Paper Title
Math 421

Alexis Tavares

(10136734)

April 10, 2015

Contents

1 Introduction

A fractal is a mathematical set that exhibits a repeating pattern visible regardless of scale. These patterns are never ending and infinitely complex. Built by recursive patterns of functions, called iterated function systems, these geometric objects display various dynamic behavior . Visually, thedr is also a beautiful pieced of art that can be explored mathematically as well as in the natural world: typically in the form of ferns and mountain ranges.

In the early 20th century, French mathematician Gaston Julia studied the iteration of these polynomials and rational functions and game up with what we now know as the Julia set. He investigated this sets propteries and behavior which he published in his 1918 paper Mmoire sur l'itration des fonctions rationnelles, later popularized by French mathematician Benoit Mandlebrot in his own works.

2 Julia Set

2.1 Definition

The following iterated process generates the Julia set[5]:

$$f(z)\colon z \mapsto z^2 + c$$

where z and $c \in \mathbb{C}$. We choose a particular c and z_0 thus generating $z_1, z_2, z_3, \cdots$ by

$$\begin{aligned} z_1 &= z_0^2 + c \\ z_2 &= z_1^2 + c \\ z_3 &= z_2^2 + c \\ &\vdots \end{aligned}$$

We can also define the set using a polynomial $f\colon \mathbb{C} \mapsto \mathbb{C}$ by defining [4]

$$f^n(z) = \underbrace{(f \circ \ldots \circ f)}_{\text{n times}}(z)$$

Both are equivalent to the two-dimensional map [3]

$$f(x,y)\colon (x,y) \mapsto (x^2 - y^2 + a, 2xy + b)$$

where $z = x + iy = (x,y)$ is the point we iterate over and $c = a + ib = (a,b)$ is the stationary parameter.

This quadratic map can be looked at as a family of transformations to the plane $\mathbb{C}$. This is most easily understood representing these values as points on the complex sphere. [3] [image goes here]

For any given starting value of z, there are two possiblities for the iterated $f(z)$ generated by z_i, [7] as i tends towards infinity either $f(z)$ will also tend towards infinity and become unbounded, else it will not and remain bounded instead. Points which do tend toward infinity make up the escape set E_c also know as the basis of attraction of ∞ [4]. This is defined as:

$$A_f(\infty) = \{z \in \mathbb{C}\colon \left|f^n(z)\right| \to \infty\}$$

which is always open.

All other points in the complex plane are considered to be in the prisoner set P_c [7] which forms the filled in Julia set [4]

$$K_f = \{z \in \mathbb{C}\colon \left|f^n(z)\right| \not\to \infty\} = \mathbb{C} \setminus A(\infty)$$

which always contains the Julia set J_f.

The family of mappings given above is conformal and points that do not tend towards infinity and always transform back onto themselves are what make up the boundary of A_f and form J_f.[3]

2.2 Properties

2.2.1 Invariance and Symmetry

Invariance, with respect to a transformation is, given a point **P** in a fractal, the point obtained by transforming **P** will also be in the fractal.[6] More formally a set G is completely invariant under a map f if $f^{-1}(G) = G$. [11] $A_f(\infty)$ and K_f are completely invariant and as a result, so is J_f since $J_f \subseteq K_f$. It can also be observed that as a mapping Julia is conformal (all angles remain unchanged by the mapping) and transforms back onto itself[6] leaving it invariant.

Julia also has the property of being point symmetric about the origin[6], sets on the real axis are reflection symmetric and those on the complex axis display rotational symmetry.[3]

2.2.2 Self-Similarity

For a geometric object qualify as a "fractal" it must exhibit some properties. Fractals are figures based on a single repeating motif and an ever reduced scale.[6] Regardless of how zoomed in (or zoomed) out one views the geometric figure, the shape and apparent motif is identical. They can also be defined as a set of points that are invariant under a semigroup of contractions [6]. It has already been shown that J_f is invariant above.

Julia self-similar [5] and in general fragments of the set are strictly similar to the set as a whole [3]. Mandlebrot gave a strict definition of similarity [7] given a rational parameter r, positive integer N, a bounded set S of points $(x_1, x_2, \ldots, x_E)$ on a Euclidean geometric space with dimension E. S is self-similar if it is the union of N nonoverlapping subsets that are all congruent to rS.

2.2.3 Fixed Points and Strange Attractors

A periodic point is a point $z_0 \in \mathbb{C}$ such that $f^n(z_0) = z_0$ for some interger value $n \geq 1$. [10] The smallest possible n that satifies this property is called the period of z_0. These points exist between specific regions of the plane and may be called attractoring, repelling or indifferent. [9] [10] Attractors compete for influence on the plane and an initial point will be driven towards attractors by the system, else it will remain on the boundry. Similarly, a repelling point drives the initial point away while all other points are indifferent and do not affect points on the plane. The distribution of these points in the plane is commanded by the parameter c which also affects the boundaries of the given regions [9]

The Julia set is the boundary of a single domain of attraction and contains points which do not go to that attractor. [9] Julia's geometry depends crucially on the attracting period point of the mapping. [13] Julia exhibits chaotic behavior [3] and like other chaotic sysmes [7] it displays strong sensitivity to initial conditions, and periodicity.

2.3 Examples

$f(z) = z^2$	the unit circle [4]
$f(z) = z^2 - 2$	the line segment between -2 and 2

since complex numbers can be uniquely mapped into real space, a one-to-one relationship can be established between C and R [15]. To draw julia select an area of the complex plane and map it to an area A of the computer window and let one pixel represent one point in the set. [15] using the foolowing algorithms
[algorithm go here]

3 Application to Image Encryption/Decryption and Compression

Image encryption is an effective technique to protect image security. Using a variety of algorithms, images can be scrambled into into keys which, given a cipher key, can be deciphered to reveal the original image. This can be used to transfer sensitive image documents via telecommunications, satellite and the internet without the fear of third party tampering or evesdropping. Algorithms for such process usually use public key protocol system to exchange a secret key (or cipher) between two comminucators and then a secret key system to transfer sensistive data. [1]

It is possible to generate cryptographic ciphers using fractal systems. Fractal ciphers have a smaller storage cost and also input sensitivity [15] making them very difficult to crack while reducing memory needed to store encrypted information. By using the Julia set in particular to encode graphical information, images can be efficiently encrypted at high quality with superior compression when compared to other methods, like JPEG.[2] Only a few parameters are needed to generate keys using Julia [14] and the sets properties create input sensitivy making these compressed images are much more difficult to decrypt. [15]

3.1 Fractal Dictionary

Graphical images can be encoded using fractal dictionary.[15] Devised by Barnesley, an image can be partioned into non-overlapping blocks (range blocks) and further sub-divided further into overlapping blocks (domain blocks). When the image is titled by range blocks which are each mapped individually to a domain block these mappings for a transform over the entire image.

It is possible to use this transformation to compress a gray-scale image to smaller size using a method called block truncated coding [15]. This technique results in small images that do not lose information and generate artifacts during the compression process. A block can be converted to a binary value using:

$$\hat{x} = \begin{cases} 1, & x \geq x_{ave} \\ 0, & x < x_{ave} \end{cases}$$

Where x is a single pixel in a block of the image and x_{ave} is the average value of that pixel. This generates a binary matrix containing single elements $\hat{x}$. If this matrix is treated as a vector containing a binary sequence then corresponding decimal value is the BTC value allowing the image to be compressed on whatever scale we choose (based on the size of the blocks). The resulting compressed image can then be encoded and decoded using collage theorem[12] which requires an iterated function with an attractor close to some given set.

3.2 Collage Theorem

Given an image in fractal geometry Barnesleys collage theorem allows us to approximate the iterated function system associated with that image.[12] Since fractal sets generally contain an infinite number of points with varying organization, specifying each point in the set is impossible. [8]An approximating set, based on relations between the original image of the attractor, is used to find the contractive (at most one fixed point) mapping to recreate the image.

[15] explains that given a domain block of size $B \times B$ the range black size is $R \times R$ for an $N \times N$ image. There are $(N - B + 1) \times (N - B + 1)$ overlapping domain blocks and $(N/R) \times (N/R)$ non-overlapping range blocks. The scheme uses self-similarity in an image and attempts to find the most similar looking domain block that minimizes distortion. While this effective at accurated encoding an decoding a given image it is unfortunately slow computationally. A 256x256 image would require 62 001 blocks of size 8x8 which means searching would require 62001x8 comparissions per range block.

3.3 Encryption and Decryption

3.3.1 The Hilbert Curve

A two dimensional hilbert surve is draw by dividing a square evenly into four. From the center of the top-left square and a curve is drawn to the center of the bottom-left square, then to the center of the bottom-right square and finally to the center of the top right square. [14] Repeating this process over and over by continually dividing squares into four other squares and drawing in the same manner the result is a curve which fills the entire original square.

Using an RGB colour model, each pixel in an image can be represented using 8 binary digits. By scrambling this bits in each colour layer (Red, Green, Blue) along the Hilbert curve we create a stream cipher. Give A, B, C co-ordinates of an image with pixels:

$$\begin{aligned}(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)\\(b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)\\(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)\end{aligned}$$

then
$\{a_i \mid i = 2k + 1\} = a_i \wedge b_j \forall k, j \in \mathbb{Z}$
and
$\{a_i \mid i = 2k\} = a_i \wedge c_j \forall k, j \in \mathbb{Z}$

descibes how the bits are scrambled. [14] We obtain keys for encrypting and image after we scramble the Julia set by the Hilbert Curve.

3.3.2 Encoding and Decoding

To encode and send an image to a reciever, public key encryption can be used. The most common algorithm is the RSA scheme which is implemented as follows:[1]

The reciever generates a key by secretly chooses two distinct prime number (p, q) that are similar in size. They then compute n (modulus) as $p \times q$ and $\phi(n) = (p-1) \times (q-1)$. Next they choose the public key e such that $1 < e < \phi(n)$ and $GCD(e, \phi(n)) = 1$. Their decryption key is then $d = e^{-1} \mod \phi(n)$. Finally, they determine the public keys (e, n) and the private keys $\phi(n), d)$.

The sender must obtain the public keys (e, n) and determine the message m to be encoded under the condition that $0 < m < n$, they encode the message as $c = m^c \mod n$ and send c to the reciever.

The reviever can then decrypt the message they recieve using $m = c^d \mod n$

Given a Julia scrambled image, the above methodology can be applied to encode an image pixel by pixel using:

$$e'_{ij} = (e_{ij} + d_{ij}) \mod l$$

where e_{ij} is the pixel value of (i, j), e'_{ij} is the pixel value following encryption, l is the number of colours in the image and d_{ij} is the pixel value in the keys obtained from scrambling Julia along the Hilbert Curve. [14] The reciever can then decrypt the given image using the reverse operation:

$$e_{ij} = (e'_{ij} - d_{ij}) \mod l$$

3.4 Examples

4 Conclusion

a conclusion goes here

References

[1] M. A. Alia and A. B. Samsudin, *A new public-key cryptosystem based on mandlebrot and julia fractal sets*, Asian Journal of Information Technology, 6 (2007), pp. 567–575.

[2] K. J. Balashov, *Fractal compression*, Apr 2015. http://cotty.16x16.com/compress.

[3] G. Elert, *Strange & complex*, Apr 2015. http://hypertextbook.com/chaos/22.shtml.

[4] J. E. Fassett, *Eigenvalues in filled julia sets*, Mathematics Magazine, 84 (2011), pp. 221–227.

[5] M. Frame, B. Mandlebrot, and N. Neger, *Fractal geometry*, Apr 2015. http://classes.yale.edu/fractals/MandelSet/welcome.html.

[6] H. Lauwerier, *Fractals Endlessley Repeated Geometrical Figures*, Princeton University Press, 1991.

[7] M. McGoodwin, *Julia jewels: An exploration of julia sets*, Apr 2015. http://hypertextbook.com/chaos/22.shtml.

[8] S. Nikiel, *Iterated Function Systems for Real-Time Image Synthesis*, Springer London, 2007.

[9] H. Peitgen and R. P.H., *The Beauty of Fractals*, Springer-Verlag Berlin Heidelberg, 1986.

[10] M. Shishikura, *Topologocal, geometric and complex analytic properties of julia sets*, International Mathematical Union Proceedins 1994, 9 (1994), pp. 886–895.

[11] B. Solomak, *Additional facts about julia sets*, Apr 2015. http://www.math.washington.edu/ solomyak/TEACH/435/Julia.pdf.

[12] unknown currently, *Collecting between the collage theorem and the optimization method to solve inverse problem of fracal image*, Journal of Kerbala University, 6 (2008), pp. 256–259.

[13] J. Yang, *Properties of julia sets*, Apr 2015. http://www.emba.uvm.edu/ jxyang/teaching/Math266notes10.pdf.

[14] S. Yuanyuan, X. Rudan, K. Ruiquin, and L. Chen, *An image encryption algorithm utilizing julia sets and hilbert curves*, PLoS ONE, 9 (2014), p. e84655.

[15] S. Yuanyuan, X. Rudan, and H. Xiaopeng, *Image compression and encryption scheme using fractal dictionary and julia set*, IET Image Processing, 9 (2015), pp. 173–183.