Periodicity of the Tent Map

M Denesh Kumar, Sriram Gopalakrishnan
Indian Institute of Technology Madras, Chennai
(Both authors contributed equally)

April 2019

Abstract

In this review, various aspects of the tent map are studied. The Bifurcation Diagram provides insight into periodic points of the map. The Frobenius-Peron equation yields insight about the time evolution of phase space density, as well as the functional equation governing invariant densities of the map. Interesting remarks can be made about a particular case of the Tent Map which is topologically conjugate to a logistic map. Finally, we discuss an application of tent maps in image encryption.

Keywords: Fixed Point, Bifurcation, Periodic Orbits, Topological Equivalence, Invariant Density, Chaos.

1 Introduction

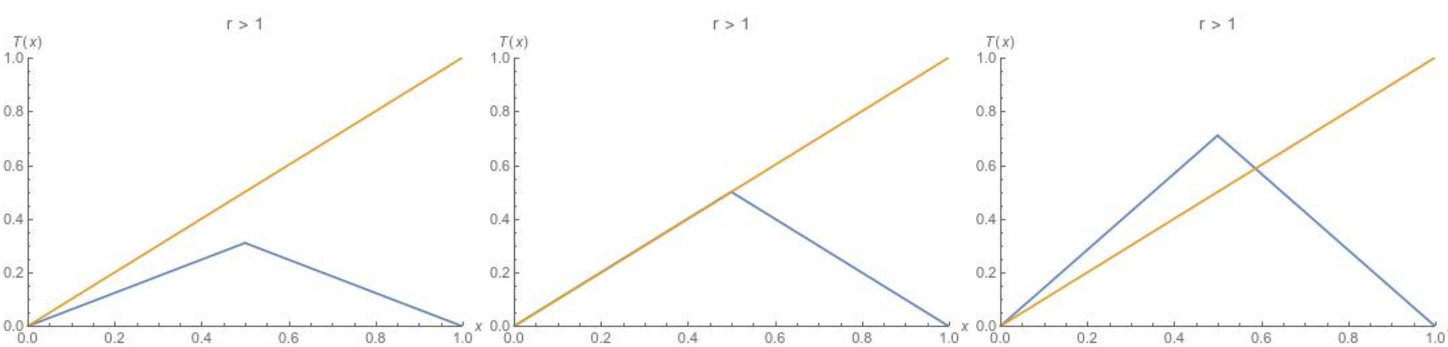
In the theory of Dynamical Systems, the Tent Map is a canonical example of a 1D Map. Chaotic 1D maps, including the tent map, have found applications in Cryptography [1, 2] and Image Encryption [3, 4].

2 The Map

The tent map is defined by

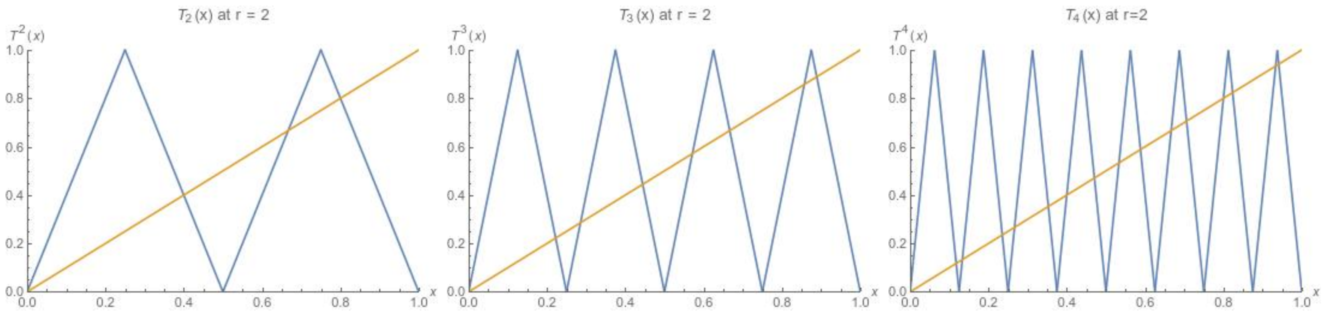
$$T_r(x) = r\ \min\{x, 1-x\} \qquad 0 \leq x \leq 1 \tag{1}$$

The name originates from the shape of $T_r(x)$ in its domain. The discrete iteration is carried out as $x_{n+1} = T_r(x_n)$. A valid dynamical map must map the domain [0,1] to itself in order to permit infinite iterations. It is easy to see that the tent map is a valid map only when $0 \leq r \leq 2$, and hence this is the range of the control parameter we will be interested in.



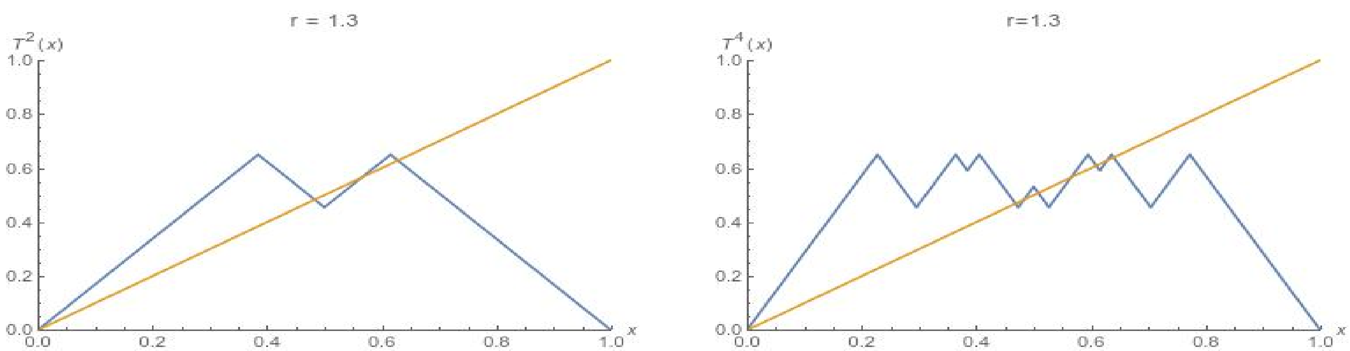
The above plots describe the nature of the tent map for three different regions of the control parameter: $r < 1$, $r = 1$ and $r > 1$. For $r < 1$, there is a stable fixed point at $x = 0$.
For $r = 1$, the entire interval $[0, 0.5]$ is fixed. However every point in this interval has a zero Lyapunov exponent, that is, a slight perturbation in x neither grows nor decays in magnitude. Hence these points are not

asymptotically stable.
For $2 \geq r > 1$, there are two unstable fixed points $(x^* = 0, \frac{r}{r+1})$.
The case of the tent map when $r = 2$ is interesting since iterates of the map $T^n(x)$ for $n \geq 2$ have a simple geometric structure.



Evidently $T^n(x)$ for $r = 2$ has 2^{n-1} tents in $[0, 1]$, because of which it has 2^n intersections with the $y = x$ line, and hence has 2^n periodic points with period less than or equal to n.

Experimenting with $T_2(x)$ and $T_4(x)$, we notice that at $r = 1$, in addition to the fixed point $x^* = \frac{r}{r+1}$,
2 prime period-2 points and 4 prime period-4 points are created.



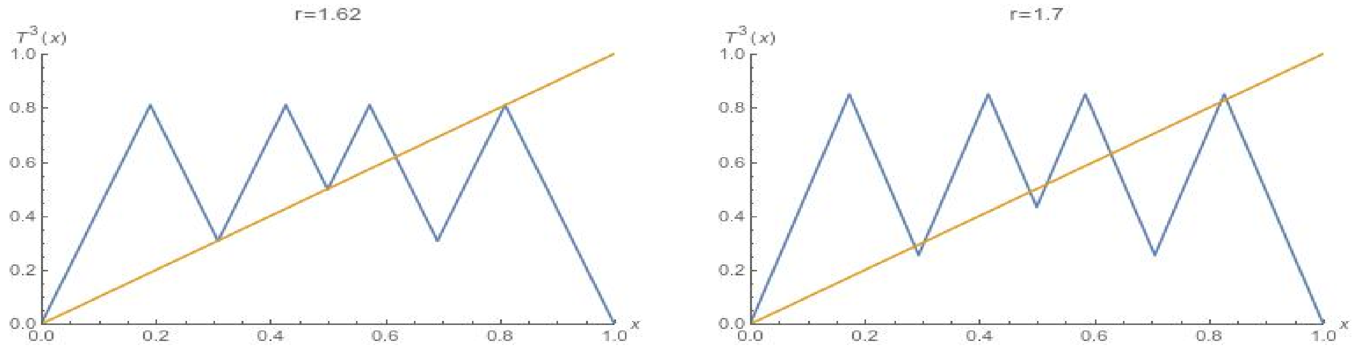
(a) $T^2(x)$ for $r = 1.3$

(b) $T^4(x)$ for $r = 1.3$

Figure 1: The plots show the creation of period-2 and period-4 points as r is increased slightly beyond 1.

This leads to an interesting extrapolation that for all integers $k \geq 1$, exactly one prime periodic orbit of period 2^k is created at $r = 1$.

Examining $T^3(x)$, we find that a prime period-3 orbit is born at $r \approx 1.62$, and there are two prime period-3 orbits for $1.62 < r \leq 2$.



(a) $T^3(x)$ for $r = 1.62$ (b) $T^3(x)$ for $r = 1.7$

Figure 2: The plots show the creation of prime period-3 points at $r = 1.62$

By Li & Yorke's theorem[5], the existence of period-3 orbits implies the existence of period-n orbits for all natural numbers n, and that there exists an uncountable subset of $[0, 1]$ that is neither periodic nor asymptotically periodic. Note that Li & Yorke's theorem is statement of sufficiency, not both necessity and sufficiency. Thus we can conclude that for $1.62 < r \leq 2$, there exists an uncountable subset of $[0, 1]$ in which repeated iteration of T_r is aperiodic. Back in 1975, Li & Yorke referred to chaos purely in the sense of the existence of such an aperiodic set.

Formally, chaos in the context of maps, as introduced by Devaney in his classic 1986 book [6], is defined as follows -

Definition 2.1. Let X be a metric space. A continuous map $f : X \to X$ is said to be *chaotic* on X if -

1. f is topologically transitive, i.e for every pair of non-empty open sets U and V in X, there is a non-negative integer n such that $f^n(U) \cap V \neq \emptyset$.
2. The periodic points of f are dense in X.
3. f has sensitive dependence on initial conditions.

Due to Banks *et. al.* (1992) [7], it is now known that condition 1 and condition 2 implies condition 3.

The tent map at $r = 2$, denoted as $T_2(x)$ has some interesting properties worth mention -

- A point $c \in [0, 1]$ is periodic ***if and only if*** it is a rational number with even numerator and odd denominator, i.e $c = \frac{p}{q}$ where p is odd and q is even. For instance, $\frac{2}{7}$ is a periodic point, but rationals such as $\frac{1}{7}$, $\frac{3}{8}$ and irrational numbers like $\frac{1}{\pi}$ and $\frac{1}{\sqrt{2}}$ are asymptotically periodic and aperiodic respectively. Note that this periodic set is still dense in $[0, 1]$.
- $T_2(x)$ is topologically conjugate to $L_4(x)$ via $h(x) = \sin^2(\frac{\pi x}{2})$. In other words, $T_2 \circ h = h \circ L_4$. As discussed in class, topological conjugacy leads to two interesting insights -
  - Since the condition can be extended as $T_2^n \circ h = h \circ L_4^n \quad \forall n \geq 1$, and because $\sin^2(\frac{\pi x}{2})$ in injective in $[0, 1]$, there is a one-to-one correspondence between periodic orbits of T_2 and L_4 for all periods.
  - Further, the Lyapunov exponent at these corresponding periodic points are equal.

  Here we use the Logistic map as $L_r(x) = r\ x(1 - x)$.
- The Frobenius-Peron evolution of phase space density for T_2 is given by -

$$\rho(x, n + 1) = \frac{1}{2}\ \rho\left(\frac{x}{2}, n\right) + \frac{1}{2}\ \rho\left(1 - \frac{x}{2}, n\right) \tag{2}$$

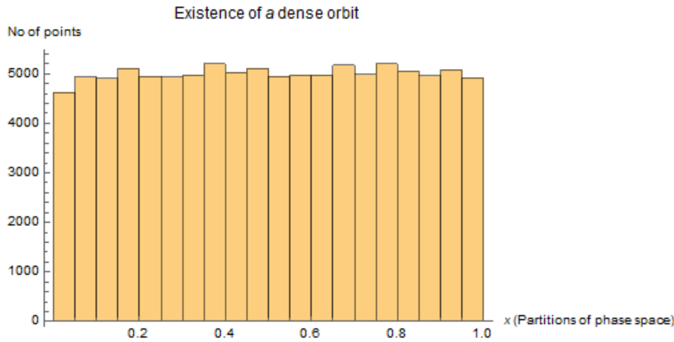


Figure 3: Histogram simulation of invariant density of $T_{1.999}(x)$

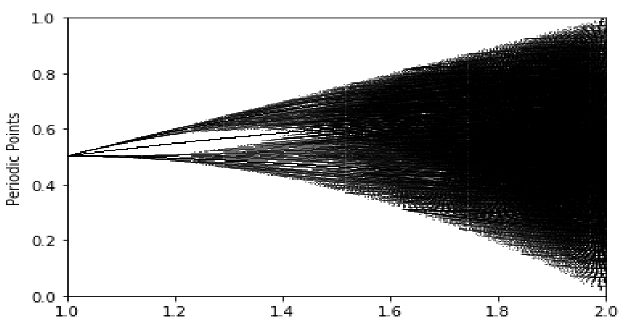
The functional equation governing invariant densities of the map is hence -

$$\rho_0(x) = \frac{1}{2}\ \rho_0\left(\frac{x}{2}\right) + \frac{1}{2}\ \rho_0\left(1 - \frac{x}{2}\right) \tag{3}$$

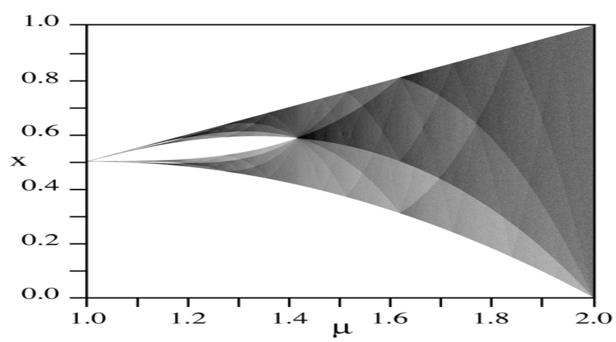
It turns out that the invariant density of T_2 is $\rho_0(x) = 1$.

3 Bifurcation diagram

The bifurcation diagram shows all the periodic points as a function of the control parameter r. It can be observed that at r=2, the enitre range of x= [0,1] is filled by the graph. This means that periodic points of all periods exists in this regime (they are dense as well) which is an indication of Chaos.



(a) Approximate Bifurcation Diagram (Python)



(b) Established Bifurcation Diagram (Wikipedia)

Figure 4: A comparison of our approximate bifurcation diagram with an established bifurcation diagram from Wikipedia.

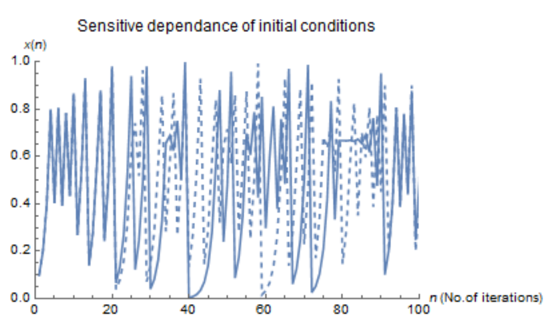


Figure 5: Illustrating sensitive dependence on initial conditions

The sensitive dependence on initial conditions for the tent map at $r = 2$ is illustrated in figure 5 where the iterates of two very close initial conditions ($x_{01} = 0.1$ and $x_{02} = 0.1000001$) are plotted as a function of n. They seem to diverge within about 20 iterations.

4 An image encryption scheme based on chaotic tent map

In this section, we look at a particular application of the tent map. The chaotic properties of the tent map are utilized in an algorithm to encrypt an image for upholding the security of the same. This method was proposed in [3] titled "An image encryption scheme based on the chaotic tent map". In what follows, we present a summary of this paper.

The Chaotic properties of the tent map serves an important role in generating sequences which when observed over a large number of iterations are statistically uncorrelated.

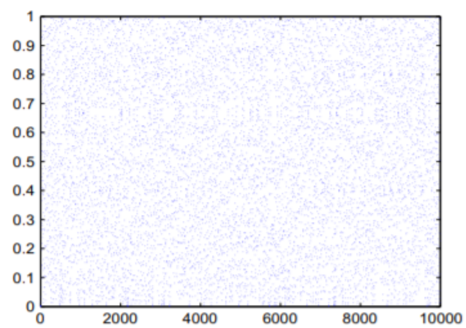


Figure 6: The plot shows the correlation analysis of the successive iterates of tent map.

The tent map with $r = 2$ satisfying the following statistical characteristics in the interval [0, 1] are important for the algorithm:

- The Lyapunov index is greater than 0 ($\lambda = ln(2)$ as calculated above). The output signal satisfies the traversal of the state, mixing and certainty.
- It has constant invariant distribution density function $f(x_i, r) = 1$.
- The system is sensitive to initial conditions.

From the above properties it follows from [7] that the the Tent Map exhibits chaos in the regime $r = 2$, which is essential for the encryption algorithm.

The following sections illustrate the algorithms for image encryption and decryption using equation (1). .

4.1 Image encryption algorithm

1. Read plain-images (original image) (M_{axb}), get size of M, (e.g)., use [a, b, c] to save the size of M, a = 256, b = 256, c = 3, let N = $axbxc$, and initiate control parameter (r) of the chaotic tent map. (Here, c represents the dimensions of the RGB layers.)
2. Input the secret (encryption) key x_0 into the algorithm. Iterate the chaotic tent map N times , and obtain the key array $x(n)$, the size of $x(n)$ is N.
3. Encrypt each element of matrix (M_{axb}) using the key array x(n), that is, mix the original image (M_{axb}) components with the key array x(n).
4. The resulting image of step (3) is the ciphered image.

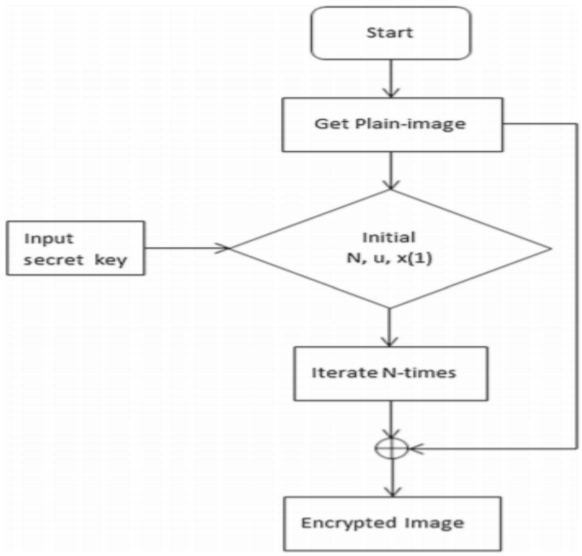


Figure 7: The image encryption algorithm.

4.2 Image decryption algorithm

1. Read ciphered images (encrypted image) ($M_{a\text{x}b}$),get size of M, e.g., use [a, b, c] to save the size of M, a = 256, b = 256, c = 3, let N = axbxc, and initiate control parameter (r) of the chaotic tent map, the control parameter (r) must same as step (1) of the Encryption scheme.

2. Input the secret (decryption) key x_0 into the algorithm, the key x_0 must same as the encryption key, if not we will not get the original image. Iterate the chaotic tent map N times using system (2) and obtain the key array $x(n)$; the size of $x(n)$ is N.

3. Decrypt each element of matrix (M_{axb}) using the key array $x(n)$, that is, pick out the original image from the ciphered image (M_{axb}) components using the key array $x(n)$.

4. The obtained image from step (3) is the decrypted (original) image.

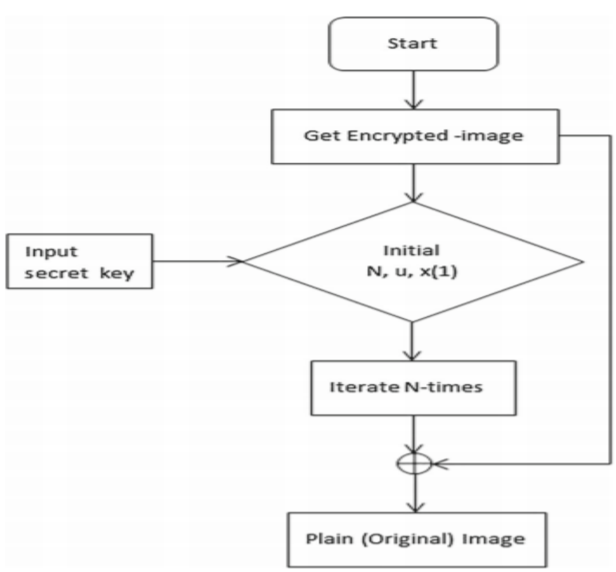


Figure 8: The image decryption algorithm.

4.3 Experimental results

The following experimental results were presented to demonstrate the efficiency of the proposed image encryption algorithm. The standard grayscale image Lenna (Fig. 9a) with the size 256 x 256 pixels was used for the experiment. The results of the encryption are presented in Fig. 9b. As can be seen from the figures, there are no patterns or shadows visible in the corresponding cipher text. The results of the decryption are presented in Fig. 9c. As can be seen from the figures, it is no different from the original image. The results of the decryption using a wrong key are presented in Fig. 9f. As can be seen from the figures, there are no patterns or shadows visible in the corresponding ciphered image.

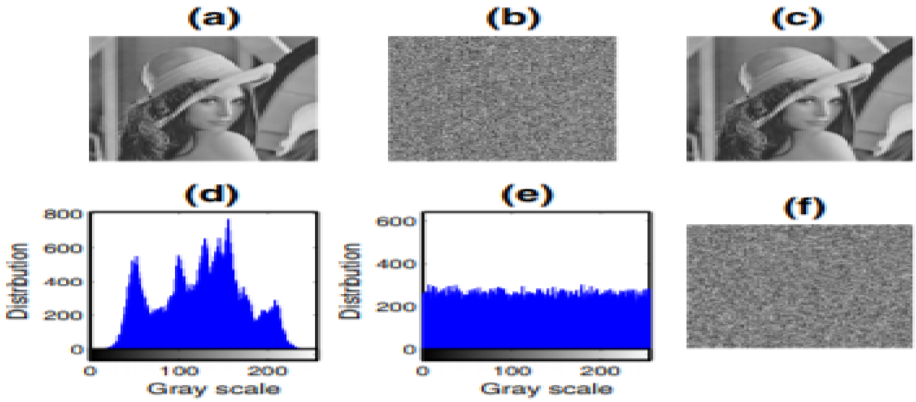


Figure 9: a) The original image. b) The encrypted image. c) The decrypted image. d) The histogram of original image. e) The histogram of ciphered image. f) The decrypted image with wrong key.

4.4 Security Analysis

In this scheme,the key taken to encrypt the image was : $x_0 = 0.000001$, $r = 1.999999$. When taking the wrong key, where the difference between the wrong and right key is only 10^{-16}. For example, using $x_0 = 0.0000009999999999$ as the wrong key to decrypt the encrypted image, the wrong decrypted image obtained is shown in Fig. 9f.

5 Conclusion

Hence, a brief analysis of the tent map was discussed along with an interesting application in Image encryption. It leads us to conclude that the tent-map is a very important theoretical concept having a lot of real-life applications.

References

[1] Xun Yi. "Hash function based on chaotic tent maps". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 52.6 (2005), pp. 354–357.

[2] NK Pareek, Vinod Patidar, and KK Sud. "Cryptography using multiple one-dimensional chaotic maps". In: *Communications in Nonlinear Science and Numerical Simulation* 10.7 (2005), pp. 715–723.

[3] Chunhu Li et al. "An image encryption scheme based on chaotic tent map". In: *Nonlinear Dynamics* 87.1 (2017), pp. 127–133.

[4] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. "A fast image encryption scheme based on chaotic standard map". In: *Physics Letters A* 372.15 (2008), pp. 2645–2652.

[5] Tien-Yien Li and James A Yorke. "Period three implies chaos". In: *The American Mathematical Monthly* 82.10 (1975), pp. 985–992.

[6] Robert Devaney. *An introduction to chaotic dynamical systems*. Westview press, 2008.

[7] John Banks et al. "On Devaney's definition of chaos". In: *The American mathematical monthly* 99.4 (1992), pp. 332–334.

[8] *Tent Map*. URL: `https://en.wikipedia.org/wiki/Tent_map`.

[9] Steven H. Strogatz. *Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry, And Engineering*. 1st ed. Studies in Nonlinearity. Westview Press, 2001. ISBN: 9780738204536.

Bifurcation Diagram of the Tent Map

April 22, 2019

This jupyter notebook is dedicated to plotting the bifurcation diagram of the famous tent map.

In [1]:
```
import numpy as np
import scipy.special as sp
import matplotlib.pyplot as plt
from math import*
from array import*
%matplotlib inline
```

In [2]:
```
R=np.arange(1,2,0.001)
X=np.arange(0,1,0.001)
dx=0.001
```

In [3]:
```
def tent(r,t):
    if 0<=t<=0.5:
        return r*t
    else:
        return r*(1-t)
```

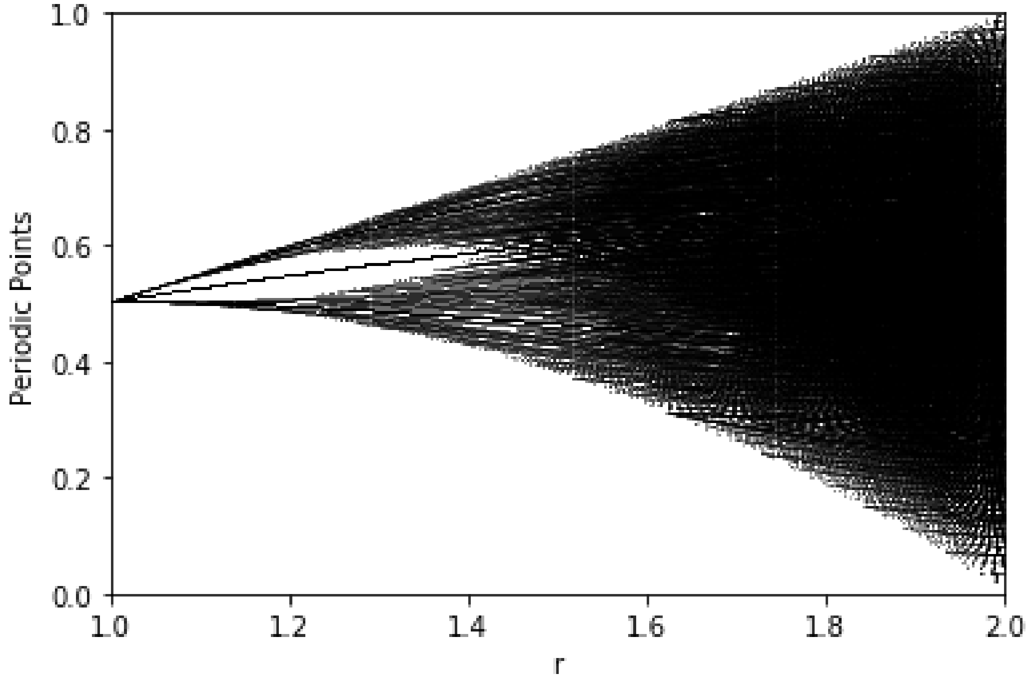
In [4]:
```
def tent_it(n,r,x):
    temp = x
    for i in range(1,n+1):
        temp = tent(r,temp)
    return (temp - x)
```

In [5]:
```
def periodicpoints(r):
    roots = []
    for x in X:
        for n in range(1,12):                          #Upto period 11.
            if tent_it(n,r,x)*tent_it(n,r,x+dx) < 0:
                roots.append(x+(dx/2))
    return roots
```

In [7]:
```
for r in R:
    plt.plot(list(r*np.ones(len(periodicpoints(r)))), periodicpoints(r), ',k',
    alpha = 0.25);

plt.xlim(1,2);
```

```
plt.ylim(0,1);
plt.xlabel('r');
plt.ylabel('Periodic Points');
```



The above plot shows an approximate picture of the bifurcation diagram. Points of period upto 11 are considered for 1000 iterations of r between 1 and 2.