\ so, \quad & f^n(U) \cap int(A) && \neq && \phi, \text{ for some } n \in \mathbb{Z}^+. \end{aligned} \tag{2}$$

This implies that, there exists an open set say U_1 in U such that $f^n(U_1) \subseteq int(A)$. But, the recurrent points are dense in U_1 since they are dense in X, also A is closed and f-invariant then $U_1 \subseteq A$.

Finally, we choose U arbitrary so we can take $U = X$ this means that $X \subseteq A$ implies that $X = A$.

4 implies 1

Let f be weakly indecomposable, i.e there exists a residual set S such that for every $x, y \in S, w(x) = w(y)$.

Now, we know by the assumption that the $R(f)$ is a dense G_δ-set and X is a Baire space then $S' = R(f) \cap S$ is a residual set. Let $x, y \in S', y$ is a recurrent point so by the definition of recurrent points $y \in w(y) = w(x)$, but $w(x) = \overline{w(x)}$ and $\overline{R(f)} = X$ so $w(x) = X$ and then f is transitive see [6].

1 implies 4

Let f be transitive, by Theorem 3.1.5 the Tr_f is nonempty dense set since X is Baire space, so Tr_f is a dense G_δ-set. So, let be the residual set $S = Tr_f$ then for all $x, y \in S, w(x) = X = w(y)$, this means that f is weakly indecomposable. □

After the above Lemma, we consider the following theorem.

Theorem. 3.3.2. *Let $f : X \to X$ be a continuous map where X is a compact perfect metric space and $f(X) = X$ and $\overline{R(f)} = X$. Then the following statements are equivalent*

1. *f is Devaney chaotic.*

2. *f is transitive and has a dense set of periodic points.*

3. *f is strongly indecomposable and has a dense set of periodic points.*

4. *f is indecomposable and has a dense set of periodic points.*

5. *f is weakly indecomposable and has a dense set of periodic points.*

Proof. $P(f) \subseteq R(f)$ then $\overline{P(f)} \subseteq \overline{R(f)}$. Now, if $\overline{P(f)} = X$, then $\overline{R(f)} = X$. So, the theorem follows from Lemma 3.3.1. □

4 Generalizations and Relaxations on Devaney's Chaos

In this section we present our main contribution in this thesis. First, we talk about the proposed generalization of Devaney's definition of chaos in metric spaces onto topological spaces. Then we present some suggested modifications on Devaney's definition conditions and consider their effect on chaos definition.

4.1 Chaos Space

V.Kumar on his PHD-Thesis in [18, Chapter 2] suggested a generalization of chaos in topological spaces, here we suggest some modifications on that generalization, and consider some results. Then we show the relation between it and other definitions of chaos.To generalize the DC-Definition of chaos in topological space. At first, we generalized the definition of sensitivity for topological spaces, since Devaney's chaos uses sensitivity definition in metric spaces. Then we give a generalization of DC-Definition by the TC-Definition as follow.

Definition. 4.1.1. *Let (X, τ) be a topological space and $f : X \to X$ be a continuous map. We say that f is **sensitive** at $x \in X$ if for any open set U containing x there exists $y \in U$ and an open set V such that $f^n(x) \in V$ but $f^n(y) \notin V$ for some $n \in \mathbb{Z}^+$, f is called sensitive if it is sensitive at every point in X.*

Next, we will consider some remarks on the sensitive functions.

Notes :

1. If f is sensitive at x then x is not an isolated point.
   By the definition of sensitive function, for any open set U containing x, there exists $y \in U$. So x is not an isolated point.

2. There are no sensitive functions in discrete spaces.
   For discrete spaces, $\{x\}$ is an open set $y \notin \{x\}$ if $y \neq x$.

3. Every function is sensitive in indiscrete spaces.
   For indiscrete space the only open sets are X and $\emptyset$.

Definition. 4.1.2. *Let (X, τ) be a topological space and $f : X \to X$ be a continuous map. Then f is chaotic on X if*

(i) $\overline{O_f(x)} = X$, *for some* $x \in X$.

(ii) Periodic points of f *are dense in* X.

(iii) f *is sensitive on* X.

We denoted this definition by TC-Definition of chaos, and the Devaney's Definition of chaos by DC-Definition.

Proposition. 4.1.1. *Let* $f : X \to X$ *be a continuous map such that* f^n *is nonconstant in every open set* U *for some* $n \in \mathbb{Z}^+$ *and suppose that* X *is* T_2 *and perfect then* f *is sensitive.*

Proof. Let $x \in X$ and U be any open set containing x. This implies that there exists $y \in U$ such that $x \neq y$. (Since X is perfect so it has no isolated points).

Now, f^n a nonconstant for some $n \in \mathbb{Z}^+$, $f^n(x) \neq f^n(y)$ for some $n \in \mathbb{Z}^+$. Suppose not, i.e $f^n(x) = f^n(y)$, for all $y \in U$ this implies that f^n is constant on the set U, which contradicts the assumption.

Since X is a T_2 space and $f^n(x) \neq f^n(y)$. Then there exists disjoint open sets V,Z such that $f^n(x) \in V$ and $f^n(y) \in Z$, but $f^n(y) \notin V$. So f is sensitive. □

4.1.1 Relation between TC-Definition and DC-Definition

In this section we talk about the realtion between the TC-Definition and the DC-Definition.

Proposition. 4.1.2. *If* U *is a finite nowhere dense set, then it does not have a finite dense subset.*

Proof. Note that A is nowhere dense means that if its closure contains no open sets as subsets.

Now, suppose that every finite set is nowhere dense, and let U be a nonempty open subset of X then (by definition of nowhere dense) U has no finite dense subset. □

Proposition. 4.1.3. *TC-Definition implies DC-Definition*

Proof. Suppose TC-Definition holds. We first prove that f is topologically transitive.

Now, since f is sensitive at x, for every $x \in X$ then X has no isolated points. So every finite set is nowhere dense. This means that no nonempty open subset U has a finite subset that dense in U.

Since, $\overline{O(x)} = X$ for some $x \in X$ and no nonempty open subset U of X has a finite dense subset in U. So, by Proposition 3.1.1 we conclude that f is topologically transitive.

Given that the set of periodic points are dense in X and we showed that f is topologically transitive. So, f is chaotic in the sense of Devaney. □

Proposition. 4.1.4. *If X is a compact metric space then the DC-Definition implies the TC-Definition.*

Proof. Suppose DC-Definition holds.

X is a compact metric space then X is complete space and has a countable base. Also, f is topologically transitive. So, by Proposition 3.1.1 $\overline{O(x)} = X$ for some $x \in X$, and the first condition holds.

The second condition also holds from the hypothesis.

It remains to show that f is sensitive on X. To do this, suppose that f has sensitive dependence on initial conditions.

So, there exists $\delta > 0$ such that for all $x \in X$ and for every neighborhood N of x, there exists $y \in N$ and $n \in \mathbb{Z}^+$ such that $d(f^n(x), f^n(y)) > \delta$.

Let $x \in X$, U be any open set containing x and $V = B_\delta(x)$ for some $\delta > 0$, then there exists $y \in U$ such that

$$f^n(x) \in V = B_\delta(x) \qquad \text{but } f^n(y) \notin B_\delta(x)$$

So, f is sensitive. □

Banks et al. [4, Theorem 1] proved that conditions (1) and (2) imply (3) and Vellekoop and Berglund [27] showed that on intervals (1) implies (2) and (3). But in TC-Definition there is no redundancies, see the following examples.

Example. 4.1. *1.* $\boxed{(i) \text{ and } (ii) \text{ do not imply } (iii)}$

Let $X = \{1, 2\}$, and let $\tau = \{X, \{1\}, \phi\}$, and define the map $f(2) = 1$, $f(1) = 2$.

Notice that, $\overline{O(1)} = \overline{O(2)} = X$ so the first condition holds and the set of periodic points $\{1, 2\}$ is dense in X.

But f is not sensitive on X, take $1 \in X$ where $\{1\}$ is an open set containing 1, but there is no point which differs from 1 in the open set $\{1\}$.

2. $\boxed{(ii) \text{ and } (iii) \text{ do not imply } (i)}$

Let $f : \mathbb{R} \to \mathbb{R}$ be a map defined by $f(x) = x$ and let τ be the usual topology on $\mathbb{R}$.

   (a) *$\overline{O(x)} = x$, for every $x \in \mathbb{R}$ then does not exists $x \in \mathbb{R}$ such that $\overline{O(x)} = \mathbb{R}$.*

   (b) *For all $x \in X, x$ is a periodic point so the set of periodic points is dense in $\mathbb{R}$.*

   (c) *f is sensitive. Take $x \in \mathbb{R}$ and U be any open set containing x, and take $V = B_\epsilon(x)$ so let $y \neq x \in U$ and choose $\epsilon = d(x, y)/2$. This implies that $f(x) = x \in V$ but $f(y) = y \notin V$.*

3. $\boxed{(i) \text{ and } (iii) \text{ do not imply } (ii)}$ *Let*

$$f(x) = \begin{cases} \frac{3x}{2}, & 0 \leq x < \frac{1}{2} \\ \frac{3(1-x)}{2}, & \frac{1}{2} \leq x \leq \frac{3}{4} \end{cases}$$

Since $|f'(x)| = \frac{3}{2}$,for all $x \in [0, \frac{3}{4}]$ then f is sensitive. However, the interval $(0, \frac{3}{8})$ has no periodic points because if we take any initial point in the interval $(0, \frac{3}{8})$ then the trajectory will not reurn there as shown in Figure 2.

Moreover, f is topologically transitive so by Theorem 3.1.4 in previous section f has a dense orbit.

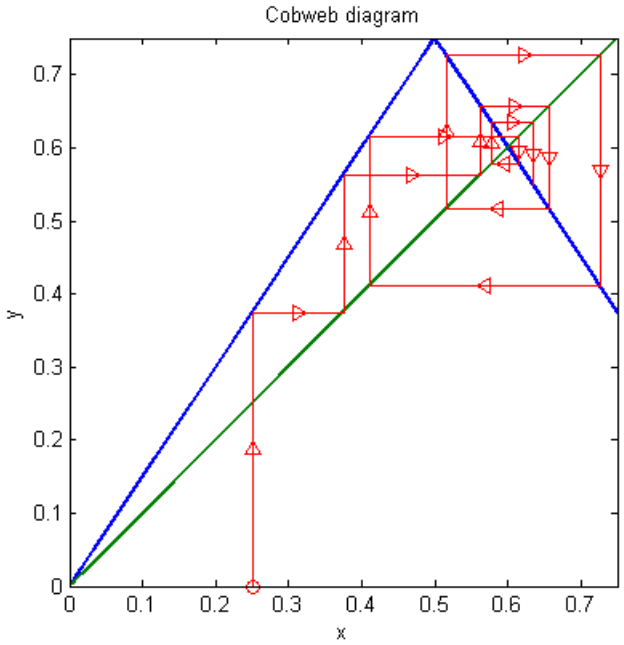


Figure 2: Cobweb diagram of Example 2.1 (3)

Proposition. 4.1.5. *Suppose that X and Y are isomorphic by the map $h : X \to Y$ then if X is chaotic in the sense of TC-Definition then Y is also chaotic in the sense of TC-Definition.*

Proof. Suppose that X is chaotic and let $h : X \to Y$ be the isomorphic map, we want to show that Y is chaotic.

let $g = hofoh^{-1}$, we will prove the following

(i) $\overline{O_g(y)} = Y$, for some $y \in Y$.

(ii) The set of periodic points of g is dense in Y.

(iii) g is sensitive on Y.

(i) Suppose $\overline{O_g(y)} \neq Y$, for all $y \in Y$. But h is onto map so there exists $x \in X$ such that $h(x) = y$. This implies that $\overline{O_g(h(x))} \neq Y$, for all $x \in X$. This means that, there exists an open set V in Y such that $\overline{O_g(h(x))} \cap V = \phi$.

Notice that

$$\begin{aligned} g^n(h(x)) &= (h \circ f \circ h^{-1}(h(x)))^n \\ &= h \circ f \circ h^{-1} \circ h \circ f \circ h^{-1} \ldots (n - times) \\ &= h \circ f^n \circ h^{-1}(h(x)) \\ &= h \circ f^n(x) \end{aligned}$$

So, $g^n(h(x)) \notin V$, for all $n \in \mathbb{Z}^+$ and then $h \circ f^n(x) \notin V$, which implies that $f^n(x) \notin h^{-1}(V)$ (Since h is one to one map), and this is true for all $x \in X$.

But $h^{-1}(V)$ is an open set in X and $\overline{O_f(x)} = X$, for some $x \in X$, and this is a contradiction so $\overline{O_g(y)} = Y$, for some $y \in Y$.

(ii) Notice that x is a periodic point of f of order n if and only if $y = h(x)$ is a periodic point of g of order n.

Suppose x is a periodic point of f of order n i.e $f^n(x) = x$. Now,

$$\begin{aligned} g^n(h(x)) &= h \circ f^n \circ h^{-1}(h(x)) \\ &= h \circ f^n(x) \\ &= h(x) \end{aligned}$$

On the other hand, if $h(x)$ is a periodic point of g of order n, this means that $g^n(h(x)) = h(x)$

$$\begin{aligned} h \circ f^n(x) &= h(x) \\ then, \quad f^n(x) &= x \end{aligned}$$

Assume that the set of periodic points of g is not dense in Y. Then, there exists an open set V in Y such that $\mathrm{P}(g) \cap V = \phi$.

and, $y \notin V$, for all y periodic points of g.

also, $h(x) \notin V$, for all x periodic points of f.

and, $x \notin h^{-1}(V)$, for all x periodic points of f.

But the periodic points of f are dense in X and $h^{-1}(V)$ is an open set in X, and this is a contradiction, so we conclude that $\overline{P(g)} = Y$

(iii) We will show that g is sensitive. Let $y_1 \in Y$, then there exists $x_1 \in X$ such that $y_1 = h(x_1)$. Let V be any open set containing y_1.

Note that $h^{-1}(V)$ is an open set containing x_1. And we know that f is sensitive in X, so there exists $x_2 \in h^{-1}(V)$and there exists an open set U such that $f^n(x_1) \in U$ but $f^n(x_2) \notin U$, for some $n \in \mathbb{Z}^+$. Notice that:

1. If $f^n(x_1) \in U$. This implies that $h \circ f^n(x_1) \in h(U)$
   So, this implies that $g^n(y_1) \in h(U)$
2. If $f^n(x_2) \notin U$. Then, $h \circ f^n(x_2) \notin h(U)$

This implies that $g^n(y_2) \notin h(U)$, where $y_2 = h(x_2)$. So, for all $y_1 \in Y$ and for any open set V containing y_1, there exists $y_2 \in V$ such that $g^n(y_1) \in V$ but $g^n(y_2) \notin V$, and then g is sensitive in Y. □

4.1.2 Other Definitions of Chaos

In this section we give more two definitions of chaos, Auslander and Yorke definition and expansive chaos.

Definition. 4.1.3. *Let $\epsilon > 0$. A map f on a set X is called Lyapunove ϵ-unstable at a point $x \in X$ if for every neighborhood U of x there is a point $y \in U$ and $n \geq 0$ such that $d(f^n(x), f^n(y)) > \epsilon$.*

We denote this definition by D-AYC.

Definition. 4.1.4. *The map f is chaotic in the sense of Auslander and Yorke if:*

(i) f is surjective.

(ii) f is unstable in the sense of Lyapunov.

(iii) X contains a dense orbit.

In [18, Definition 2.2.4] give us a definition of unstability in a topological space as follow.

Definition. 4.1.5. *[18, Definition 2.2.4] Let (X, τ) be a topological space and $f : X \to X$ be a continuous map. We say that f is **stable** at x if given any neighborhood U of x there is a neighborhood V of x such that, $f^n(V) \subseteq U$, for all $n > 0$.*

f is called **unstable** at x if there exists a neighborhood U of x such that for any neighborhood V of x, $f^n(V) \nsubseteq U$ for some $n > 0$.

Now, we give a generalization of Auslander-Yorke in topological spaces in [18, Definition 2.2.5].

Definition. 4.1.6. *[18, Definition 2.2.5] Let (X, τ) be a topological space and let $f : X \to X$ be a surjective continuous map. We say that f is chaotic in the sense of Auslander-Yorke on X if:*

(i) $\overline{O(x)} = X$, for some $x \in X$.

(ii) f is unstable at x, for all $x \in X$.

Denote it by τ-AYC.

The following proposition gives the relation between definition of unsatbility in metric space and topological space as.

Proposition. 4.1.6. *If f is unstable in the sense of Definition 4.1.3, then f is unstable in the sense of Definition 4.1.5.*

Proof. Let $x \in X$, so there exists $U = B_\epsilon(f^n(x))$ where $\epsilon > 0$. Let V be any neighborhood of x, there exists $y \in V$ such that $d(f^n(x), f^n(y)) > \epsilon$, for some $n \geq 0$.

$$\begin{array}{lrcl} \textit{then}, & f^n(y) & \notin & B_\epsilon(f^n(x)) = U \\ \textit{and}, & f^n(V) & \nsubseteq & U, \text{ for some } n \geq 0 \end{array}$$

So we conclude by the previous proposition that D-AYC definition of chaos implies τ-AYC definition of chaos. □

Relation between TC-definition and τ-AYC definition of chaos

Proposition. 4.1.7. *TC-definition implies τ-AYC definition.*

Proof. Suppose the TC-definition holds. Since if f is sensitive then for any neighborhood V of x, there exists $y \in V$ and an open set U with $f^n(x) \in U$ and $f^n(y) \notin V$ for some $n \geq 0$. Which implies that

$$f^n(V) \nsubseteq U \text{ for some } n \geq 0$$

We conclude that f is stable and so f is chaotic in the sense of τ-AYC definition. □

Now, we consider the definition of expansive functions and then mention the definition of expansive chaos as in [18, Definition2.2.9]. Finally, we give some results related to these definitions.

Definition. 4.1.7. *Let (X, d) be a metric space and $f : X \to X$ be a continuous map. Then f is **expansive** on X if there exists $\delta > 0$ such that for every $x, y \in X$ with $x \neq y$, $d(f^n(x), f^n(y)) \geq \delta$, for some $n \in \mathbb{Z}^+$.*

Definition. 4.1.8. *Let (X, d) be a metric space and $f : X \to X$ be a continuous map. Then f is expansively chaotic if*

1. *f is transitive.*
2. *The set of periodic points are dense in X.*
3. *f is expansive.*

We denote this definition by EC-Definition.

Consider the following remarks.

Remark.. 1. if f is an expansive function then it is sensitive.

This is clear from the definitions.

But the converse is not true in general. Consider the following example.

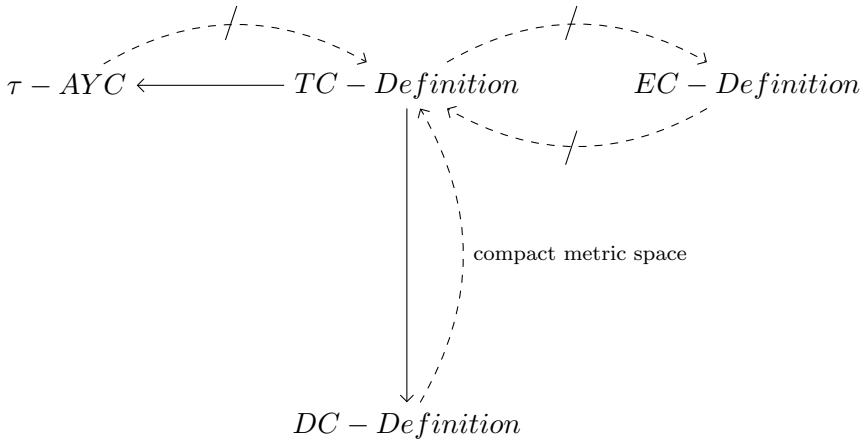
Example. 4.2.

$$f(x) = \begin{cases} 2x & 0 \leq x < \frac{1}{2} \\ 4x - 1 & \frac{1}{2} \leq x \leq \frac{3}{4} \end{cases}$$

$f'(x) = 2$, for all $x \in (0, \frac{1}{2})$, and $f'(x) = 4$, for all $x \in (\frac{1}{2}, \frac{3}{4})$ so f is expanding and then it is sensitive. However, the expanding of f in the interval $[\frac{1}{2}, \frac{3}{4}]$ is more rapid than the expand in the interval $(0, \frac{1}{2})$, so we can't find δ as in the definition of expansive function. This means that f is not expansive.

2. The TC-Definition does not imply the EC-Definition.
   The tent map is chaotic in the sense of TC-Definition but it is not chaotic in the sense of EC-Definition since f is not expansive.

3. The EC-Definition does not imply the TC-Definition.
   This does not hold since the UV-transitivity does not imply the OX-transitivity. So according to Proposition 3.1.1 this holds if X is a complete metric space with a countable base.



4.2 New Proposed Definition of Chaos

In this section we propose some modifications on Devaney's definition of chaos and then show some related results as follow.

Definition. 4.2.1. *Let X be a metric space with metric d, and let $f : X \to X$ be a continuous map. We say that f has a* ***weakly sensitive dependence on initial conditions*** *if there is a positive real number δ, such that for every point $x \in X$ and every neighborhood N of x there exists a point $y \in N$ and nonnegative integers n, m such that*

$$d(f^n(x), f^m(y)) > \delta.$$

Definition. 4.2.2. *Let X be a Topological space, and let $f : X \to X$ be a continuous map. f is called* ***weakly transitive*** *if for every nonempty open subsets U and V of X, there exists a natural number k such that $f^k(U) \cap V \neq \phi$ or $U \cap f^k(V) \neq \phi$.*

Remark.. If f has sensitive dependence on initial conditions then f has a weakly sensitive dependence on initial conditions, but the converse is not true in general. Consider the following example.

Example. 4.3. *Take $f(x) = \frac{1}{2}x - 1$, where $x \in [0, 1]$. And define the usual metric space $d(x, y) = |x - y|$. $|f'(x)| = \frac{1}{2} < 1$, so according to Proposition 2.1.1, f does not have a sensitive dependence on initial conditions.*

However, take $x \in [0, 1]$, and let $\delta > 0$ such that $|x - y| < \delta$ where $y \in [0, 1]$ and take $\epsilon = \frac{1}{4}[1 - \delta] > 0$, so there exists $n = 1, m = 2$ such that $|f(x) - f^2(y)| > \epsilon$.

$$\begin{aligned}
|f(x) - f^2(y)| &= |\frac{1}{2}x - 1 - \frac{1}{4}y + \frac{3}{2}| \\
&= |\frac{1}{2}x - \frac{1}{4}y + \frac{1}{2}| \\
&\geq \frac{1}{2} - \frac{1}{4}|2x - y| \\
&= \frac{1}{2} - \frac{1}{4}|x + x - y| \\
&\geq \frac{1}{2} - \frac{1}{4}|x| - \frac{1}{4}|x - y| \\
&\geq \frac{1}{2} - \frac{1}{4} - \frac{1}{4}\delta \\
&= \frac{1}{4} - \frac{1}{4}\delta \\
&= \frac{1}{4}[1 - \delta] = \epsilon.
\end{aligned}$$

So we conclude that f has weakly sensitive dependence on initial conditions.

Remark.. It is clear that if f is UV-transitive then f is weakly transitive. The converse is true if X is a compact perfect metric space and $f(X) = X$.

Lemma. 4.2.1. *Let $f : X \to X$ be a continuous map where X is a compact perfect metric space and $f(X) = X$. Then f is transitive if and only if f is weakly transitive.*

Proof. If f is transitive then f is clearly weakly transitive.
For the converse, by Theorem 3.1.4 , the following two statements are equivalent.
For every nonempty open subsets U and V, there exists $k \in \mathbb{Z}^+$ such that

$$f^k(U) \cap V \neq \phi.$$

For every nonempty open subsets U, V, there exists $k \in \mathbb{Z}^+$ such that

$$f^{-k}(U) \cap V \neq \phi.$$

Now, $f^{-k}(U) \cap V \neq \phi$ if and only if $f^k(f^{-k}(U) \cap V) \neq \phi$
This means that

$$\phi \neq f^k(f^{-k}(U) \cap V) \subseteq f^k(f^{-k}(U)) \cap f^k(V)) \subseteq U \cap f^k(V).$$

We conclude that, $U \cap f^k(V) \neq \phi$ if and only if $f^k(U) \cap V \neq \phi$

□

Remark.. In [4, Theorem 1], Banks et al. proved that if f is transitive and has a dense set of periodic points then f has sensitive dependence on initial conditions. Also, if f is weakly transitive and has a dense set of periodic points then f has a sensitive dependence on initial conditions as it is given in the next theorem:

Theorem. 4.2.1. *Let X be a metric space and let $f : X \to X$ be a continuous map. If f is weakly transitive and the periodic points are dense in X then f has a weakly sensitive dependence on initial conditions.*

Proof. Notice that there exists $\delta_0 > 0$ such that we can find two periodic points p_1 and p_2 where their orbits are disjoint with distance more than δ_0. Let t, s be any positive numbers such that:

$$d(f^t(p_1), x) + d(f^s(p_2), x) \geq d(f^t(p_1), f^s(p_2)) \geq \delta_0$$

If $d(f^t(p_1), x) \leq \dfrac{\delta_0}{2}$ then $d(f^s(p_2), x) \geq \dfrac{\delta_0}{2}$ and the other way around.

So there exists a periodic point say p_3 such that the distance between the orbit of p_3 and any point $x \in X$ is at least $\dfrac{\delta_0}{2}$.

$$d(x, f^t(p_3)) \geq \frac{\delta_0}{2}, \quad \text{for all } t \in \mathbb{Z}^+$$

Now, suppose $\delta = \dfrac{\delta_0}{8}$ be the sensitivity constant and let $x \in X$ and N be any neighborhood of X. Suppose $V = N \cap B_\delta(x)$ where $B_\delta(x) = \{y \in X \mid d(y, x) < \delta\}$.

So V is a nonempty open set since it is intersection of two open sets and there exists $p \in V$ where p is a periodic point of order n. Set

$$U = \bigcap_{i=0}^{n} f^{-i}(B_\delta(f^i(p_3)))$$

So U is nonempty open set since it is the intersection of open sets and $p_3 \in U$. But f is transitive so for any two nonempty open set U and V there exist $y \in V$ such that $f^k(y) \in U$ where k is a nonnegative integer.
Now, Let $m \in \mathbb{Z}^+$ such that $\dfrac{1}{n} + \dfrac{k}{n} \leq m \leq 1 + \dfrac{k}{n}$. Then $1 \leq mn - k \leq n$ and $f^{mn}(p) = p$. Also,

$f^{mn}(y) = f^{mn-k}(f^k(y)) \ \in f^{mn-k}(U) \subseteq B_\delta(f^{mn-k}(p_3))$

This implies that

$$d(x, f^{mn-k}(p_3)) \leq d(x,p) + d(p, f^{mn}(y)) + d(f^{mn}(y), f^{mn-k}(p_3))$$

Notice that:

1. $d(x,p) < \delta, \qquad$ since $p \in B_\delta(x)$ and $p \in U$.
2. $d(f^{mn}(y), f^{mn-k}(p_3)) \leq \delta, \quad since f^{mn}(y) \in B_\delta(f^{mn-k}(p_3))$
3. $d(x, f^{mn-k}(p_3)) \leq \dfrac{\delta_0}{2} = 4\delta$

It follows that

$$4\delta \leq d(p, f^{mn}(y)) + 2\delta \Longrightarrow d(p, f^{mn}(y)) > 2\delta$$

This means that

$$2\delta < d(p, f^{mn}(y)) < d(p, f^{mn}(x)) + d(f^{mn}(x), f^{mn}(y))$$

Then, $\ d(p, f^{mn}(x)) + d(f^{mn}(x), f^{mn}(y)) > 2\delta$

So $\qquad d(p, f^{mn}(x)) > \delta$ or $d(f^{mn}(x), f^{mn}(y)) > \delta$

In either of these cases we find a point p and y in N such that $d(p, f^{mn}(x)) > \delta$ or $d(f^{mn}(x), f^{mn}(y)) > \delta$ so f has a weakly sensitive dependence on initial conditions.

□

Remark.. In [27], it has been proved that on an interval if f is transitive then f is Devaney chaotic.

Now, if we suppose that X is a connected metric space with dimension 1 the theorem does not hold. See this example.

Example. 4.4. *Let $X = S^1/\{e^{i2\pi p/q} | p, q \in \mathbb{Z}, q \neq 0\}$ equipped with the usual arc length metric.*

Firstly, S^1 is a connected metric space. Consider the map $h : [0, 2\pi] \to \mathbb{R}^2$ where $h(x) = (\cos x, \sin x)$, since f is continuous map and $[0, 2\pi]$ is connected, the image is the unit circle which is connected.

On the other hand, S^1 has no cut points, so the set $S^1/\{e^{i2\pi p/q}|p,q \in \mathbb{Z}, q \neq 0\}$ is also connected. Also, the dimension of the set X is 1.

Now, in [2, Example 1] it has been proved that f is transitive, but the set of periodic points are not dense. This means that f is not chaotic in the sense of Devaney.

We generalize Lemma 2.1.1 as follows.

Lemma. 4.2.2. *Let $f : X \to X$ be a continuous map where X is a totally ordered connected metric space with dimension 1. If U is a subset of X which contains no periodic points of f and $z, f^m(z)$ and $f^n(z) \in U$ with $0 < m < n$, then either $z < f^m(z) < f^n(z)$ or $z > f^m(z) > f^n(z)$.*

Proof. Suppose not, i.e there exists $z \in U$ such that $z < f^m(z)$ and $f^m(z) > f^n(z)$ where $0 < m < n$, where U is a subset that has no periodic points of f.

Consider the function $h(x) = f^m(x)$ this means that $z < h(z)$ and we claim that $z < h(z) < h^{r+1}(z)$ for all $r \in \mathbb{Z}^+$ and then the assumption is not true, so the proof holds. We prove the claim above by induction, assume $z < h(z) < h^r(z)$ to show that $z < h(z) < h^{r+1}(z)$, suppose it is not true i.e $h(z) > h^{r+1}(z)$ for some $r \in \mathbb{Z}^+$, let $g(x) = h^r(x) - x$ on the interval $[z, h(z)]$ then by induction hypothesis $g(z) = h^r(z) - z > 0$ and

$$\begin{aligned} g(h(z)) &= h^r(h(z)) - h(z) \\ &= h^{r+1}(z) - h(z) < 0 \end{aligned}$$

Now, since X is totally ordered connected metric space so we can generalize the Intermediate Value Theorem and then there exists $c \in (z, h(z))$ such that $g(c) = 0$ so $h^r(z) = z$ and then $f^{rm}(z) = z$ is a periodic point in U.

On the other hand let $r = n - m > 0$ then $z < h^{(n-m)m}(z) < f^m(z)$ since $f^{n-m}(f^m(z)) < f^m(z)$.

Now, consider the function $k(x) = f^{(n-m)m}(x) - x$ on the interval $[z, f^m(z)]$ then $k(z) > 0$ and $k(f^m(z)) < 0$. Again by the Intermediate Value Theorem there exists $t \in (z, f^m(z))$ such that $f^{(n-m)m}(t) = t$, this means that there is a periodic point t in U which contradicts the assumption. □

Then, we consider the generalization of Theorem 2.1.2 as follows.

Proposition. 4.2.1. *Let $f : X \to X$ be a continuous map where X is a totally ordered connected metric space with dimension 1. If f is transitive then the set of periodic points of f is dense and f has a sensitive dependence on initial condition.*

Proof. Suppose that f is transitive. So by the results in Theorem 2.1.1 it suffices to show that the periodic points are dense in X.

Assume not, there exists open set $U \subseteq X$ such that U has no periodic points. Let $x \in U$.

Let N be an open neighborhood of x such that $N \subset U$ and let E be an open set in U/N. Since f is transitive, so for any two nonempty sets U and E, there exists $y \in U$ such that $f^m(y) \in E$, where m is a nonnegative integer. Since U has no periodic points so $y \neq f^m(y)$.

Let $\epsilon = d(y, f^m(y))$ and let $U' = \{x | d(x, y) < \epsilon/3\}$ be a neighborhood of y, $V = \{z | d(z, f^m(y)) < \epsilon/3\}$ be a neighborhood of $f^m(y)$ then $U' \bigcap V = \phi$. Now, f is continuous then f^m is also continuous and so for any neighborhood V of $f^m(y)$ in I there exists a neighborhood U of y in I such that $f^m(U) \subseteq V$. Consider two cases

Case 1: If $U \subseteq U'$.

Then $U \bigcap f^m(U) = \phi$. Again, f is transitive, so there exists $z \in U$ such that $f^n(z) \in U$, where $n > m$. Finally, there exists $0 < m < n$ and $z, f^n(z) \in U$, but $f^m(z) \notin U$, so this contradicts the lemma.

Case 2: If $U' \subseteq U$.

Then $U' \bigcap f^m(U) = \phi$. Again, f is transitive, so there exists $z \in U'$ such that $f^n(z) \in U'$, where $n > m$. Finally, there exists $0 < m < n$ and $z, f^n(z) \in U'$, but since $z \in U$ so $f^m(z) \in f^m(U)$ and $U' \bigcap f^m(U) = \phi$ so $f^m(z) \notin U'$, and this contradicts Lemma 4.2.2. □

We propose the following definition of chaos.

Definition. 4.2.3. *Let X be a metric space, $f : X \to X$ be a continuous map, we say f is chaotic on X if:*

1. *f is weakly transitive.*

2. *The set of periodic points is dense.*

3. *f is weakly sensitive.*

In our paper [16] we present and discuss this new definition of chaos.

5 Building Hash Functions Using Chaotic Functions

5.1 Basics

Hashing has been a very significant field in computer science for the last few decades. Hash functions were generally developed to compress an input string into a shorter one. Hashing gained extensive interest of its application in computer security systems. In this section we review the basic concepts behind hash functions, their applications and construction [19], [25].

5.1.1 Definition of a Hash Function

A hash function H is an algorithm that translates a variable-length message M into a fixed-length hash value $h = H(M)$. Mathematically, $H : M \rightarrow Y$, where H is a map from the message M to the hash value Y. Figure 3 shows how a hash function is applied to an input message. For every input message a hash value of size 3-digits is computed. One interesting property of a hash function is its sensitivity to slight changes in input messages. In figure 3, the change of the capital letter 'A' in the first message to small case 'a' in the second message led to a significant change in the computed hash value [25].

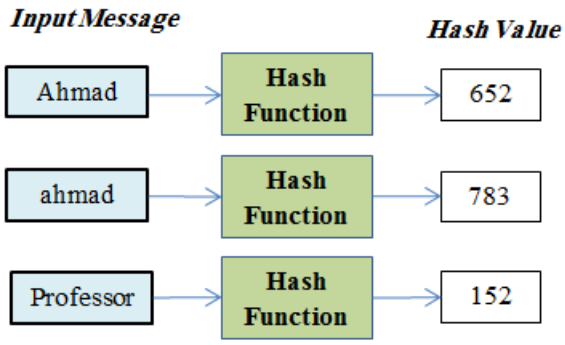


Figure 3: Example of hash function

Hash functions have a wide range of applications, two main categories: Security applications and Non-Security applications. Non-Security applications include building hash tables for database indexing, error detection,

and Identity generation. Security applications include message authentication, digital signature generation, data verification, and data encryption in security systems. In this section we consider hash functions for security applications, and more specifically, a type of hash functions used in data security systems which is referred to as cryptographic hash function.

The majority of cryptographic hashing algorithms partition a message into blocks of n-bits, then each block is manipulated bit by bit using bitwise operations. Figure 4 depicts a simple example of a cryptographic hash function. The message is partitioned into 16-bit blocks and the algorithm uses a 16-bit secret key. The algorithm normally starts from an initial hash value and iteratively applies the exclusive OR (XOR) function on the three inputs: message block M_i, secret key K, and intermediate hash value h_i. The XOR function is a bitwise function takes as input a sequence of binary digits, if the number of digits equal '1' are odd it returns '1', otherwise it returns '0'. For example, XOR("001011") = 1, and XOR("000011") = 0. After processing all the message blocks, a 16-bit hash value is generated. It is obvious that a hash function is a many-to-one function, i.e. there are multiple messages M that produce the same hash value h. Before looking at

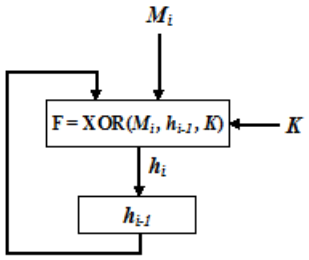


Figure 4: A simple example of a hash function

some properties of hash functions, let us consider the following definitions.

Definition. 5.1.1. *A function $f : \{0,1\} \to \{0,1\}$ is **one-way** if f can be computed by a polynomial time algorithm, but for every randomized algorithm A that runs in time polynomial in n, every polynomial $p(n)$, and all sufficiently large n*

$$Pr[f(A(f(x))) = f(x)] < \frac{1}{p(n)}$$

*Where the probability is over the choice of x from the uniform distribution on $\{0,1\}$, and the randomness of A. Informally, a **one-way function** is a*

function that is easy to compute on every input, but hard to invert given the image of a random input.

Definition. 5.1.2. *Suppose the random variable X can assume k different values. Suppose also that the $P(X = x_k)$ is constant. Such that,*

$$P(X = x_k) = 1/k$$

Then X is said to be uniformly distriputed.

The perfect cryptographic hash function must fulfill the following main properties:

a The computation of the hash value is simple and easy to apply for any given message.

b Applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random.

c A cryptographic hash function should be sensitive to any tiny variation in the message. A change to any bit or bits in the message results, with high probability, in a significant change to the hash code.

d A cryptographic hash function is a one-way function. In other words, given a hash value it is infeasible to generate the source message.

e It is extremely difficult to find two different messages that have the same hash value.

5.1.2 Applications and Security Requirements

Cryptographic hash functions have a wide range of applications especially in networks security and Internet protocols. To understand the requirements of cryptographic hash functions and their security implications, we take a look at few of its applications.

1. **Message Authentication**

   Message authentication is a service that assures the integrity of a message traveling between two ends; a sender and a receiver. The purpose of message authentication is to detect any modification on the message mainly by an attacker.

Figure 5 describes how a hash function can be used for message authentication. For example, Alice sends a message M to Bob and Bob wants to be sure that the received message is from Alice and not from a third party. Alice and Bob will share a secret K, Alice will compute the hash value of the message using the secret key, and send both the message and the hash value to Bob. Bob will use the secret key to re-compute the hash value of the received message, and compare it to the received hash value if they are the same then the message is authentic and generated by Alice, otherwise the message will not be authentic. A third party who intercepts the message and the hash value cannot change the message and the hash value without any knowledge of the secret key and the hash function H.

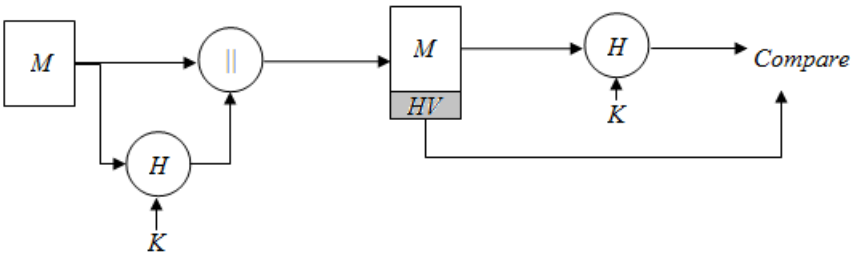


Figure 5: An example of using hash function H for message M authentication

Commonly, the above method is known as Message Authentication Code (MAC) or keyed hash function. If a secret key is not to be used, some kind of secrecy around the hash function is necessary [25].

2. **Password Verification**

Another important application of hash functions is password verification. A hash function is used to create a password file that stores only the hash value of each password. The password file is kept safe on the server. Now instead of sending the password over the network link, the hash value of the password is computed and sent to the server, which compares it with the hash value stored in the password file to verify the password correctness.

3. **Security Requirements**

For a cryptographic hash function to be useful in a security system it must satisfy few security requirements. Before proceeding in the security requirements of cryptographic hash functions we first define few terms.

Pre-image. For a hash value $h = H(x)$, we call x the pre-image of h. In other words, a pre-image x is the original data block whose hash value is h, computed using the function H. A hash function H is a many-to-one mapping, as so, for any given hash value h, there will be multiple pre-images. A collision happens if we have two non-equal pre-images x, y and $H(x) = H(y)$. Collisions are undesirable phenomena in cryptographic hash functions. An attacker is a person (or program) that tries to break the hash function. Several types of attacks can be conducted by an attacker:

. Given the message x, the attacker tries to find a message $y \neq x$ with the same hash value h. This attack is known as second pre-image attack.

. Given a hash value h, the attacker can find a message x that produces the hash value h. This attack is known as pre-image attack.

. For a given cryptographic hash function H, the attacker tries to find two messages; x, and y, where $x \neq y$ and $H(x) = H(y)$. A well known attack of this kind is the birthday attack.

A concern can arises when designing a cryptographic hash function is that how we make it impossible or at least too difficult for the attacker who wants to break the hash function. To ensure security, a secure hash function must satisfy the following conditions:

(a) High Sensitivity to tiny variations in the message bits. A sensitive function to initial values (i.e. initial message) will produce significantly different results for very small changes in the initial value.

(b) Pre-image resistance: For a hash value h, it must be infeasible to find any message m with the hash value $h = H(m)$. This condition is a result of the one-way property of the hash function. Functions that do not fulfill this property are weak against pre-image attacks.

(c) Second pre-image resistance. For a message x it is too difficult to find a message $y \neq x$ such that $H(x) = H(y)$. Functions that miss this property are vulnerable to second pre-image attacks. This property is related to the randomness and sensitivity of the hash function.

(d) Collision Resistance. A collision occur if two messages x, and y are found to have the same hash value. Such a pair of messages is known as cryptographic hash collision.

The Sensitivity property is needed to elude an attacker who tries to find two messages with the same hash value. A hash function that maps two messages x and $x + \delta$ into the hash values h, and $h + \delta$ respectively, where δ is the amount of variation in the message bits, and h is n-bit hash value, is more likely to be broken by an attacker, because it simplifies the search process for message $y \neq x$ while both has the same hash value h. On the other hand, if changing one or two bits in the message bits produces significant changes in the hash value, the search space expands to 2^n. and for large n, e.g. 64 or larger, it becomes too expensive and hard to test each message in the search space.

5.1.3 Construction of Hash Functions

A hash function operates on arbitrary length message and produces a fixed length n. To do so, we have to partition the input message into a set of blocks of fixed length r, then we apply a one-way compression function sequentially on each message block. The length of the message does not need to be divisible by r. Thus some message preprocessing and padding is needed. This type of hash functions is called iterated functions, and most of the widely used cryptographic hash functions are built using iterated functions. Figure 6 depicts the structure of a hash function. One can summarize the hashing steps as follows:

a. Message Preprocessing: Given an arbitrary length message M of length l; the message is padded and extended to length $(l + p)$ where $(l + p)\ mod\ r = 0$; i.e. the extended message M' length is multiple of r. Then the message is broken into a sequence of blocks $m_i : i = 1, , N$ each of length r.

b. An additional block represents the original message length l is added to the extended message M'.

c. After finishing the message preprocessing: a compression function f is applied iteratively on the sequence of message blocks starting from an initial value (IV) for the hash value. The of the compression function at each step is used as input, in addition to a message block, to the subsequent function iteration. The of the final function iteration is considered the final hash value.

d. The final hash value might be processed further by a transfer function G, to produce a new hash value with better shape.

$$\begin{aligned} h_0 &= IV \\ h_i &= f(m_i, h_{i-1}, K), \quad i = 1, \ldots N+1 \end{aligned}$$

The of the hash function H is the last value h_{N+1}. The secret key K in the hash function can be used as initial value for h_0, or as input to the compression function f.

This kind of construction using iterated functions is also called Merkle-Damgrad construction. Merkle and Damgrad proved independently, that if a collision resistant compression function f is used, then the above construction of hash function $H : KM \to h$ guarantees that the hash function H is also collision resistant, and any collision in H has its origin as collision in the compression function f.

The most widely used cryptographic hash functions MD5 and SHA follow the structure of Merkle-Damgrad construction of hash functions. We will take a close look at the SHA-2 hash function of the SHA hash functions family, to better understand the hash functions construction.

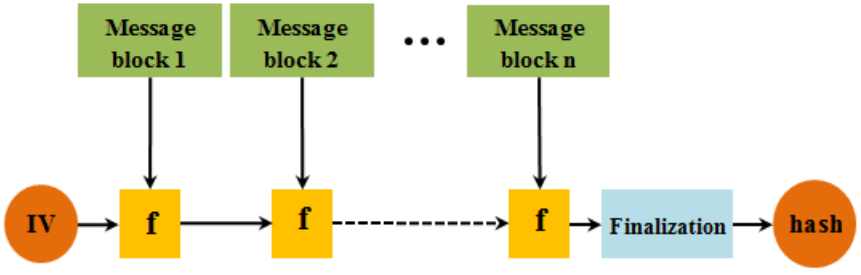


Figure 6: The Merkle-Damgrad hash construction[25]

Secure Hash Function (SHA) is a family of hash functions published by the American NIST (National Institute of Standards and Technology)[24]. The first two versions SHA-1 and SHA-2 have been broken and no longer used in security systems. SHA-2 succeeded SHA-1 in 2010. SHA-2 has multiple versions differ only in the size of the generated hash value as follows: SHA-224, SHA-256, SHA-384, and SHA-512. We will discuss the SHA-512 hash function as it is the most secure in the family, and its structure is similar to the rest of the SHA-2 functions.

SHA-512 operates on a message with maximum length 2^{128} bits and computes a hash value of size 512-bits. The input message is padded and extended with the original message length then divided into 1024-bits blocks. A buffer of 8 registers (a, b, c, d, e, f, g, h) is initialized to represent h_0. After message padding and initializing the hash value h_0, the hash algorithm operates on the message blocks sequentially in a similar manner to Merkle-Damgrad construction.

The compression function used by SHA-512 consists of 80 rounds as depicted in figure 7. The first round takes as input a message word W_0, and a key K_0, and the from processing the previous message block (h_{i-1}). The of each round is used as input for the next round. The of the last round (round 80) is added to the first round input hash value h_{i-1}. After all 1024-bit blocks are processed, the is the 512-bit hash value of the last block processed. We can summarize the behavior of the SHA-512 for N blocks message as follows:

$$\begin{aligned} h_0 &= IV, \\ h_i &= SUM(h_{i-1}, abcdefgh_i), \quad i = 1, \ldots N+1 \\ h &= h_N \end{aligned}$$

5.2 Chaos Theory as basis for Hash Function Construction

Chaos theory is an established field in mathematics with applications in a wide range of scientific fields such as physics, biology, economics, engineering, etc. Chaos theory studies dynamical systems behavior and describes their main characteristics such as: sensitivity to tiny changes in initial conditions, random-like behavior, and the one-way property. Due to these properties chaotic systems have become a very good candidate for use in the field

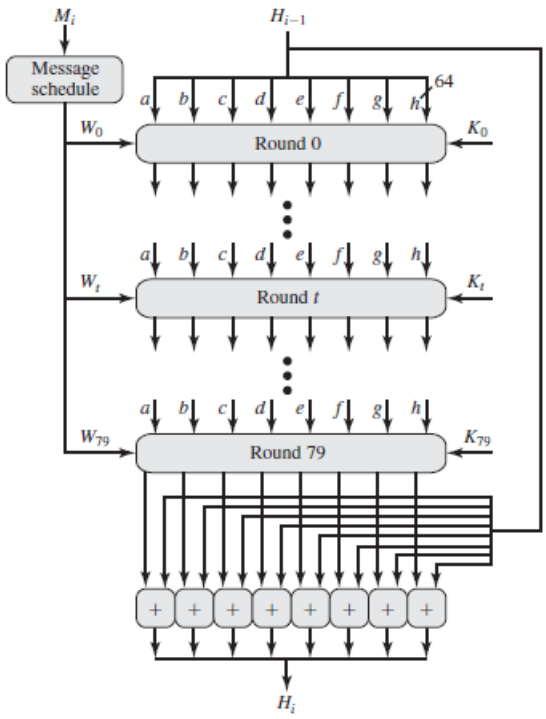


Figure 7: SHA-512 Processing of a Single 1024-Bit Block [25]

of cryptography. In this section we study the various types of chaotic maps, and their use in cryptographic algorithms, more specifically constructing hash functions.

Conventional hash functions as MD4, MD5, SHA-1, and SHA-2 use Merkle-Damgrad construction. The used iterated functions are realized through complicated methods based on logical XOR operations, bit swapping, and multi-round iterations. Research in the last few years showed several defects and weaknesses in the conventional hash functions. As a result, research in the chaos-based hash functions exhibit an attractive design direction.

5.2.1 Prior Work

Chaotic maps inhibit a unique set of properties like high sensitivity to initial conditions, one-way mapping, and randomness. Such properties are crucial to secure hash function applications, as a result chaotic maps have been a major research area for constructing novel and secure hash functions.

In recent years, there has been a considerable amount of research in the construction of cryptographic hash functions based on chaotic maps. Research in this field considered a variety of chaotic maps: logistic map [2], [27], one- and two-dimensional piecewise linear maps [2], [16], Nonlinear chaotic maps, and high-dimensional chaotic maps. Few works investigated the use of other types of chaotic systems, like hyper chaotic map, chaotic neural networks, and chaotic iterations. in what follows, we discuss research efforts used the Logistic map and Piecewise linear maps.

1. **Chaotic Logistic Map**
   The one-dimensional Logistic chaotic map is given by:

$$f(x) = r * x(1 - x), \quad 0 \leq x \leq 1$$

   Where r is a control parameter used to obtain the preferable behavior of the chaotic map. For $r = 4$, the logistic map exhibits a perfect chaotic behavior.

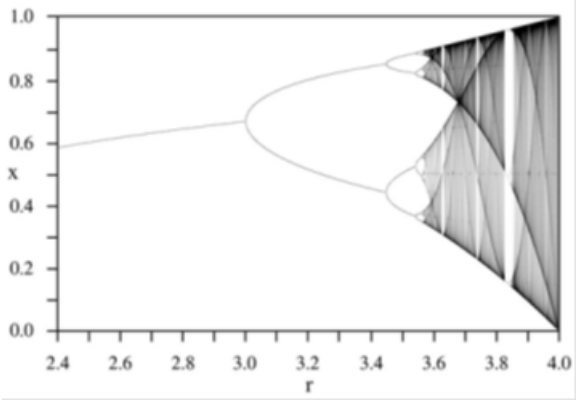


Figure 8: Bifurcation diagram of the Logistic map [10]

The chaotic logistic map attracted a lot of attention and research, because of its simplicity and interesting properties. Researchers proposed a variety of cryptographic algorithms either for hashing or encryption based on the logistic map. One example of such research is the work of R. Bose [10]. In his work, he suggested a simple hash function for message encryption. The hash function uses the chaotic logistic map with parameter $r = 4$. The proposed hash function works as follows:

(a) Start from an initial value x_0, the logistic map is iterated for N iterations to produce a value x_N.

(b) The fraction value of x_N is used to obtain a 64-bit key.

(c) The logistic map is iterated continuously after that, and after every M iterations, the map is used to obtain a 64-bit key as in (ii).
Each generated 64-bit key is used in encrypting a 64-bit message block.

To work, the algorithm requires determining first few arguments: the initial value x_0, number of iterations N, M, and sensitivity of the system. The sensitivity of the system is measured as the difference in the initial value x_0 that produces a difference > 0.0625 after N iterations of the logistic map, according to R. Bose, the number of logistic map iterations N depends on the system sensitivity. For example, R. Bose [10] gives a table in which for sensitivity of order 10^{-30}, the number of iterations N should be equal to 100, and for sensitivity 10^{-19}, $N = 59$. The value of M is decided by the key size, R. Bose used $M = 60$ for 64-bit key.

In addition to building hash functions, the logistic map is also used to encrypt messages. The work done by M.S Baptista [5] suggested an encryption method using the logistic map. The map interval $[0, 1]$ is divided into S ϵ-intervals, and each character is assigned its own ϵ-interval. The encryption algorithm is quiet simple; let us see how a message like "hi" is encrypted:

(a) Given an initial value x_0, the logistic map is iterated until we reach the interval of the character 'h', then the character is coded by the number of iterations required to reach its interval.

(b) Continue to iterate the map until we reach the interval of the character 'i', then we code the letter 'i' with the number of iterations required to reach its interval from the point we reached in the interval of 'h'.

(c) Step 2 is repeated for every character from the point the previous character is reached. The method proposed by M.S. Baptista is simple and easy to apply, the initial value x_0 and parameter p are the secret keys of algorithm. But it is susceptible to hackers'

attacks, if a hacker succeeded in discovering the secret key (i.e. initial value x_0) he can easily decrypt the message.

While the work done on the logistic map provided experimental proofs of feasibility, and resistance to attack scenarios, a thorough analysis of the logistic map reveals few weaknesses for the use in security systems. First, the invariant density of the logistic map is not uniform, which conflicts with the need for uniform hash functions, otherwise a collision attack will break the hash function quickly. Only when the map parameter $r = 4$, the logistic map exhibits perfect chaotic behavior; the dynamical properties of the logistic map are different if the map parameter r is different, which may allow an attacker to collect useful information to reduce the attack complexity. As a result, the logistic map is not a good candidate for high security system [19].

2. Piecewise Linear Chaotic Maps

Piecewise linear chaotic maps (PWLCM) stand as strong competitors to the logistic map. Because of their perfect properties, like uniformity, mixing and ergodicity, and ease of realization by software and hardware. Such a set of properties make PWLCMs an attractive choice for a lot of researchers. One dimensional piecewise tent map is given by

$$f(x) = \begin{cases} x/\alpha; & 0 \leq x \leq \alpha \\ (1-x)/(1-\alpha) & \alpha < x \leq 1 \end{cases}$$

with a control parameter α in the interval $(0, 1)$. Another piecewise linear chaotic map commonly used is given by

$$f(x) = \begin{cases} x/\beta; & 0 \leq x < \beta \\ (x-\beta)/(0.5-\beta); & \beta \leq x < 0.5 \\ (1-\beta-x)/(0.5-\beta); & 0.5 \leq x < 1-\beta \\ (1-x)/\beta & 1-\beta \leq x \leq 1 \end{cases}$$

The control parameter β is in the interval (0,0.5) and ensures that the map runs in a chaotic state.

A work done by L. Yantao [18] demonstrates a method for using the tent map cascaded with the piecewise linear map given above to build a hash function. The proposed hash function processes n message blocks M_i in parallel, each block is 1024-bits divided into 128 bytes (8-bit word m_{ij}). The hash function construction proceeds as follows

(i) Starting from m_{i1} as initial value, for every $i = 1, 2 \ldots n$, the tent map is iterated $\lfloor m_{ij} \times \frac{j}{128} \rfloor$ times, with $\alpha = (\frac{i}{n} \times \frac{j}{128})/2$.

(ii) The of the tent map iterations is used as initial value for the piecewise linear map above. The map is iterated $\lfloor m_{ij} \times (1 - \frac{j}{128}) \rfloor$ times, with $\beta = \alpha/2$.

(iii) The algorithm now repeats the steps (i) and (ii) with the of the piecewise linear map in (ii) is used as initial value for the tent map iterations in step (ii).

For each m_{ij}, the of the piecewise linear map is approximated to the nearest integer, which is either 0 or 1. The 0s and 1s gathered from the message block represent a 128-bit sequence. The sequences from all n message blocks are XORed to generate the final 128-bit hash value.

In a subsequent work [20], L. Yantao suggests a simpler approach using only the tent map. However, the suggested function operates on the message blocks M_i sequentially in a similar manner to Merkle-Damgrad hash construction discussed in the previous section.

5.3 Using the Chaotic Double Map

The double map is given by:

$$f(x) = \begin{cases} 2x; & 0 \leq x \leq \frac{1}{2} \\ 2x - 1 & \frac{1}{2} < x \leq 1 \end{cases}$$

The Double map is a very simple function yet it exhibits a chaotic behavior. In this section we demonstrate how the double map can be used to construct a hash function and message encryption. In [15], it is proved that f is topologically transitive, has a dense set of preiodic points and has sensitive dependence on initial condition, we give the proofs here

1. f is topologically transitive. It suffices to show that f has a dense orbit, so let $z = \sum_{j=1}^{\infty} \frac{c_j}{2^j}$ where c_j is as follow

$$\underbrace{01}_{\text{(1-block)}}, \underbrace{00011011}_{\text{(2-block)}}, \underbrace{000001010011100101110111}_{\text{(3-block)}}.$$

We claim that $\overline{O(z)} = [0, 1]$. Let $x = \sum_{j=1}^{\infty} \frac{a_j}{2^j}$ be an arbitrary point on the interval $[0, 1]$, and let $\delta > 0$ be given. Then there exist $m \in \mathbb{Z}^+$ such that $\frac{1}{2^m} < \delta$. Now the string of $a_1, a_2, \ldots, a_m$ must appear as one of the m-blocks in the binary expansion of z. Hence there exists $k \in \mathbb{Z}+$ such that $f^k(z) = \sum_{i=1}^{\infty} \frac{c_{i+k}}{2^i}$ where $a_1 = c_{k+1}, a_2 = c_{k+2}, \ldots, a_m = c_{k+m}$. This implies that

$$\begin{aligned} |f^k(z) - x| &= \Big| \sum_{j=m+1}^{\infty} \frac{a_j}{2^j} - \sum_{i=m+1}^{\infty} \frac{c_{i+k}}{2^i} \Big| \leq \sum_{i=m+1}^{\infty} \frac{1}{2^i} \\ &= \frac{1}{2^m} < \delta \end{aligned}$$

So we conclude that $\overline{O(z)} = [0,1]$.

2. $\overline{P(g)} = [0,1]$. Let $x = \sum_{j=1}^{\infty} \frac{a_j}{2^j}$ where $a_j = 0, 1$. Then $f(x) = a_1 + \sum_{j=2}^{\infty} \frac{a_j}{2^{j-1}} \pmod 1 = \sum_{j=2}^{\infty} \frac{a_j}{2^{j-1}} = \sum_{i=1}^{\infty} \frac{a_i}{2^i}$.

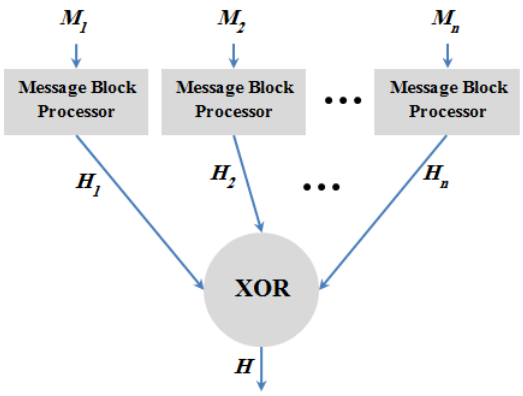
   Note that
   $$f^n(x) = f^n\left(\sum_{i=1}^{\infty} \frac{a_i}{2^i}\right) = \sum_{i=1}^{\infty} \frac{a_{i+n}}{2^i}$$
   Moreover, x is a periodic point of period n if and only if $f^n(x) = x$ and this is equivalent to $a_{i+n} = a_i$, for every i.

   We know that there exists $m \in \mathbb{Z}+$ such that $\frac{1}{2^m} < \delta$ Now, let $y = \sum_{i=1}^{\infty} \frac{b_i}{2^i}$ be a periodic point of period m, where $b_1, b_2, \ldots, b_m$ repeats and $b_1 = a_1, b_2 = a_2, \ldots, b_m = a_m$. Then
   $$\begin{aligned} |x - y| &= \Big| \sum_{j=m+1}^{\infty} \frac{a_j}{2^j} - \sum_{j=m+1}^{\infty} \frac{a_j}{2^j} \Big| \leq \sum_{j=m+1}^{\infty} \frac{1}{2^j} \\ &= \frac{1}{2^m} < \delta \end{aligned}$$
   Hence, the set of periodic points are dense in $[0,1]$

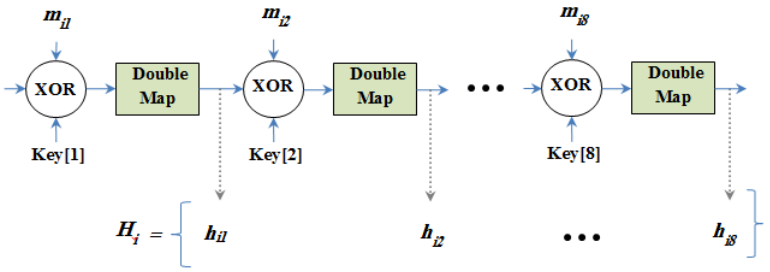
3. It remains to show that f has sensitive dependence on initial conditions. By Proposition 2.1.1
   $$|f'(x)| = 2, \qquad \text{for all } x \in [0,1].$$
   This means that f has a sensitive dependence on initial conditions.

5.3.1 Suggested Hash function

In this section we developed a new method for constructing hash functions using the Double map. We adapted a construction model similar to that used by L. Yanato [18], which is a hybrid of the sequential Merkle-Damgrad model and the parallel processing model. This model achieves better performance, yet maintains strong security level. The suggested hash function uses a 64-bit secret key (K) and produces a 64-bit hash value (H). Figure 9 depicts the hash function data flow:



(a) The hashing function basic structure, M_i is a 64-bit message block, H_i is a 64-bit intermediate hash value, and H is the 64-bit Hash value.



(b) The message blocks processor. m_{ij} is a message block character. h_{ij} is an intermediate 8-bit hash value.

Figure 9: Double Map based Hash Function

1. We first partition the message into a set of blocks $M_0, M_1, \ldots M_n$, where each message block is 64-bits wide, i.e. 8 characters. If the message length is not multiple of 64-bit, we pad the message with a sequence: "10101010" until it is multiple of 64-bits.

2. Partition each message block M_i, into 8-bit words m_{ij} (one character). Each message block consists of 8 such words.

3. Each message block is processed independently from other blocks and a 64-bit temporary hash Hi value is computed from message block M_i.

4. The temporary hash values H_i are XORed to generate the final Hash value H.

The processing of a single Message block is done as follows:

1. Each 8-bit word is XORed with an 8-bit secret key word and the of the last Double map iteration (or 0 for the first 8-bit word in the message block). The XOR operation produces an 8-bit word.

2. Normalize the 8-bit word of the XOR operation such that it represents a value in the interval $[0, 1]$. We divide the 8-bit word with the decimal number 255.0.

3. Iterate the Double map using the normalized value for N iterations.

4. From the fraction of the value of the Double map last iteration, we extract the most significant 8-bits. Those 8-bits represent a sub-hash value h_{ij}.

5. The concatenation of the sub-hash values computed from the 8 characters in the message block represent the 64-bit temporary hash value of each message block Hi.

To determine the number of Double Map iterations (N) we have to determine the level of sensitivity we want to achieve. For example, if we use a 16-bit word to represent a decimal value in the interval $[0, 1]$ as initial value to the Double Map, then changing 1-bit corresponds to a minimum difference 10^{-5} in the initial value. i.e. If we changed the rightmost bit in the binary number it corresponds to $2^{-16} = 1.53 * 10^{-5}$ difference in the initial value. According to Table 1, for such sensitivity level the required number of iterations (N) is 12.

In the suggested hash function, we use 8-bits to represent the decimal initial value of the Double Map, as a result, changing a 1-bit out of the 8-bits corresponds to sensitivity approximately equal to $3 * 10^{-3}$, hence, according to Table 1 the required number of iterations equals 6.

5.3.2 Experiments

To demonstrate the efficiency of the suggested hash function, we did a set of experiments as follows. Appendix A lists the C source code of the developed hash function. Original Message text:

"Department of Mathematics, Birzeit University"

The computed hash value for this message is (in hexadecimal format):

58BD083954517FD8

Table 1: Analysis of the number of Double map iterations versus initial value sensitivity.

Sensitivity	Corresponding word size (in bits)	Number of map iterations (N) to achieve difference > 0.08
10^{-2}	6	2
10^{-3}	9	6
10^{-4}	12	9
10^{-5}	16	12
10^{-10}	32	32
10^{-20}	64	64
10^{-30}	96	98

Appendix B lists the steps of computing the hash value for the message above.

In the following experiments we study the effect of changing the message characters, message length, and secret key (K) on the computed hash value. We try to see how tiny and trivial changes in the original message or the secret key affect the proposed hashing algorithm efficiency.

1. **Change in Message Characters**

   In this set of experiments we consider keeping the length of the message and the secret key unchanged and only test the effect of changes in the message characters.

   Test 1 Consider replacing the character ',' in the original text with the character '/', the new hash value is:

   98BE0409945273D8

   This change in characters in the original text corresponds to change in two binary bits in the original text, however, the generated hash values differs 14 binary bits from the 64-bits of the hash value.

Test 2 Another example of tiny change in the original text is a misspelling of the "Birzeit" word into "Birziet", i.e. swapping the characters 'e' and 'i' in original word. This change produces the hash value:

A8BE0409945273E8

The generated hash value differs 18 binary bits from the original text hash value.

Test 3 Another moderate change in the original text we could consider is swapping the positions of the phrases "Birzeit University" and "Department of Mathematics":

"Birzeit University, Department of Mathematics"

This change produces the following hash value:

DF7754DDA5226F58

This hash value differs 28 binary bits from the original text hash value.

2. **Change in Message Length**

Test 1 Another type of change to consider is the length of the message, consider a tiny change like dropping the ',' character after "Mathematics" from the original text. The generated hash value will be:

2ED569CD7B3C6AA8

The generated hash value differs 32-bits out of 64-bits (length of hash value) from the original text hash value.

Test 2 Another example is given by adding a space character to the start of the original text before the word "Department", the generated hash value is

362681B6DAAE9F1D

The generated hash value differs 37-bits out of 64-bits from the original text hash value.

Test 3 Let us see how a major addition to the message text can affect the computed hash value. Consider adding the phrase "College of Science," after "Department of Mathematics", the computed hash value will be

6793613F22A48670

The computed hash value differs 36-bits out of 64-bits in the original text hash value.

3. **Change in Secret Key**

We now consider how the suggested hash function reacts to changes in the secret key (K) while the original message text is kept unchanged. In the above experiments, the used secret key was an eight character string given as follow: "ABCDEFGH".

Test 1 Consider changing the first character of the Key string from 'A' capital to 'a' small letter. The computed hash value is

A742F7C6ABAE7FD8

The computed hash value differs in 48-bits out of 64-bits of the original text with the original key hash value.

4. **Completely Different Messages**

   What if we have completely different message, how much the hash values of two completely different messages will differ? Let us consider the message

   "IT Division, Jawwal Company, Ramallah"

   The hash value of the message above is

   9BD1D9B9964E7E58

   The computed hash value of the above message differs in 23-bits out of 64-bits of the original message "Department of Mathematics, Birzeit University".

The proposed hashing function has several attractive features:

1. The Processing of the whole message is parallelized by making message blocks processed independently. This will improve the performance of the algorithm.

2. The computations per single Double map iteration are quite simple: multiplications by 2 can be converted into the cheaper addition operation, instead the more expensive multiplication operation.

3. The number of the Double map iterations is few which reduces the computational cost.

The proposed hashing algorithm provides a moderate level of security, with minimal computational complexities. There are two ways to strengthen the security level; increasing the word size of the map initial value (e.g. from 6-bits to 32-bits) to increase the sensitivity level. The second way is to increase the length of the hash value (e.g. from 64-bits to 128- or 256-bits). We can increase the size of the hash value by increasing the size of the message block. For example when increasing the size of hash value from 64-bits to 128-bits, the size of the message block will increase from 8 characters to 16 characters.

A Hashing Algorithm Code

Here we list the C source code implementing the hash function that we developed in section 5.3.1.

```
//-------------------------------------------------------------//
/*
    This function takes as input a message and a key,
    and operates on them to compute the hash value.
*/
unsigned long long int hash(unsigned char key[],
                            unsigned char * message){


  // Compute padded message length
  int len = strlen(((char*)(message)));

  int slen = len;
  int add = (slen%8 > 0)? 8 - slen%8 : 0;

  slen += add;

  // allocate padded message memory
  unsigned char * PM = new unsigned char[slen];

  // Message padding
  for(int i = 0; i < len; i++)    PM[i] = message[i];
  for(int i = len; i < slen; i++) PM[i] = 0xAA;

  int N = slen/8;
  int M = 8;

  unsigned long long int * hvs = new unsigned long long int[N];

  // Start iteratively processing of message blocks
  for(int i = 0; i < N; i++)
  {
    hvs[i] = 0;
    unsigned char tkey = 0;
    for(int j = 0; j < M; j++)
```

```
    {
      unsigned char byte = PM[8*i+j];
      // Xor with key
      byte = byte ^ key[j] ^ tkey;

      float iv = (byte & 0xFF)/255.0;

      // iterate map
      iv = iterateMap(iv, 6);

      unsigned char h0 = (unsigned char)(iv * 255);

      tkey   = h0;

      hvs[i] = (hvs[i] << 8) | h0;
    }
  }

  // xor hvs
  unsigned long long HVal = 0;

  for(int i = 0; i < N; i++)
  {
    HVal = HVal ^ hvs[i];
  }

  return HVal;
}

//-----------------------------------------------------------------//
// This function computes the Double Map

float DoubleChaoticMap(float x){

  if( x < 0.0 )       return 0.000000000000;
  else if( x < 0.5 )  return 2.000000000000*x;
  else if( x < 1.0 )  return (2.000000000000*x - 1.000000000000);
  else                return 0.000000000000;

  return 0.0;
```

```
}

//-------------------------------------------------------------------//
/*
  This function takes an initial value 'x' and number of
  iterations"niters", then iterates the Double Map.
*/

float iterateMap(float x, int niters){

  float y = x;
  for(int j = 0; j < niters; j++)
  {
    y = DoubleChaoticMap(y);
  }
  return y;
}

//
```

B Hashing Algorithm Example

```
Process the Message: "Department␣of␣Mathematics,␣Birzeit␣University"

message length = 360-bits, hence, add 24-bits to the message to
make message length multiple of 64-bits,
then compute the number of message blocks = 6.

List of message blocks: {"Departme", "nt␣of␣Ma", "thematic",
                         "s,␣Birze", "it␣Unive", "rsity  "}

Used Secret Key = EFGHABCD

Start Processing of the message...

process the message block: "Departme"

XOR(mij,key[i], IV)   Double Map Iteration Output
--------------------  ------------------------------------
XOR('D', E, 00) = 01, 0.25098  -- to Hex -->  40
XOR('e', F, 40) = 63, 0.847059 -- to Hex -->  d8
XOR('p', G, d8) = ef, 0.984314 -- to Hex -->  fb
XOR('a', H, fb) = d2, 0.705883 -- to Hex -->  b4
XOR('r', A, b4) = 87, 0.882355 -- to Hex -->  e1
XOR('t', B, e1) = d7, 0.960785 -- to Hex -->  f5
XOR('m', C, f5) = db, 0.964706 -- to Hex -->  f6
XOR('e', D, f6) = d7, 0.960785 -- to Hex -->  f5

process the message block: "nt␣of␣Ma"

XOR(mij,key[i], IV)   Double Map Iteration Output
--------------------  ------------------------------------
XOR('n', E, 00) = 2b, 0.792157 -- to Hex -->  ca
XOR('t', F, ca) = f8, 0.243137 -- to Hex -->  3e
XOR('␣', G, 3e) = 59, 0.337255 -- to Hex -->  56
XOR('o', H, 56) = 71, 0.360785 -- to Hex -->  5c
XOR('f', A, 5c) = 7b, 0.870588 -- to Hex -->  de
XOR('␣', B, de) = bc, 0.184315 -- to Hex -->  2f
XOR('M', C, 2f) = 21, 0.282353 -- to Hex -->  48
XOR('a', D, 48) = 6d, 0.356863 -- to Hex -->  5b

process the message block: "thematic"
```

```
XOR(mij,key[i], IV)    Double Map Iteration Output
-------------------    ---------------------------------------
XOR('t', E, 00) = 31, 0.298039 -- to Hex -->  4c
XOR('h', F, 4c) = 62, 0.596079 -- to Hex -->  98
XOR('e', G, 98) = ba, 0.682354 -- to Hex -->  ae
XOR('m', H, ae) = 8b, 0.886276 -- to Hex -->  e2
XOR('a', A, e2) = c2, 0.690197 -- to Hex -->  b0
XOR('t', B, b0) = 86, 0.631374 -- to Hex -->  a1
XOR('i', C, a1) = 8b, 0.886276 -- to Hex -->  e2
XOR('c', D, e2) = c5, 0.443138 -- to Hex -->  71

process the message block: "s, Birze"

XOR(mij,key[i], IV)    Double Map Iteration Output
-------------------    ---------------------------------------
XOR('s', E, 00) = 36, 0.552941 -- to Hex -->  8d
XOR(',', F, 8d) = e7, 0.976471 -- to Hex -->  f9
XOR(' ', G, f9) = 9e, 0.654903 -- to Hex -->  a7
XOR('B', H, a7) = ad, 0.419609 -- to Hex -->  6b
XOR('i', A, 6b) = 43, 0.815687 -- to Hex -->  d0
XOR('r', B, d0) = e0, 0.219608 -- to Hex -->  38
XOR('z', C, 38) = 01, 0.25098  -- to Hex -->  40
XOR('e', D, 40) = 61, 0.345098 -- to Hex -->  58

process the message block: "it Unive"

XOR(mij,key[i], IV)    Double Map Iteration Output
-------------------    ---------------------------------------
XOR('i', E, 00) = 2c, 0.043137 -- to Hex -->  0b
XOR('t', F, 0b) = 39, 0.305882 -- to Hex -->  4e
XOR(' ', G, 4e) = 29, 0.290196 -- to Hex -->  4a
XOR('U', H, 4a) = 57, 0.835295 -- to Hex -->  d5
XOR('n', A, d5) = fa, 0.745098 -- to Hex -->  be
XOR('i', B, be) = 95, 0.39608  -- to Hex -->  65
XOR('v', C, 65) = 50, 0.078432 -- to Hex -->  14
XOR('e', D, 14) = 35, 0.301961 -- to Hex -->  4d

process the message block: "rsity  "

XOR(mij,key[i], IV)    Double Map Iteration Output
-------------------    ---------------------------------------
XOR('r', E, 00) = 37, 0.803922 -- to Hex -->  cd
XOR('s', F, cd) = f8, 0.243137 -- to Hex -->  3e
XOR('i', G, 3e) = 10, 0.015686 -- to Hex -->  04
XOR('t', H, 04) = 38, 0.054902 -- to Hex -->  0e
```

```
XOR('y', A, 0e) = 36, 0.552941 -- to Hex -->  8d
XOR(' ', B, 8d) = 65, 0.34902  -- to Hex -->  59
XOR(' ', C, 59) = b0, 0.17255  -- to Hex -->  2c
XOR(' ', D, 2c) = c2, 0.690197 -- to Hex -->  b0

Generated list of Temporary Hash values:

40d8fbb4e1f5f6f5
ca3e565cde2f485b
4c98aee2b0a1e271
8df9a76bd0384058
b4e4ad5be65144d
cd3e040e8d592cb0

Result of XORing Temporary Hash Values = 8df7eaba6c7f247a
```

References

[1] Abu Khalil B., Master Thesis, May 2012, "Devaney's Definition of Chaos and Other Form", Birzeit Univty, Palestine.ersi

[2] Assaf D., and Gadbois S., "Definition of Chaos", Letter in American Mathematics Monthly, 99, pp. 112-122,1992.

[3] Aullbach, B. and Keininger B., "On Three Definitions of Chaos", Nonlinear Dynamics and system theory, 1, pp. 23-37, 2001.

[4] Banks J., Brooks J., Cairns G., Davis G. and Stacey P., "On Devaney's Definition of Chaos", Letter in American Mathematics Monthly, 99, pp. 332-334, 1992.

[5] Baptista M.S., "Cryptography with Chaos", Physics Letters A 240:50 - 54, Elsevier Science, March 1998.

[6] Barge M. and Martin J., "Dense orbits on the interval", Michigan Mathematics Journal, 34, pp. 3-11, 1987.

[7] Blanchard F., Glasner E., Kolyada S., and Maass A., "On Li-Yorke pairs" J. Reine Angew. Mathematics, 547, pp. 51-68, 2002.

[8] Blanchard F., "Topological chaos: What may this mean?", Mathematics Dynamical Systems Archive, Cornel University Library, 2008.

[9] Block L.S. and Coppel W.A., "Dynamics in one dimension", Lecture Notes in Mathmatics, 1995.

[10] Bose R., and Banerjee A., "Implementing Cryptography using Chaos Functions", 7th Int. Conf. on Advanced Computing and Communications, Dec 20 - 22, 1999, Roorkee, India.

[11] Cranell A., "The role of transitivity in Devaneys denition of chaos", Letters in American Mathematics Monthly, 102, pp. 788-793, 1995.

[12] Degirmenci N. and Kocak S., "Existence of a dense orbit and topological trnasitivity: when they are equivalent?", Acta Mathematics, Hungarian, 99, pp. 185-187, 2001.

[13] Denker M., Grillerberger C., Sigmurd K., "Ergodic theory on compact spaces", Lecture note of mathmatics, 1976.

[14] Devaney R. L., **"An introduction to chaotic dynamical systems"**, Addison Wesley Puplishing Company Advanced Book Program, Redwood City, CA, second edition, 1989.

[15] Elaydi S. N., **"Discrete chaos with applications in science and engineering"**,2nd edition, Chapman & Hall/CRC, 2007, Boca Raton, FL USA.

[16] Hamza T., Saleh M.,"New proposed definition of chaos".

[17] Kolyada S., and Snoha L., "Some Aspects Of Topological transitivity", a survey, 1997, 2-35.

[18] Kumar V., PHD thesis, Septemper 2001, "On Chaos and Fractls in general topological spaces", Cohin University of Science and Technology, Kerala, Inida.

[19] Li Y., Xiao D., Deng S., Han Q., and Zhou G., "Parallel Hash function construction based on chaotic maps with changeable parameters", Springer Journal on Neural Computing & Applications, 20, pp. 1305-1312, 2011.

[20] Li Y., Xiao D., and Deng S., "Secure hash function based on chaotic tent map with changeable parameter", High Technology Letters, 18, pp. 7 - 12, March 2012.

[21] Li T., and Yorke J., "Period three implies chaos", Letters in American Mathematics Monthly, 82, pp. 985-992, 1975.

[22] Oestreicher C., "A History of Chaos Theory", Journal of Dialogues Clin Neurosci, 9, pp. 279 - 289, 2007.

[23] Peris A., "Transitivity, dense orbit and discontinuous functions", Bulletin of the Belgian Mathematical Society - Simon Stevin, 6, pp. 321-471, 1999.

[24] S. Silverman, "On maps with dense orbits and the definition of chaos", Rocky Mountain Journal of Mathematics, 22, pp. 353-375, 1992.

[25] Stalling W., **"Cryptography and Network Security: Principles and Practice"**, 5th edition, Prentice Hall, 2011, NY, USA.

[26] Touchey P., "Yet another denition of chaos", Letters in American Mathematics Monthly, 104, pp. 411-414, 1997.

[27] Vellekoop M. and Berglund R., "On Intervals, Transitivity = Chaos", Letter in American Mathematics Monthly, 101, pp. 353-355, 1994.

[28] Walters P., **"An introduction to ergodic theory"**, Springer-Verlag, New York, 1982.

[29] Wang X. and Huang Y., "Devaney chaos revisited", Mathematics Dynamical Systems Archive, Cornel University Library, 2012.

[30] Wiggins S., **"Introduction to applied nonlinear dynamical systems and chaos"**, Texts in Applied Mathematics, 2, 1990.