

**Proceedings of
IX Congreso del Máster
en Investigación Matemática**

Facultad de Matemáticas, Universitat de València,
January 25th - 26th, 2022

This book contains the contributions of the IX Congreso del Máster en Investigación Matemática.

I.S.B.N.: 978-84-09-43171-7

January 25th - 26th, 2022

Report any problems with this document to imm@imm.upv.es.

Edited by:

- J.R. Torregrosa (Universitat Politècnica de València)
- M^a Carmen Martí (Universitat de València)
- A. Vidal-Ferràndiz (Universitat Politècnica de València)

investmat



VNIVERSITAT
DE VALÈNCIA



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Contents

Applications of fractals, for image compression and realistic terrain generation <i>Cayetano Manchón Pernís</i>	1
Applications of fractals, for image compression and realistic terrain generation <i>Emilia Giulia Tersigni</i>	8
Fractals everywhere? <i>Fernán González Ibáñez</i>	16
Introduction to set theory <i>Adrián Fidalgo Díaz, José Alejandro Serón Rodrigo and Marc Tomás Martínez</i>	21
A fuzzy system to improve image denoising method <i>Khleef Almutairi and Samuel Morillas</i>	27
Three mathematical modelling of the glucose-insulin process for Type 1 Diabetes patients. Control and numerical results. <i>Marcos Llamazares López, Alberto Pérez Galende and Álvaro Vargas Moreno</i>	33
Graph Neural Network Convolutions: mathematical principles and an application to chemistry <i>Enric Alberola Boloix, Pablo Merino San José and Ángel Rolando</i>	45
Cryptographic systems: a mathematical review <i>Pérez-Diukina, C., Sabater-García, P., and Zaragoza-Chichell, J.</i>	50
Partial Differential Equations in Random Walk Spaces <i>Álvaro González Cortés, Daniel Isert Sales and Eduardo Sena Galer</i>	54

Applications of fractals, for image compression and realistic terrain generation

Cayetano Manchón Pernis ^b

(b) tano@tano.xyz

1 Introducción

Fractals and the theory on which they are based can be used for different applications, for example, using the self-similarity properties of fractals we can develop image compression methods, on the other hand, we can also take advantage of their great resemblance to elements of nature to generate realistic terrain for video games or animation. We will discuss these two applications and show the results obtained.

2 Image compression

Fractals can be used for lossy image compression [10] [9], this kind of compression assumes a loss of information when compressing the image under a certain tolerance level, i.e., you cannot get exactly the same image you compressed.

The idea comes from dividing into range blocks and domain blocks, the range blocks must not overlap and must cover the whole image, the domain blocks can overlap and do not have to cover the whole image. From here it is necessary to find a set of contractive affine transformations over the domain blocks to generate all the range blocks.

This search can be very computationally expensive, for this reason, the type of contractive mappings to be tested and the number of possible domain blocks are usually limited. With that in mind a possible solution of the problem would be:

- We divide the image in range blocks, note that these blocks are the ones that will form the final image once decompressed, to save information it is important that the codification of each transformation occupy less memory than each block, for example, we can take blocks 8×8 , if the image is 512×512 we will obtain a total of $64 \times 64 = 4096$ blocks.
- We divide the image in a list of all the possible domain blocks that we are going to consider, for example we consider 16×16 blocks allowing overlapping between them, with a 512×512 image we can obtain $497 \times 497 = 247009$ blocks.
- Then we test the contractive transformations between the range blocks and the domain blocks, note that we always apply the same contraction, we scale by 0.5 each domain block. With this in mind, for each range block, we look for the domain block that most closely resembles it after applying the transformation. Note that we can also test different orientations to find better matches.

- After this we have a list of domain blocks and contractive mappings that can be used to reconstruct the original image.

We can start from an arbitrary image from which we obtain the initial domain blocks and apply iterated transformations until the original image is obtained.

2.1 Results

We have made a variation of the previous algorithm and applied the compression to an image in order to analyze the results.

Our implementation of the algorithm [11] consists of dividing the image into range blocks just as previously explained and then search in the same image for the most similar one but with two times the size, if one is found, this range block is removed from the image and added as a transformation. We apply this iteratively until we finish with all the Range Blocks, finally we will have obtained a fragment of the original image that we will be able to reconstruct if we apply the transformations in the inverse order to how we obtained them.

In the images 1, 2 we can see the results of compression and decompression when applying the mentioned algorithm and in the images 3, 4 the same but increasing the tolerance when comparing the blocks, we can appreciate a higher compression ratio at the cost of a loss of quality, we could also test different types of contractive mappings which would increase the quality at the price of increasing the computational cost.

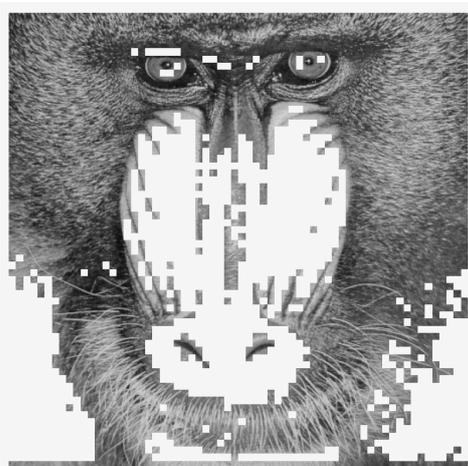


Figure 1: Image compressed

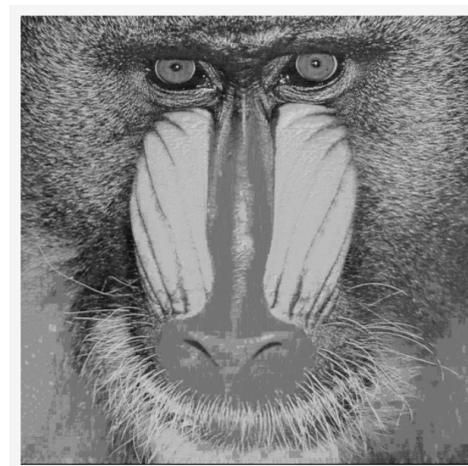


Figure 2: Image decompressed

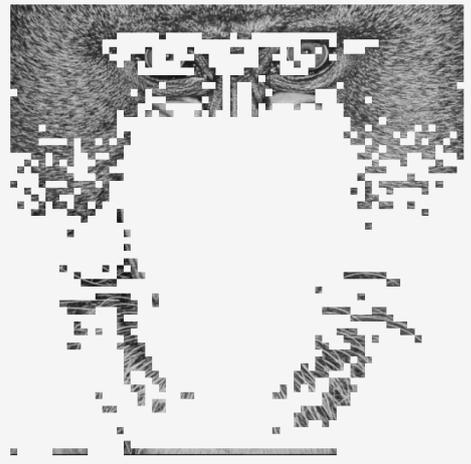


Figure 3: Image compressed high tolerance

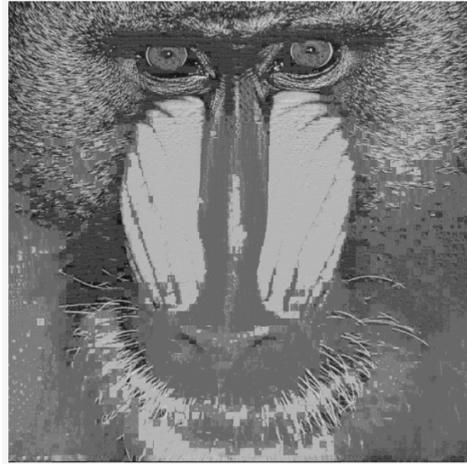


Figure 4: Image compressed high tolerance

3 Procedural terrain generation

Fractals are commonly used in computer graphics for the procedural terrain generation [6] [5]. For this purpose, height maps are generated, they are 2-dimensional grids that store in each cell how high that particular point should be. The reason for using fractals is that fractional Brownian motion, which is also often called $1/f^\beta$ type noise, has a strong resemblance to the structure of mountains.

We will use the fractal dimension, D_f given by D_e the Euclidean dimension and H as the holder exponent, this relates to the noise $1/f^\beta$ as follows:

$$D_f = D_e + 1 - H = D_E + \frac{3 - \beta}{2}$$

In order to preserve the fractal properties it must be satisfied that:

$$H \in (0, 1) \quad \beta \in (2, 3)$$

The H maps directly to the roughness of the terrain, increasing roughness as H approaches 0 and increasing smoothness as H approaches 1.

We will discuss two well known algorithms for fractal terrain generation, "Midpoint displacement" and "Noise synthesis".

3.1 Midpoint displacement algorithm

The idea of the algorithm in 1D consists of, first we give fixed values to the extremes of the height map, then we take the midpoint and its new value will be the interpolation between its extremes plus a random offset using a Gaussian distribution, in the next iteration we take two new midpoints, interpolate and add the offset, we repeat this until the height map is complete. The key point is that at each iteration the random offset is calculated by:

$$\text{rand}(\text{minh}, \text{maxh}) \times (1 - H)^{\text{iter}}$$

Where $\text{rand}(\text{minh}, \text{maxh})$ refers to obtaining the random value between the interval $(\text{minh}, \text{maxh})$ and iter refers to the current iteration.

In figures 5, 6, 7 and 8 generated from our implementation [12] we can see the evolution of the algorithm.

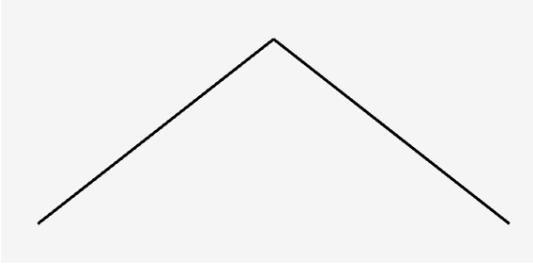


Figure 5: 1 subdivision

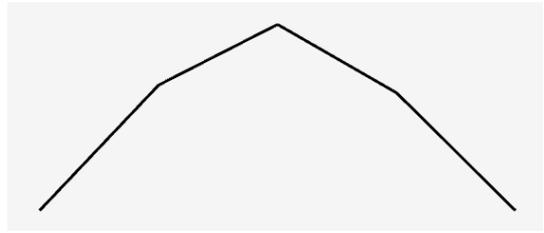


Figure 6: 3 subdivisions



Figure 7: 7 subdivisions

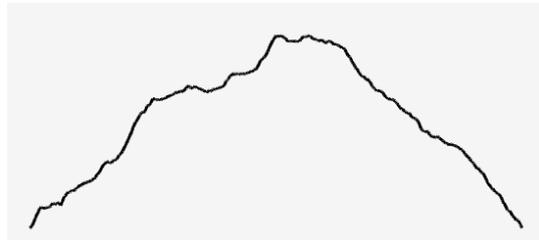


Figure 8: 1023 subdivisions

This is good, but to do it in 2D "displacing the midpoint" is not that obvious, in order to apply this idea to surfaces we use the diamond-square algorithm [2] [3] [4] that selects intermediate points of the height map in a robust way.

As you can see in the figure 9 first we put fixed values to the corners, then for each square with values already set we take the midpoint and give as value the average of the four corners plus the random offset (this is the diamond step), for each diamond with values we take the midpoint and give as value the average between the four corners plus the random offset (this is the square step), repeat these two steps until the height map is complete.

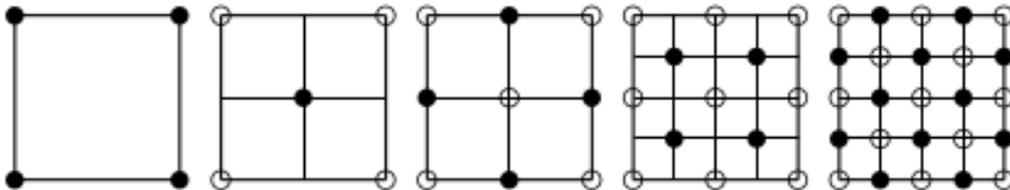


Figure 9: Square diamond algorithm [5]

In figures 10, 11 and 12 generated from our implementation [12], we can see the results and how varying the H parameter affects the smoothness of the terrain.

3.2 Noise synthesis algorithm

The Midpoint Displacement algorithm gives good results but has certain limitations, its recursive nature and the need to know the global state of the height map to complete it makes it an inefficient algorithm at large scales.

On the other hand, Noise Synthesis [6] is a purely functional algorithm that enables you to obtain the height of a point x,y without the need of having a global knowledge of the map. This allows you to generate height maps of indeterminate size in a parallel way.

To learn about this method we must first introduce several concepts. **Noise function**, is a

Figure 10: Midpoint $H = 0.40$ Figure 11: Midpoint $H = 0.50$ Figure 12: Midpoint $H = 0.60$

random continuous map defined as: $f : \mathbb{R}^2 \rightarrow Y$ with $Y = (-1, 1)$. **Octaves** the number of examples of noise functions used. **Lacunarity** the frequency variation in each octave.

The idea is to start with a noise function, Perlin Noise [1] is a good function to generate terrain, and add octaves whose frequency varies according to the lacunarity and its amplitude according to the H .

Being L the lacunarity, and N the total number of octaves. The function can be expressed as follows:

$$\text{NoiseSynth}(x, y) = \sum_{n=0}^{N-1} (\text{noise}(x \times L^n, y \times L^n) \times (1 - H)^n)$$

In the figures 13, 14, 15, 16, 17 generated from our implementation [12], we can see the results obtained by varying some of the parameters, H affects the result as expected, and as we increase the number of octaves or we increase the number of octaves or the lacunarity the roughness increases.

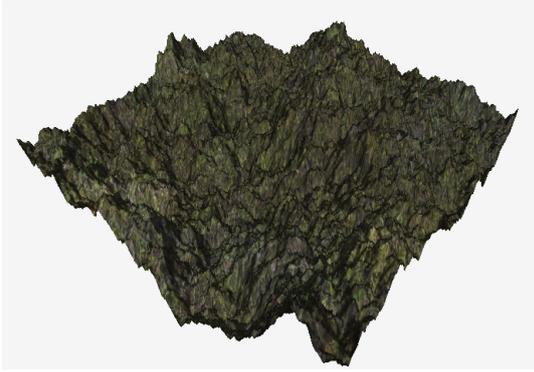


Figure 13: Noise syntethesis with $octaves = 12$, $lacunarity = 2.0$ and $H = 0.40$



Figure 14: Noise syntethesis with $octaves = 12$, $lacunarity = 2.0$ and $H = 0.50$



Figure 15: Noise syntethesis with $octaves = 12$, $lacunarity = 2.0$ and $H = 0.60$



Figure 16: Noise syntethesis with $octaves = 6$, $lacunarity = 2.0$ and $H = 0.50$



Figure 17: Noise syntethesis with $octaves = 6$, $lacunarity = 2.5$ and $H = 0.50$

4 Conclusions

We have seen the usefulness of fractals in solving real-world problems, looking for fractal shapes in problems and finding the mathematical way to fit them there. Both image compression and terrain generation are very broad fields where a wide variety of algorithms can be created using fractals to solve problems, each with its advantages and disadvantages.

References

- [1] Perlin, K. An image synthesizer. *ACM Siggraph Computer Graphics*. **19**, 287-296 (1985)
- [2] Koh, E. & Hearn, D. Fast generation and surface structuring methods for terrain and other natural phenomena. *Computer Graphics Forum*. **11**, 169-180 (1992)
- [3] Sala, N., Metzeltin, S. & Sala, M. Applications of mathematics in the real world: Territory and landscape. (2002)
- [4] Fournier, D. & Carpenter, L. Computer Rendering of Stochastic Models, Graphics and Image Processing, Editor J. Foley. *Doi*. **10** (1982)
- [5] Olsen, J. Realtime procedural terrain generation. (2004)
- [6] Musgrave, F., Kolb, C. & Mace, R. The synthesis and rendering of eroded fractal terrains. *ACM Siggraph Computer Graphics*. **23**, 41-50 (1989)
- [7] Chiba, N., Muraoka, K. & Fujita, K. An erosion model based on velocity fields for the visual simulation of mountain scenery. *Journal Of Visualization And Computer Animation*. **9** pp. 185-194 (1998)
- [8] Fisher, Y., Jacobs, E. & Boss, R. Fractal image compression using iterated transforms. *Image And Text Compression*. pp. 35-61 (1992)
- [9] Barnsley, M. & Others Fractal image compression. *Notices Of The AMS*. **43**, 657-662 (1996)
- [10] Lacroix, B. Fractal image compression.. (Carleton University,1999)
- [11] Pernis, C. Implementation of image compression experiments. (2021), <https://github.com/cmp102/fractal-image-compression>
- [12] Pernis, C. Implementation of procedural terrain generation experiments. (2021), <https://github.com/cmp102/fractal-terrain>

Applications of Mathematics in Epidemics

Emilia Giulia Tersigni ^b,

(b) eter@alumni.uv.es

1 Introduction

Broadly speaking, a model is an abstract representation of selected aspects of reality. Certain parameters are isolated and their relationships are studied in order to capture the pattern of a natural phenomenon, on which, among other things, forecasts are intended to be made.

Each model serves a special purpose in a specific period; from certain assumptions and based on a set of data, it gives a result with a certain level of confidence. Models are not a tabula rasa, there is information that is assumed to be (approximately) true and that is not constantly made explicit. Exemplarily, the transmission rate or the immunity lapse are assumed once they are unknown. Data are the inputs, the primary elements of the models, so the better quality they are, the better results they are likely to report. For example, records of hospitalised coronavirus deaths are more accurate than those of (probable) coronavirus deaths, since in the former case the records are one-to-one with the truth, whereas in the latter case there is at least an under-recording of those who died in their homes without any evidence. In addition to answering the key questions we have indicated, epidemiological models need to be tested. Every model is evaluated before it is put into operation, we may mention that the success of a model is measured by its experimental adequacy: good models are those that make realistic predictions, let us say the closest to the truth.

2 SIR model

In this section we will analyze the classic Kermack and Mc-Kendrick model (for more details see [1]) a SIR-type model, by dividing the population of people attacked by the virus into three classes.

We will start with class S which corresponds to the group of individuals susceptible to a communicable disease. These individuals do not have immunity to the infectious agent so they may become infected if exposed. The second class, denoted by I , represents the group of infected individuals who are capable of transmitting the disease to susceptible persons with whom they come into contact. Finally, class R represents individuals who have or have had the infection and who become immune to the disease or die, and as a consequence these individuals do not affect the dynamics of disease transmission when they come into contact with other people.

The model presented here is based on the following assumptions (see [4]):

The population to be considered in this model is constant and its size is equal to N , that is, the same birth and death rates will be considered throughout the process of spread of the disease,

since the duration of an epidemic is short. The immigration and emigration of the population will not be estimated, that is, the population will be considered closed. The latency period from the instant of exposure to that at which the person becomes infectious is small enough not to be taken. Infectious individuals will leave their class at a constant rate γ to belong to the recovered class.

2.1 Ordinary differential equations of the model

This subsection is based on [3, 4].

According to the previous assumptions we will present the differential equations that model an epidemic, based on the division that was made (N, S, I, R), as shown in Figure 1 that represents the model diagram.

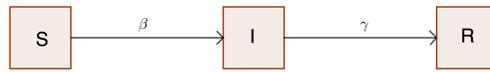


Figure 1: Diagram of SIR model

The number of susceptible individuals that become infectious is proportional to the product of the number of susceptible individuals by infectious individuals, that is, the rate of loss of susceptible individuals is βSI . Thus we obtain the first equation that describes the susceptible individuals.

$$S'(t) = -\beta S(t)I(t),$$

the negative sign indicates the loss of susceptible individuals.

$\beta S(t)I(t)$ further suggests the rate of gain of infectious persons, and represents the rate of gain of recovered persons, that is, I suggests the output of the infectious class, thus we obtain the differential equation for the infected.

$$I'(t) = \beta S(t)I(t) - \gamma I(t),$$

and the equation describing the recovered is,

$$R'(t) = \gamma I(t),$$

since it suggests exit from the infectious class with a positive γ rate.

Considering that total population N was divided into *Susceptible*, *Infectious* and *Recovered*, we have that $N = S(t) + I(t) + R(t)$.

From the above we obtain the following system of equations (1) which is known as the classical Kermack and Mc-Kendrick model.

$$\begin{cases} S'(t) = -\beta S(t)I(t), & S(0) = S_0 \\ I'(t) = \beta S(t)I(t) - \gamma I(t), & I(0) = I_0 \\ R'(t) = \gamma I(t), & R(0) = R_0, \end{cases} \quad (1)$$

3 Modifications made to the model to describe successive waves of COVID-19

In this section we will analyze whether SIR-type model is able to make accurate predictions about the course of diseases such as COVID-19 (for more details see [2]).

3.1 Can the SIR model predict successive waves of COVID-19?

Looking at the model assumptions, neither births nor deaths are considered, not even those produced by the infection under study. Furthermore, the fact that β and γ are constant does not reflect the effect of realistic measures such as social distancing or scientific breakthroughs. Figure 2 shows how far the classical SIR model is from modeling correctly the course of COVID-19 in a specific territory.

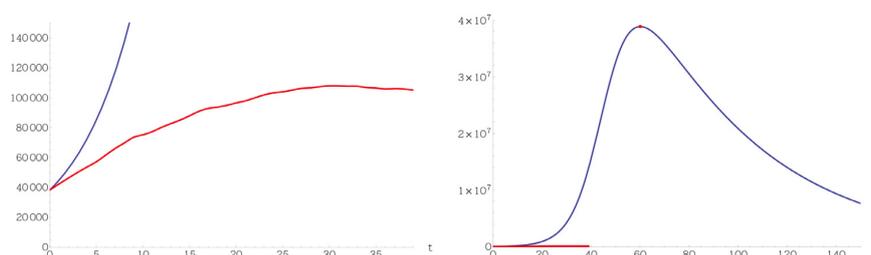


Figure 2: In these graphs we have depicted in red the evolution of active cases of COVID-19 in Italy between the 20th of March 2020 (zero in the horizontal axis) and the 29th of April 2020 (tick 39 in the horizontal axis). In blue we have depicted the evolution predicted by the classical SIR model calibrated with the data released by the Italian authorities on the 20th of March 2020. It can be clearly seen that the classical SIR model is not an adequate tool to model this pandemic.

In the following we will look at a mathematical model that maintains the simplicity of the classical SIR model, but at the same time predicts with a considerable accuracy the evolution of COVID-19 under certain reasonable assumptions. The model is tested with the official data regarding the course of COVID-19 in Italy and Spain.

The model will be a non-independent SIR-type model with vital dynamics, non-constant population and exponentially decaying infection and death rates to model the expansion of the COVID-19 in various territories, focusing on 2 of the most affected by this pandemic disease. It is calibrated according to the data gathered in a period of time that includes at least 30 days, beginning at least 10 days after the declaration of either partial or total lockdown.

The model we recommend here is based on two sets of assumptions. The principles of the first set outline the equations of the model. We consider in essence a SIR model with vital dynamics with the following characteristics:

- (a) Neither the transmission rate β nor the death rate μ' due to COVID-19 are constant in our model. The accessible official data in the countries studied suggest that in the early stages of pandemic disease in countries with strict control on social distancing, both β and μ' decay exponentially (see, for example, Figures 2 and 3) to their baseline values β and μ' respectively. This would possibly be due to the fact that the evolution of the variables is still a transient and therefore some time is required until the parameters reach their asymptotic values.

- (b) We consider a recuperation rate γ that is not necessarily constant either. Although the observed values of γ are somehow stable in the three territories studied, the monthly variations of γ generate significant changes in the main epidemiological parameters. The way in which we chose the values of γ is explained in the set of principles that give the calibration of the model.
- (c) We consider the existence of a constant birth rate $\lambda > 0$ that is the same for all three categories S , I and R . We further assume that all the descendants are born free of infection, but without immunity.
- (d) Finally, we consider the existence of a constant death rate $\mu > 0$ due to death reasons other than COVID-19.

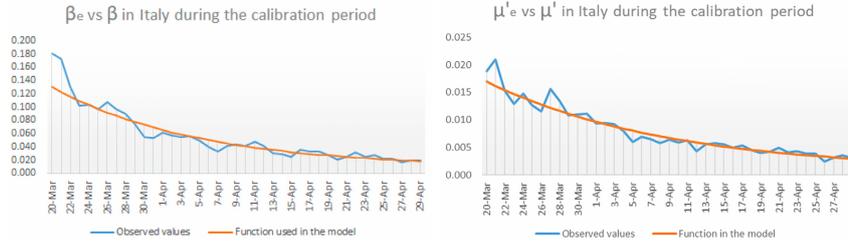


Figure 3: In the left, representation of β_e and β for Italy during the calibration period. In the right, representation of μ'_e and μ' for Italy during the calibration period.

The above assumptions produce the following relationship among the variables S , I , R :

$$\begin{cases} S'(t) = (\lambda - \mu)S(t) + \lambda(I(t) + R(t)) - \beta S(t)I(t), \\ I'(t) = \beta S(t)I(t) - \gamma I(t) - \mu' I(t) - \mu I(t), \\ R'(t) = \gamma I(t) - \mu R(t). \end{cases} \quad (2)$$

The second set of hypotheses defines how the parameters β , μ' , γ , λ and μ have to be chosen, or in other terms, the way the model should be calibrated:

- (a) The values of λ and μ are provided in Table 1 ([2]).
- (b) As mentioned above, although the observed monthly mean values of the recovery rate γ are fairly stable in all the territories studied, it should not be assumed that γ is necessarily constant. When data from Italy and the United States are examined in relation to mortality and recovery, variations in rates are noted until asymptotic values are reached. However, we assume that γ is constant during each calendar month or along the calibration period for each country. The values assigned to γ are based on the observed monthly mean values of γ . Commonly the values of γ turn out to be very uniform, with quite a few exceptions, such as the months of May and June in Italy, with values that are twice as big as in the other months studied.
- (c) With regard to the determination of β and μ' we have seen a significant drop in the infection and mortality rate in the official data published by the authorities of the three territories studied. The functions β and μ' are defined by means of an exponential regression on the official data. It should be mentioned that, according to the actual data, mortality

approaches its asymptotic value in a relatively short period of time. This is consistent with the assumption that major changes, such as novel control policies or a sudden change in sociological behavior have the potential to produce a transient state in which the model parameters have the potential to change until they approach their baseline values.

It is essential to specify that we have run this model using the normalized variables:

$$S_N(t) = \frac{S(t)}{N}, \quad I_N(t) = \frac{I(t)}{N}, \quad R_N(t) = \frac{R(t)}{N},$$

where $N = S + I + R$ is the total population. In this new variables the model would be

$$\begin{cases} S'_N(t) = (\lambda - \mu)S_N(t) + \lambda(I_N(t) + R_N(t)) - \beta S_N(t)I_N(t), \\ I'_N(t) = \beta S_N(t)I_N(t) - \gamma I_N(t) - \mu' I_N(t) - \mu I_N(t), \\ R'_N(t) = \gamma I_N(t) - \mu R_N(t), \end{cases} \quad (3)$$

where the parameters $\lambda, \mu, \beta, \mu'$ and γ are all normalized.

We assume that the initial population of the nations under analysis is the population they had in 2018.

In order to asses the precision of the model, we have compared the reported active cases $I_e(t)$ and the model's outcome for $I(t)$ during the 40-day calibration period in Figure 4.

When we have $\beta(t)$ and $\mu'(t)$ for Spain for a defined choice of β_0 and μ' we perform a 37 day simulation of the model and compare the result with the reported data. Note that cumulative deaths here are counted from 24 March, not from the beginning of the pandemic disease.

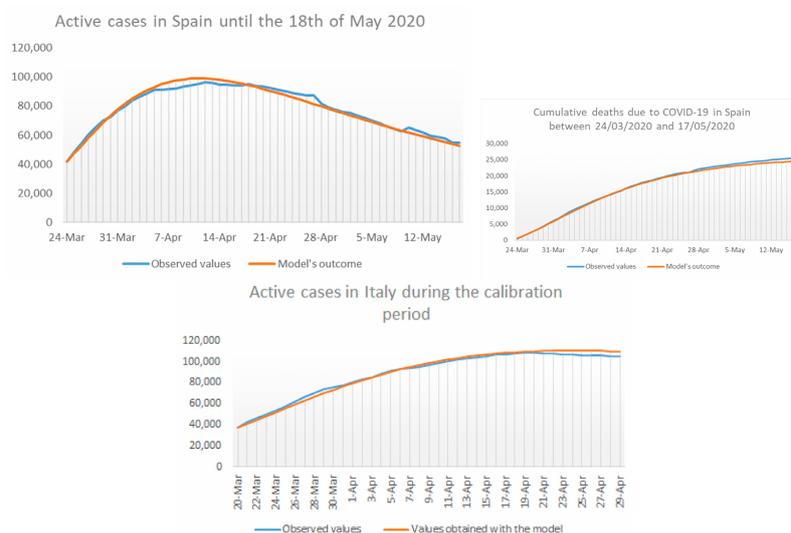


Figure 4: In the left, representation of the daily number of reported active cases in Spain $I_e(t)$ compared with the model's outcome $I(t)$. In the right, representation of the deaths by COVID-19 in Spain from March 24th until May 17th, 2020. Here $D_e(t)$ appears in blue whereas $D(t)$ is shown in red. On the bottom, representation of the daily number of active cases in Italy $I_e(t)$ compared with the model's outcome for $I(t)$ during the calibration period, from 20/03/2020 to 29/04/2020.

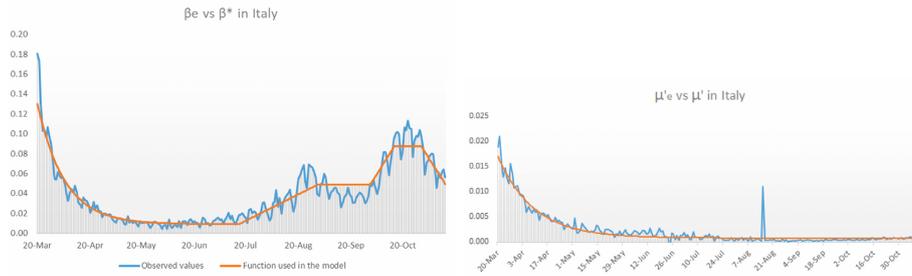


Figure 5: In the left, comparison of the transmission function $\beta^*(t)$ used in the model and the observed values of $\beta_e(t)$ until mid November 2020. In the right, comparison of the death rate function $\mu'(t)$ used in the model and the observed values of $\beta_e(t)$ until mid November 2020.

In the Italian situation we have the possibility to look at a slight but steady increase in the values of $\beta_e(t)$ from July onwards (see blue graph in Figure 5).

The function $\beta^*(t)$ is depicted in Figure 5 in red, together with $\beta_e(t)$.

The accuracy of the model's outcomes with $\beta(t)$ replaced by $\beta^*(t)$ is shown Figures 6.

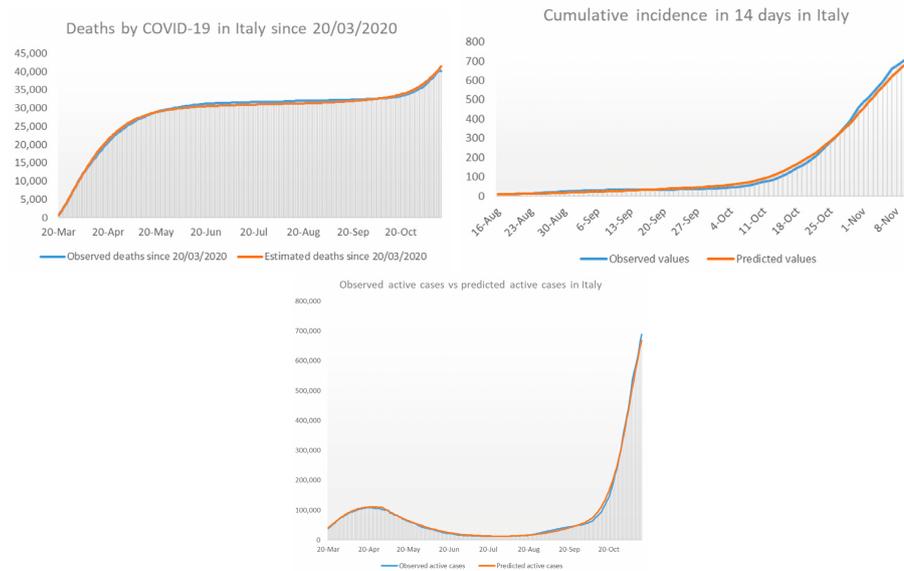


Figure 6: In the left, the number of deaths by COVID-19 in Italy since the 20th of march compared with the deaths predicted by the model. In the right, comparison the observed cumulative incidence in 14 days per 100,000 inhabitants in Italy since mid August with the values predicted by our model. On the bottom, comparison of the model's outcome for $I(t)$ and the observed values $I_e(t)$ of active cases in Italy until mid november 2020.

Running the model with $\beta^*(t)$ the outcome for cumulative incidence in 14 days per 100,000 inhabitants and the real reported incidence have been sketched in Figure 7.

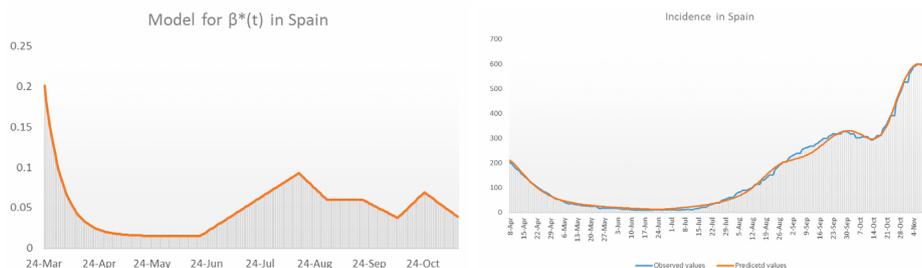


Figure 7: In the left, heuristic construction of the transmission function $\beta^*(t)$ for Spain during the second surge. In the right, we show the cumulative incidence in 14 days per 100,000 inhabitants in Spain obtained with our model compared with real cumulative incidence data.

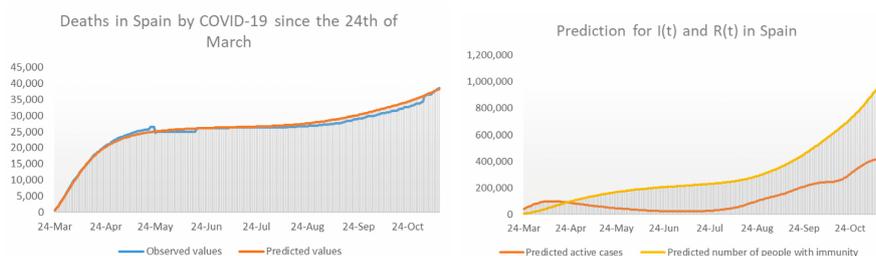


Figure 8: In the left, real data of cumulative deaths by COVID-19 are compared with the model outcome for cumulative deaths since the 24th of March. In the right, estimated values of active cases and people with immunity in Spain between the 24th of March and mid November 2020.

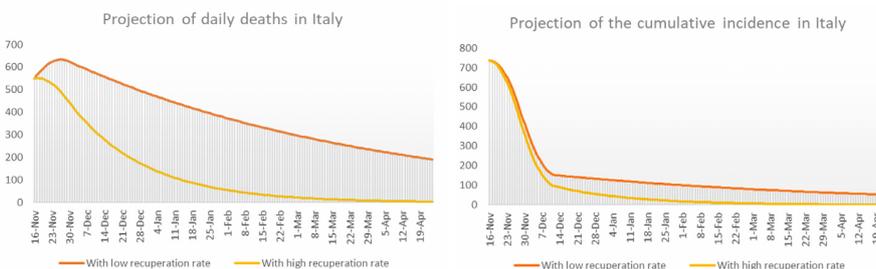


Figure 9: In the left picture we have a projection on the daily number of deaths in Italy starting in mid November 2020. In the right we have a projection on the cumulative incidence in 14 days per 100,000 inhabitants in Italy starting in mid November 2020.

4 Results

In this paper we have observed that the course of coronavirus in 2 territories, Italy and Spain, can be modelled by means of a simple SIR-type model with non-constant parameters. The limits, after a transient state, tend to approach their asymptotic values. In other words, especially true for the mortality rate μ' and the recovery rate. The transmission rate also shows a tendency to approach its asymptotic value, but is sensitive to sociological changes, such as increased mobility, a relaxation of social distancing and the massive use of protective equipment such as masks. We have shown that a correct choice of transmission capacity makes it possible to obtain quite realistic

results. Using the model, we have also been able to make some predictions for the situation in Italy. These predictions are quite negative even in the best-case scenario, which should serve as a motivation to redouble everyone's efforts.

5 Conclusions and discussion

Explanatory mathematical models of infectious diseases are intended to allow to predict the evolution of the disease considering a wide range of possible scenarios. In this paper we propose a mathematical model to study the current transmission dynamics of SARS-CoV-2. We tested the model using registered cases and population data from Spain and Italy. The model is able to predict others wave of the pandemic.

References

- [1] KERMACK, W.O.; MCKENDRICK, A.G., *A contribution to the mathematical theory of epidemics*, Proceedings of the Royal Society of London. Series A **115(772)**, (1927), pp. 700-721.
- [2] MUÑOZ-FERNÁNDEZ, G.A.; SEOANE, J.M.; SEOANE-SEPÚLVEDA, J.B., *A SIR-type model describing the successive waves of COVID-19*, Chaos, Solitons, Fractals **144**, (2021).
- [3] PLIEGO, E.C., *Modelos epidemiológicos de enfermedades virales infecciosas*, Benemérita Universidad Autónoma de Puebla, Puebla, 2011.
- [4] SÁNCHEZ, G.F.; MIRAMONTES, P.; GUTIÉRREZ, J.L., *Clásicos de la Biología Matemática*, 1st edition, Siglo XXI, 2002.

Fractals everywhere?

Fernán González Ibáñez [‡]

(‡) gonifer@alumni.uv.es

1 Are fractals real ?

Do fractal structures exist in real world? The first idea which came to our minds is "yes". We have seen the books from Benoit Mandelbrot "*Fractal Objects*" or "*The Fractal Geometry of Nature*" [1] or the thousands of articles which have the name "fractal" in the title but if we see the definition of Hausdorff measure, how do they know if an object is a fractal?

Mandelbrot in his book *The Fractal Geometry of Nature* states that fractal patterns are present in a lot of fields of science but not in all of them. Mandelbrot also said that fractals must have a high order of self-similarity, such as the fractality in metal fractures which can be measured with more than 5 magnitude order [2], not less than 3 in a lot of articles, such as Avnir *et al.* showed [3].

1.1 Geography

Since the birth of the concept of fractals, they have been have been linked to the orography of the terrain. From rivers to coasts, all the elements that nature has shaped has irregular patterns [6] [5]. As previously, mentioned the idea of fractal object was born measuring the coast of Great Britain as a law of powers: $Length(G) = M \cdot G^{1-D}$ where M is a positive constant, G is the length of the straight segment while Length(G) is the length of the full coast measured with straight lines of length G and D is the fractal dimension least equal the unit. In the case of Great Britain coast $1 - D = -0.25$ therefore $D = 1.25$ but in the case of the South African coast $D = 1.04$. [8]

Meanwhile, Mandelbrot in 1961 also hypothesised that rivers have a fractal dimension of 1.2. This idea was based on the work of M. Gray in 1961. This work reported that there was a relationship between the length and the area of a river given by the following expression $L(R) = 1.4 \cdot A^{0.568}$ [7]. Mandelbrot took this work and approximated the fractal dimension multiplying the exponent by two. This idea was wrong. Later in 1988 David G. Tarboton *et al.* published an article stating that the fractal dimension of the rivers are nearby 2, in some cases upper like Souhegan rive in New Hampshire which fractal dimension is 1.8 while Squanacook also in New Hampshire has 2.5 [9]. Later in 1996 Montgomery showed that the fractal dimension was correlated with the sinuosity of a river and the environment [10].

Fractal dimension can be seen in geography as the complexity of a geographical feature such as the the coast, the border between two countries or the sinuosity of a river. However, this number should never be taken as a proof of the fractality of the geographical feature.

1.2 Economy

In Economy exists a hypothesis about the behaviour of the markets called Fractal Market Hypothesis (FMH). This hypothesis states that analysing financial time series is based on fractal geometry, specifically the self-affine properties of stochastic fields. There exists other hypothesis about the behaviour of the markets based on mathematical concepts such as the Random Walk or Efficient Market Hypotheses [11].

The Fractal Market Hypothesis was born in the 1990s with the work of Edgar Peters [11]. This idea was previously hypothesised by Mandelbrot in his book "*The fractal geometry of nature*" but he was not the first to come up with this idea. In 1938 Nelson Elliot had already observed the self-affinity in the financial time series data [12].

This hypothesis is supported by multiple articles such as the work of Takayuki Mizuno et al. analysing the foreign exchange data of USD-JPY for 13 years where they found out that the fluctuation of the foreign exchange of USD-JPY has the self-similarity property in long terms. However, the self-similarity disappears when the window is small. The fractal dimension of the foreign exchange data of USD-JPY is nearby 1.7 [13]. The FMH is supported by the article of Skjeltorp, where the Norwegian stock market is studied and it undermines the random walk hypothesis [14].

1.3 Biology

As previously mentioned, nature is irregular and depends a lot of the weather, the environment ... But the growth of some fruits such as broccoli or cauliflower has self-similar property but is the statistical one. Nevertheless, this self-similarity of this fruits is not regular, given the radius and the number of number of branches per node can obtain pretty different results. This statement is a counterpoint to fractal theory, although in the article of Grey and K. Kjems refuted the hypothesis of Broccoli and Cauliflower has fractal structure. However in this article the authors presented the other hypothesis of diffusion-limited aggregation [15]. Nowadays the variants of broccoli or cauliflower, such as Romanesco Minaret, have a higher statistical self-similar structure.

Also fractal behaviour is present in the growth of bacterial, as shown in the article of Obert *et al.* [16]. In this article, they study the growth patterns of two microbial species but they may give rise to some doubts about the fractal structure of this growth and about the difference between this patter and the one generated by diffusion-limited aggregation.

Therefore it can be concluded that living organisms have power-law-like growth. This hypothesis was discarded by Panico and Starling where they stated that retinal neurons and vessels are not fractals they are just space-fillings curves or in the work of Grey *et al.* natural patterns are diffusion-limited aggregation [[15], [20]].

1.4 Cosmology

The large-scale distribution of matter in the universe, similar to a Gruyère cheese with its large voids and cheese zones, is called the cosmic web. The early work of John Peebles estimated a constant fractal dimension of $D = 1.23 \pm 0.04$ [18]. We now know that this fractal dimension is scale-dependent. The cosmic web has a multifractal structure. Jaan Einasto *et al.* published an estimate of the effective fractal dimension $D(r) \leq 3$ observed in the SDSS galactic catalogue, the cosmic simulations Millennium and EAGLE, and the prediction of the LCDM cosmological model [17].

The effective fractal dimension of a random distribution of galaxies is $D = 3$, the distribution of galaxies near the voids of the cosmic web leads to $D = 2$, in these walls a filamentary distribution

is observed with $D = 1$; finally, within galactic clusters a point-like distribution is found with $D = 0$. Thus, the change of $D(r)$ with distance r , in units of Mpc/h^1 , allows us to determine the scale of each of these structures. At small scales $D(0) = 1.5$, as predicted by the LCDM model; this value decreases to a minimum $D(0.8) = 0$; then grows to $D(3) = 2$; and finally continues to grow to $D(100) = 3$, at the largest distances considered. [19]

1.5 How fractals are measured?

Since the idea of fractals was sketched by Benoit Mandelbrot in late 60's based on the idea of Fry Richardson [6]. The idea of fractal have been applied in many fields of sciences as it haven been seen in the previous section. In that context the measure of the fractal dimension have been the main goal. To achieve this objective there are a family of algorithms which are based on the idea of Minkowski–Bouligand dimension or Box Dimension have been used.

This dimension has many names, such as, information dimension, Kolmogorov entropy, capacity dimension among others. The origin of this dimension is near in time to Hausdorff dimension, at the beginning of the XX century. The definition of Box Dimension was provided by Pntrjagin and Schnirelmann in his article "Sur une propriété métrique de la dimension". This dimension is used in real world problems due to it is easy to calculated or estimated for a finite range of values.

Definition 1. [4] Let $\delta > 0$ and $F \subset \mathbb{R}^n$ a non-empty bounded subset. The smallest number of set of diameter at most δ that cover F as $\mathcal{N}_\delta(F)$. Thus the box dimension of F is given by:

$$\dim_B(F) := \lim_{\delta \rightarrow 0} \frac{\log(\mathcal{N}_\delta(F))}{\log(\frac{1}{\delta})} \quad (1)$$

A theoretical connection between Hausdorff dimension and box dimension is that $\dim_H(F) \leq \underline{\dim}_B(F) \leq \overline{\dim}_B(F)$. The Box counting dimension is very useful due to the following theorem:

Theorem 1. [4] Let $\delta > 0$ and F be a non-empty bounded subset of \mathbb{R}^n . The following definitions of $\mathcal{N}_\delta(F)$ are equivalent for box dimension calculation purposes:

1. The smallest number of sets of diameter at most δ that cover F .
2. The smallest number of closed balls of radius δ that cover F .
3. The smallest number of cubes of side δ that cover F .
4. The number of δ -cubes that intersect F .
5. The largest number of disjoint balls of radius δ with centres in F .

From the above theorem, two equivalent dimensions arise: the box counting dimension and the circle counting dimension. The famous one is the box counting due to is simpler introduce a square than circle in a computer.

One of the most common topics is "neurons have a fractal structure" and it is a very popular topic in medicine and neuroscience. The first step to analysis this structure is to reformulate it as "neurons has statistical self-similar structure" This hypothesis was discredited in 1995 by Panico and Sterling who tested that Retinal neurons and vessels are not fractals [20]. In their work they developed a synthetic fractal pattern which has the same fractal dimension although it was a draw without some lines.

Therefore, applying the box-counting method to patterns that that there are not fractals its only a upper-bound for the Hausdorff measure as it was proved by Moran that this only equal in a very specific case therefor the Hausdorff dimension can be the same as the Euclidean one making all of this articles a dead letter.

¹Megaparsec per hour

1.6 Does fractal really exists?

As previously, mentioned fractals in nature do not exist due to its finite nature and the definition of fractal dimension needs the infinite to exist. Nature must necessarily be pre-fractal, self-similar only on a certain number of scales.

In non-mathematical articles, the results are presented with a resolution of 3 or 4 orders of magnitude, as showed in the article of Avnir *et al.* where they say that: "have been swayed by the widespread image and belief that fractality has been found over many orders of magnitude in experimental documentation" [3]. In this article they studied more than 90 papers of Physical Review Letters and Physical Review published between 1990 and 1996 with the word fractal. Most of these physical systems show self-similarity only in scale factors within two orders of magnitude and none were observed to be more than 3 orders of magnitude. Therefore if an article contains the word fractal it should be taken with care. The article must have a high order of self-similarity and not less than three orders.

References

- [1] MANDELNBROT, BENOIT, *The fractal geometry of nature*, W.H. Freeman, 1982.
- [2] BENOIT B. MANDELNBROT AND DANN. E. PASSOJA AND ALVIN J. PAULLAY, *Fractal character of fracture surfaces of metals*, Nature,308(5961,721–722) 1984.
- [3] DAVID AVNIR AND OFER BIHAM AND DANIEL LIDAR AND OFER MALCAI, *Is the Geometry of Nature Fractal?*, Science, 01-1998.
- [4] MANUEL FERNÁNDEZ-MARTÍNEZ AND JUAN LUIS GARCÍA GUIRAO AND MIGUEL ÁNGEL SÁNCHEZ-GRANERO AND JUAN EVANGELISTA TRINIDAD SEGOVIA, *Fractal Dimension for Fractal Structures*, Fractal and Fractional., **5(2)** : 2019.
- [5] ZAKHAROV, V S AND SIMONOV, D A AND GILMANOVA, G Z AND DIDENKO, A N, *The fractal geometry of the river network and neotectonics of south sikhote-Alin*, Russ. J. Pac. Geol,Pleiades Publishing Ltd, **14-6** : 526–541, November 2020.
- [6] BENOIT MANDELNBROT, *How Long Is the Coast of Britain? Statistical Self-Similarity and Fractional Dimension*, Science, 156, 636–638, 1967.
- [7] DONALD M. D. GRAY, *Interrelationships of watershed characteristics*, Journal of Geophysical Research, 66,1215-1223, 1961.
- [8] AKHLAQ HUSAIN AND JAIDEEP REDDY AND DEEPIKA BISHT AND MOHAMMAD SAJID, *Fractal dimension of coastline of Australia*, Scientific Reports, **11(1)** : 2021.
- [9] DAVID G. TARBOTON AND RAFAEL L. BRAS AND IGNACIO RODRIGUEZ-ITURBE, *The fractal nature of river networks*, Water Resources Research), 24, 08-1998.
- [10] KEITH MONTGOMERY, *Sinuosity and Fractal Dimension of Meandering Rivers*, Area, **4** : 491–500,26,1996.
- [11] PETERS, EDGAR, *Fractal market analysis : applying chaos theory to investment and economics*, J. Wiley & Sons, 1994.
- [12] ELLIOTT, RALPH, *The wave principle*, Snowball Publishing, 2012.

- [13] TAKAYUKI MIZUNO AND SHOKO KURIHARA AND MISAKO TAKAYASU AND HIDEKI TAKAYASU, *Analysis of high-resolution foreign exchange data of USD-JPY for 13 years*, Physica A: Statistical Mechanics and its Applications, 1-2(324), 296–302 6-2003.
- [14] JOHANNES A SKJELTORP, *Fractal market analysis : applying chaos theory to investment and economics*, Physica A: Statistical Mechanics and its Applications, 3(283), 486–528, 2000.
- [15] FRANCOIS GREY AND JØRGEN K. KJEMS, *Aggregates, broccoli and cauliflower*, J. Wiley & Sons, 1994.
- [16] M OBERT AND P PFEIFER AND M SERNETZ, *Microbial growth patterns described by fractal geometry*, Journal of Bacteriology, 172(3), 1180–1185,03-1990.
- [17] GAITE, JOSE, *The fractal geometry of the cosmic web and its formation*, Adv. Astron. : 1–25, May 2017.
- [18] PEEBLES, P. J. E., *The large-scale structure of the universe*, Princeton University Press, 1980.
- [19] EINASTO, J. AND HÜTSI, G. AND KUUTMA, T. AND EINASTO, M., *Correlation function: biasing and fractal properties of the cosmic web*, Astronomy and Astrophysics, 640, 08-2020.
- [20] JOSEPH PANICO AND PETER STERLING, *Retinal neurons and vessels are not fractal but space-filling*, The Journal of Comparative Neurology,365(3), 479-490 10-1995.

Introduction to set theory

Adrián Fidalgo Díaz [‡], José Alejandro Serón Rodrigo [‡] and Marc Tomás Martínez [‡]

(‡) Universitat Politècnica de València, afiddia@posgrado.upv.es

(‡) Universitat de València, joasero@alumni.uv.es

(‡) Universitat de València, marcto3@alumni.uv.es

1 Introduction

Set theory is an interesting branch of mathematics, out of its applications we can find being employed as a foundational system for the whole of mathematics or providing as framework to develop a mathematical theory of infinity. In this article we will present the set theory from an axiomatic point of view. In particular we will introduce the Zermelo-Fraenkel set theory with the axiom of choice. This model, denoted by ZFC, consists of the axioms of extensionality, pairs, unions, subsets, replacement, infinity and the axiom of choice.

Later, we will define two important concepts of set theory: the ordinals and the cardinals, which are both a generalization of naturals. The former represents order, while the latter represents quantity.

2 Main results

2.1 The model ZFC

We will explain all axioms except the axiom of infinity, which will we discussed later on.

- The **axiom of extensionality** asserts that two sets which have the same elements are equal:

$$\forall v_0 \forall v_1 (\forall v_2 (v_2 \in v_0 \Leftrightarrow v_2 \in v_1) \Rightarrow v_0 \simeq v_1)$$

- The **axiom of pairs**:

$$\forall v_0 \forall v_1 \exists v_2 \forall v_3 (v_3 \in v_2 \Leftrightarrow (v_3 \simeq v_0 \vee v_3 \simeq v_1))$$

The **axiom of unions**:

$$\forall v_0 \exists v_1 \forall v_2 (v_2 \in v_1 \Leftrightarrow \exists v_3 (v_3 \in v_0 \wedge v_2 \in v_3))$$

- The **axiom of subsets** asserts that for every set a exists a set b whose elements are the subsets of a :

$$\forall v_0 \exists v_1 \forall v_2 (v_2 \in v_1 \Leftrightarrow \forall v_3 (v_3 \in v_2 \Rightarrow v_3 \in v_0))$$

- The **axiom scheme of replacement** comprises all formulas of the following form:

$$\begin{aligned} & \forall v_0 \forall v_1 \dots \forall v_n \\ & (\forall w_0 \forall w_1 \forall w_2 ((F[w_0, w_1, v_1, \dots, v_n] \wedge F[w_0, w_2, v_1, \dots, v_n]) \Rightarrow \\ & w_1 \simeq w_2) \Rightarrow \exists v_{n+1} \forall v_{n+2} (v_{n+2} \in v_{n+1} \Leftrightarrow \exists w_0 (w_0 \in v_0 \\ & \wedge F[w_0, v_{n+2}, v_1, \dots, v_n]))) \end{aligned}$$

where n is an integer and $F[w_0, w_1, v_1, \dots, v_n]$ is a formula of L .

- The **axiom of choice**: Let $(a_i)_{i \in I}$ be a family of set such that a_i is non-empty for every $i \in I$. Then $\prod_{i \in I} (a_i)$ is not empty.

2.2 Ordinal numbers

Definition 1. Let α be a set. We say that α is an **ordinal** if

1. α is transitive, that is, every element of a set that belongs to α also belongs to α :

$$\forall v_0 \forall v_1 ((v_0 \in \alpha \wedge v_1 \in v_0) \Rightarrow v_1 \in \alpha),$$

2. the relation \in is a well order on α , that is,

- \in is transitive,
- \in is reflexive,
- if $x, y \in \alpha$, $x \neq y$, then $x \in y$ or $y \in x$.
- every non-empty subset of α has a least element.

We write $On[v_0]$ to denote the formula that express that v_0 is an ordinal.

Let α be a set, an **initial segment** of α is a subset β of α with the property

$$y \in \beta, x \in y \Rightarrow x \in \beta.$$

A **proper initial segment** of α is an initial segment that is not the empty set or α , such as

$$S_x = \{y \in \alpha : y \in x\}.$$

Proposition 1. Let α be an ordinal. The following statements are true:

1. $\alpha \notin \alpha$,
2. if $\beta \in \alpha$, then β is an ordinal,
3. if $\beta \in \alpha$, then $\beta = S_\beta$,
4. if β is another ordinal, then $\alpha \subseteq \beta$ if and only if $\alpha \leq \beta$.

Proposition 2. Let X be a transitive set of ordinals such that, for all distinct elements x and y in X , $x \in y$ or $y \in x$. then X is an ordinal.

Proposition 2 and its corollaries are extremelly useful to construct the ordinals.

Corollary 1. If α is an ordinal and β is an initial segment of α , then β is an ordinal. Moreover, if $\beta \neq \alpha$, then $\beta \in \alpha$.

Corollary 2. *If α is an ordinal, then $\beta = \alpha \cup \{\alpha\}$ is an ordinal.*

The ordinal $\alpha \cup \{\alpha\}$ will be denoted as α^+ , and is called **successor** of α . If a non-empty ordinal is not the successor of another ordinal, then it is called **limit ordinal**.

Proposition 3. *If f is an isomorphism from α to β , α, β ordinals, then $\alpha = \beta$ and f is the identity on α .*

As a consequence, we have the following proposition:

Proposition 4. *If α and β are ordinals, then exactly one of the following holds:*

1. $\alpha \in \beta$,
2. $\beta \in \alpha$,
3. $\alpha = \beta$.

Now, Proposition 2 can be rephased as ‘every transitive set of ordinals is an ordinal’. We are interested in the class formed by all ordinals (all sets v_0 that satisfy $On[v_0]$). Every non-empty class of ordinals contains a least element.

Proposition 5. *The class of ordinals is not a set.*

The idea of the ordinals as a numeric system analogous to natural numbers is based on the following theorem:

Theorem 1 (Zermelo’s Theorem). *Let X be a well-ordered set, then there exists one and only one ordinal α isomorphic to X . Moreover, there is only an isomorphism from α to X .*

We denote as $Ord(X)$ the ordinal that is isomorphic to a well ordered set (X, R) , which is unique. We may use the ordinals as a criterion to ‘measure’ the ‘length’ of a well-ordered set. If X and Y are isomorphic well-ordered sets, then $Ord(X) = Ord(Y)$. As ordinals have a uniqueness property, we can use $Ord(X)$ being the ‘length’ of the well-ordered set X .

We propose to take the ordinals as a system of numbers, generalizing the idea of natural numbers. To describe ordinals as numbers, the first ordinal is the empty set, which we can relate to the first natural, and the following ordinals are obtained using the definition of successor,

$$\begin{aligned}
 0 &= \emptyset \\
 1 &= \{\emptyset\} = \{0\} \\
 2 &= \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\
 3 &= \{0, 1, 2\} \\
 4 &= \{0, 1, 2, 3\} \\
 &\dots \\
 n &= \{0, 1, 2, \dots, n-1\} \\
 &\dots
 \end{aligned}$$

We need to introduce a new axiom, to extend to infinite ordinals:

- The **axiom of infinity**:

$$\exists v_0 (On[v_0] \wedge \neg v_0 \simeq \emptyset \wedge \forall v_1 \neg v_0 \simeq v_1 \cup \{v_1\})$$

There exists a limit ordinal, or equivalently, there exists an infinite ordinal.

As the class of all ordinals is well-ordered, there exists a least infinite ordinal, denoted by ω , and

$$\omega = \{0, 1, 2, \dots, n, \dots\},$$

the least infinite ordinal is equal to the set of finite ordinals. Its successor is

$$\omega^+ = \omega + 1 = \{0, 1, 2, \dots, n, \dots, \omega\}.$$

We can define operations on ordinals analogously to the operations we define with integers. All details of the operations can be found on [2].

Definition 2. Let α, β ordinals, we set

$$A = \alpha \uplus \beta \equiv (\alpha, \mathbf{0}) \cup (\beta, \mathbf{1}),$$

with a well order of A

$$(\nu, i) <_A (\tau, j) \iff (i < j) \vee (i = j \wedge \nu < \tau).$$

The **ordinal sum** is set as

$$\alpha + \beta = \text{Ord}(A, <_A)$$

We can define the **ordinal product** as an iterated sum.

Definition 3. Let α, β ordinals, the **ordinal product** is

$$\alpha \times \beta = \sum_{\eta < \beta} \alpha.$$

Theorem 2. Let α, β, γ be ordinals. Then,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$,
2. $\alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma$,
3. $\alpha \times (\beta + \gamma) = (\alpha \times \beta) + (\alpha \times \gamma)$,
4. $\alpha + \mathbf{0} = \alpha = \mathbf{0} + \alpha$,
5. $\alpha \times \mathbf{0} = \mathbf{0} \times \alpha = \mathbf{0}$,
6. $\alpha^+ = \alpha + 1$,
7. if α and β are finite, then so are $\alpha + \beta$ and $\alpha \times \beta$,
8. if $\alpha^+ = \beta^+$, then $\alpha = \beta$,
9. if α and β are finite, then $\alpha < \beta$ if and only if there exists γ , non-zero ordinal, such that $\alpha + \gamma = \beta$.

Finally, we define the ordinal exponentiation based on the ordinal product, as follows:

Definition 4. Let α be an ordinal. α^β is defined by recursion so that

$$\begin{aligned} \alpha^0 &= 1, \\ \alpha^{\beta+1} &= \alpha^\beta \times \alpha, \\ \alpha^\beta &= \lim_{\eta < \beta} \alpha^\eta, \text{ if } \beta \text{ is a limit ordinal.} \end{aligned}$$

The operations defined above can be used to obtain a picture of the ordinal number system, as a generalization of the natural numbers. We can see all detail on [3].

$$\begin{aligned} &0, 1, 2, \dots, n, \dots, \omega, \omega + 1, \omega + 2, \dots, \omega + n, \dots, \omega + \omega = \omega \times 2, \\ &\omega \times 2 + 1, \omega \times 2 + 2, \dots, \omega \times 2 + n, \dots, \omega \times 3, \dots \\ &\omega \times \omega = \omega^2, \omega^2 + 1, \omega^2 + 2, \dots, \omega^3, \dots, \omega^3 + \omega, \dots, \omega^3 + \omega^2, \dots, \omega^4, \dots \\ &\omega^\omega, \omega^\omega + 1, \dots, \omega^{\omega \times 2}, \dots, \omega^{\omega \times 3}, \dots, \omega^{\omega \times \omega} = \omega^{\omega^2}, \dots, \omega^{\omega^3}, \dots, \omega^{\omega^\omega}, \dots \end{aligned}$$

2.3 Cardinal numbers

The natural concept of counting the elements of a given set is deeply rooted in all human beings of any culture. Following the construction of the ordinal numbers, we can generalize this idea of ‘counting’ to extend our notions of comparing finite sets to also infinite sets. This is the path to define a new type of numbers: cardinal numbers. Before we start formalizing these, we must understand what it means to compare the largeness of different sets. The idea behind is very simple, two sets are equal in size if it is possible to totally map one using as indexes the elements of the other. Correspondence is the key to understand this type of concepts about the size of sets and so it shows the Definition 5:

Definition 5. *Given two sets x and y , we say that x is **subpotent** to y if there exists an injection from x to y . In addition, if a bijection can be form between the two sets, we say they are **equipotent**.*

The Definition 5 establishes a good comparing sets criteria that induces a natural meta-relation within the class of all sets. This relation can be expressed as x is related with y if they are equipotent. It is easy to prove that this meta-relation is reflexive, symmetrical and transitive, and so splits the class of all sets into different equivalence classes. The next pass shall be to choose a representative of each class.

Definition 6. *Given a set x , we define $\text{card}(x)$ as the least ordinal that is equipotent to x and we called it the **cardinal** of x .*

Theorem 3. *(Cantor-Bernstein) If x is subpotent to y and y is subpotent to x , then x and y are equipotent.*

Definition 7. *Let x and y be two disjoint sets with $\lambda = \text{card}(x)$ and $\mu = \text{card}(y)$, we define the following operations on their cardinals:*

1. $\lambda + \mu = \text{card}(x \uplus y)$,
2. $\lambda \times \mu = \text{card}(x \times y)$,
3. $\lambda^\mu = \text{card}(x^y)$.

Theorem 4. *(Cantor) Let λ be a cardinal, then $2^\lambda > \lambda$.*

The Cantor’s Theorem 4 makes possible to construct a larger cardinal of any given cardinal λ by doing 2^λ . Also, contains a result of huge importance as it is the fact that the power set is strictly bigger than the original set (any set, not only cardinals). This, which can seem obvious for finite cardinals, is deeply shocking when thinking about the size of infinite cardinals.

Proposition 6. *Let \mathbb{R} be the set of real numbers, then $\text{card}(\mathbb{R}) = 2^{\aleph_0}$.*

Proposition 7. *If x is a set of cardinals, then $\sup x$ is also a cardinal.*

Theorem 5. *Let λ, μ be cardinals. If at least one of them is infinite, the following statements are true:*

1. $\lambda + \mu = \sup\{\lambda, \mu\}$,
2. $\lambda \times \mu = \sup\{\lambda, \mu\}$.

The construction of the cardinal numbers and its main results can be reviewed in [2] and [3].

3 Conclusions

Set theory is a discipline deeply in contact with pure logic, its starting point is close to the rudimentary definitions on which mathematics are sustained. Sets are an indispensable tool to make reasoning through every single part of this science of numbers and ‘x’s. Also, we have seen that they can be used to generalise in different ways natural numbers. The ordinals are a good representation of the notion of order carried by the set \mathbb{N} but extend this concept to the domain of infinite sets. They are also useful to construct induction proofs over non finite sets. In the same way, from ordinals, another generalization of naturals can be constructed, this time by extending the meaning of ‘quantity’. These are the cardinal numbers, which are indeed a subset of ordinals that can help us to compare whether finite or infinite sets. It is clear that all these applications of set theory are an important part of mathematics and they transform the infinite into a knowable concept.

References

- [1] RENÉ CORI, DANIEL LASCAR AND DONALD H. PELLETIER, *Mathematical Logic: A course with exercises - Part I - Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems*, Oxford University Press, 2001.
- [2] RENÉ CORI, DANIEL LASCAR AND DONALD H. PELLETIER, *Mathematical Logic: A course with exercises - Part II - Recursion Theory, Gödel’s Theorems, Set Theory, Model Theory*, Oxford University Press, 2001
- [3] KEITH DEVLIN, *The joy of sets : fundamentals of contemporary set theory*, Springer-Verlag, 1992.
- [4] HEINZ-DIETER EBBINGHAUS, *Ernst Zermelo: An Approach to His Life and Work*, Springer, Berlin, Heidelberg, 2007
- [5] JEAN VAN HEIJENOORT, “*Investigations in the foundations of set theory*”, *From Frege to Gödel: A Source Book in Mathematical Logic*, Harvard University Press, 1967.

A fuzzy system to improve image denoising method

Khleef Almutairi ^b and Samuel Morillas ^d

- (b) Department of Applied Mathematics, Universitat Politècnica de València, Camino de Vera s/n, Valencia, 46022, Spain. Email: kkalmuta@doctor.upv.es
- (d) Department of Applied Mathematics, Universitat Politècnica de València, Camino de Vera s/n, Valencia, 46022, Spain. Email: smorillas@mat.upv.es

1 Introduction

In 1965, Zadeh [9] introduced fuzzy logic as an extension of the constitution of classical logic beyond false and true values. Fuzzy logic consists of three main processing parts: fuzzification, inference engine and defuzzification. Since then, this method has been found to be applicable in many research lines, especially in image processing and decision-making.

In the image processing field, many methods of denoising have been presented with the goal of suppressing Gaussian noise and preserving the details and structure of the colour images. The earliest ways for smoothing the Gaussian noise were based on a linear approach, for instance, *arithmetic mean filter* (AMF) [8], which has the ability to suppress the noise by taking advantage of the zero-mean property; however, the texture and details of the images are blurred. This flaw sparks off the development of many non-linear methods to detect the image edges and smooth them with less capability to protect them from blur. Within the non-linear methods, a well-known method *bilateral filter* (BF) [11] uses the average to take advantage of the zero-mean property. Also, other methods of filtering use different ways to improve the result by minimizing the noise in the colour images; for example, the method *Eigenvector analysis filter* (EIG) [1] uses the technique of weighted pixel averaging to approach the colour images denoising problem based on eigenvectors.

In this study, a fuzzy inference system is designed and used to determine the amount of noise that should be removed from the colour images. The transformation of the image space from RGB space to an eigenvector space is required to perform the eigenvectors analysis to have the ability to process the correlation between the channels and then extract the three coefficients, as the colour images have three channels – red, blue and green. These coefficients are intended to be the inputs of the fuzzy system.

The setting of the fuzzy inference system is going to conclude which of the three channels should be smoothed in low or high performance, depending on the information of the channels. The amount of denoising is related to the information in the image. If there are edges and details that we need to preserve in the window of an image, gentle smoothing is required. On the other hand, flat regions in the image indicate that no information needs to be retained; hence, the system is smooth at its highest capability.

Therefore, the system produces three smoothing coefficients for each of the three windows of the image and using these results; we can proceed with the denoising process. When the noise is suppressed and the quality is improved, the image is returned to its RGB space.

Lastly, after obtaining the results, it is necessary to compare the system's output with the original picture and other different filtering methods based on a well-known image quality assessment method: Peak signal-to-noise ratio (PSNR) [8], which is a way of measuring how well details of the images are preserved. If the result of the fuzzy inference system is less than the expectation in this comparison, we require adjustments to the parameters or the set of the rules in the fuzzy system to maximize the smoothing capability.

This method has shown promising results without a shadow of a doubt in terms of PSNR during the primary experimental and trial stages; as the experimental results section stated, and it should be pointed out, the fuzzy inference system still requires more optimization of the parameters and rules setting for denoising colour images at a maximum capability.

This extended abstract is structured as follows: Section 1.2 gives an explanation of the designed method. Section 1.3 showed the experimental results and a comparison against other methods of minimizing noise. Lastly, the conclusion is presented in section 1.4.

2 Method details

This section presents the proposed fuzzy inference system components for denoising the colour images based on the general structure shown in Figure 1.

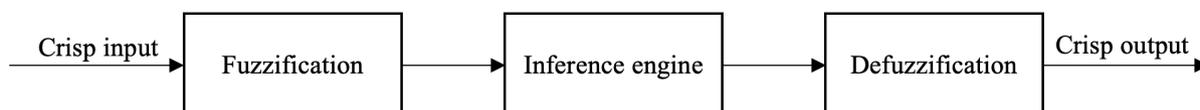


Figure 1: Components of designed fuzzy inference system

The fuzzy inference system [4, 7] consists of four important phases: (i) crisp values that used as inputs to the system are the values that obtained from the eigenvector analysis called $\sigma_n(u^i)$, $\sigma_n(u^j)$, and $\sigma_n(u^k)$ and this analysis is explained in greater details in [1] and we will demonstrate the fuzzy inference system only; (ii) Fuzzification process means the transformation of the crisp inputs to linguistic terms over the membership function, and the membership functions are used in the fuzzification and defuzzification steps of the fuzzy inference system. In the system, the crisp inputs are fuzzified into three sets as the parameters of the eigenvector analysis produced three, and each parameter will be in a separate input set, and every fuzzy set is divided into two subsets: low and high. The parameters for inputs and outputs sets are specified by trials and error, and finding an appropriate procedure to set them is part of future work. It has been chosen the membership function be Gaussian, and these membership functions are adopted due to their simplicity and dependency only on two parameters which will be useful to save time during the optimization stage. (iii) inference process, this stage is applying the set of linguistic rules in the form of **IF - THEN** and in this step, the inference transforms the fuzzy input values to fuzzy output values. The set of the rules that are defined for processing the denoising in the fuzzy

inference system is the following:

- **IF** the inputs $\sigma_n(u^i)$ is low, and $\sigma_n(u^j)$ is low and $\sigma_n(u^k)$ is low **Then** the smoothing coefficients C_i is low and, C_j is low and C_k is low.
- **IF** the inputs $\sigma_n(u^i)$ is low, and $\sigma_n(u^j)$ is low and $\sigma_n(u^k)$ is high **Then** the smoothing coefficients C_i is low and, C_j is low and C_k is high.
- **IF** the inputs $\sigma_n(u^i)$ is low, and $\sigma_n(u^j)$ is high and $\sigma_n(u^k)$ is low **Then** the smoothing coefficients C_i is low and, C_j is high and C_k is low.
- **IF** the inputs $\sigma_n(u^i)$ is high, and $\sigma_n(u^j)$ is low and $\sigma_n(u^k)$ is low **Then** the smoothing coefficients C_i is high and, C_j is low and C_k is low.

After the inference processing, the result must be defuzzified to obtain the final crisp output C_i , C_j and C_k that used to smooth the colour image, the last phase of the fuzzy inference system is (iv) defuzzification which consists of transforming the linguistic variables to crisp values through the membership functions, and the membership function that used in the last phase are Gaussian membership function for the same reason aforementioned. The fuzzy inference system inputs and outputs are depicted in Figure 2.

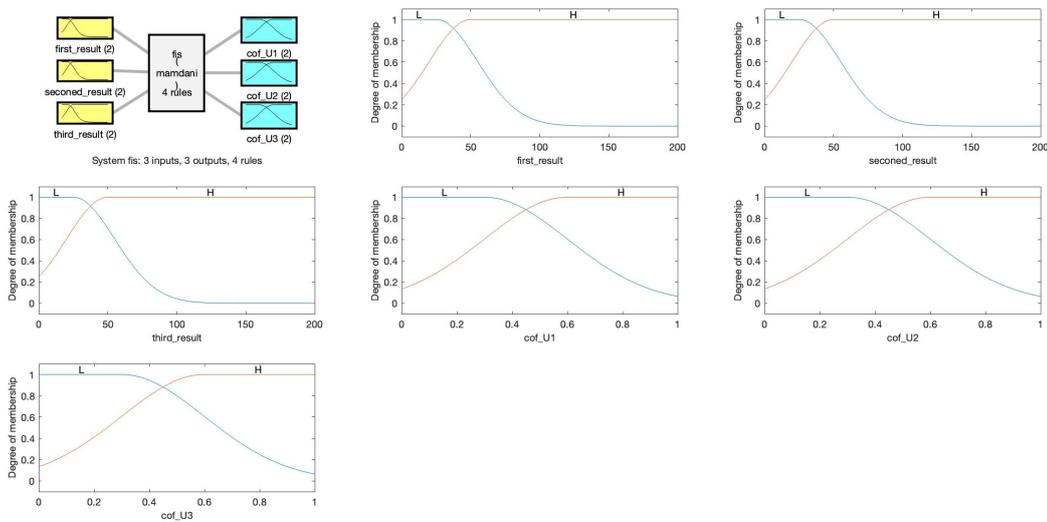


Figure 2: The designed fuzzy inference system consisting three inputs (the first three from the left) sets and three output sets

3 Experimental results

In this section, test images of Pills, Lenna and Head-Phone of different sizes have been used for this experiment to evaluate the effectiveness of the proposed method. These images are contaminated with different levels of Gaussian noise. The use of PSNR to assess the performance of the proposed method compared against following filters: *Bilateral filter* (BF) [11], *Fuzzy vector median filter* (FVMF) [3], *Fuzzy Noise Reduction Filter* (FNRF) [2], *Collaborative Wavelet Filter* (CWF) [5,6] and lastly, *Eigenvector analysis filter* (EIG) [1].

The results of filters showed in the Tables 1, 2 and 3 and in each table, the best result for each noise level is written in blue, and the second-best is written in red. Roughly speaking, the proposed method has advantages in about 60% of cases, either first or second-best results, achieving a minimizing of noise as well as preserving the image structures. These results tended to improve in future work.

Furthermore, some denoised images using the proposed filter and EIG filter are exhibited in the Figures 4, 5 and 6. Generally, the images produced by the proposed method are visually satisfying in terms of details preservation and suppressing the noise in viewpoint.



Figure 3: Test images (size): (a) Pills (50x50), (b) Lenna (90x90), (c) Head-Phone (100x100)

PSNR of Pills image				
Filter	$s = 5$	$s = 10$	$s = 20$	$s = 30$
None	34.44	28.41	22.60	19.21
BF	35.52	30.18	26.36	24.24
FVMF	28.02	26.83	24.82	23.45
FNRF	34.83	32.38	28.23	26.09
CWF	38.24	33.17	26.60	23.02
EIG	37.30	32.58	28.52	26.20
Proposed	37.14	32.53	28.54	26.16

Table 1: Performance comparison in terms of PSNR using the Pills image contaminated with different standard deviation s of Gaussian noise. In each table, the best result for each noise level and performance measure is written in blue, and the second best, in red.

PSNR of Lenna image				
Filter	$s = 5$	$s = 10$	$s = 20$	$s = 30$
None	34.44	28.33	22.54	19.17
BF	35.88	30.98	27.40	25.36
FVMF	29.03	27.81	25.86	24.88
FNRF	35.33	32.62	28.73	26.71
CWF	39.64	34.37	28.48	26.14
EIG	37.74	33.25	29.04	26.98
Proposed	37.66	33.08	29.08	26.90

Table 2: Performance comparison in terms of PSNR using the Lenna image contaminated with different standard deviation s of Gaussian noise. In each table, the best result for each noise level and performance measure is written in blue, and the second best, in red.

PSNR of HeadPhone image				
Filter	$s = 5$	$s = 10$	$s = 20$	$s = 30$
None	40.17	34.20	28.30	25.00
BF	40.19	28.81	25.47	24.48
FVMF	24.35	24.19	23.89	23.50
FNRF	32.23	31.75	30.26	28.62
CWF	40.05	35.36	30.96	28.06
EIG	40.17	36.43	31.86	29.09
Proposed	40.44	35.92	31.36	28.72

Table 3: Performance comparison in terms of PSNR using the Head-Phone image contaminated with different standard deviation s of Gaussian noise. In each table, the best result for each noise level and performance measure is written in blue, and the second best, in red.



Figure 4: Visual comparison of filters output: (a) Original Pills image, (b) corrupted image with $s = 10$ Gaussian noise, (c) EIG filter output (d) Proposed filter output



Figure 5: Visual comparison of filters output: (a) Original Lenna image, (b) corrupted image with $s = 20$ Gaussian noise, (c) EIG filter output (d) Proposed filter output

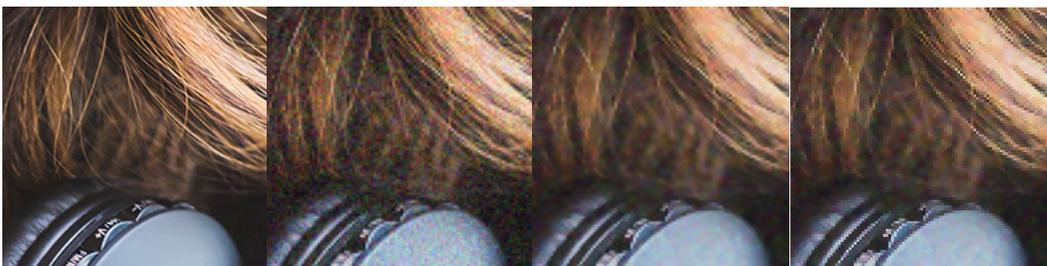


Figure 6: Visual comparison of filters output: (a) Original Head-Phone image, (b) corrupted image with $s = 30$ Gaussian noise, (c) EIG filter output (d) Proposed filter output

4 Conclusion

In this extended abstract, we introduce an ongoing filtering method using a fuzzy inference system to determine the amount of noise that should be minimized. The proposed method has shown the use of fuzzy logic is effective despite its simplicity and competitive results in the primary stages against other filtering methods—the need for more experiments and optimization of the system to maximize the capability of the smoothing.

References

- [1] LATORRE-CARMONA, P., MIÑANA, J.-J. & MORILLAS, S., *Colour image denoising by eigenvector analysis of Neighbourhood Colour Samples.*, Signal, Image and Video Processing, **14(3)**: pp. 483—490, 2019.
- [2] SCHULTE, S., DE WITTE, V., KERRE, E.E., *A fuzzy noise reduction method for colour images.*, IEEE Trans., **16**: pp.1425—1436, 2007.
- [3] SHEN, Y., BARNER, K., *A Fuzzy vector median-based surface smoothing.*, IEEE Trans. Vis. Comput. Graph., **10**: pp.252—265, 2004.
- [4] MENDEL, J., *A Fuzzy logic systems for engineering: a tutorial.*, Proceedings of the IEEE., **83**: pp. 345—377, 1995.
- [5] DABOV, K., FOI, A., KATKOVNIK, V., EGIAZARIAN, K., *Image denoising by sparse 3D transform-domain collaborative filtering*, IEEE Trans. Image Process., **16**: pp. 2080—2095, 2007.
- [6] DABOV, K., FOI, A., KATKOVNIK, V., EGIAZARIAN, K., *Color image denoising via sparse 3D collaborative filtering with grouping constraint in luminance-chrominance space.*, Proceedings of the IEEE International Conference on Image Processing ICIP2007, pp. 313—316, 2007.
- [7] ROSS, T.J., *Fuzzy logic with engineering applications*, John Wiley & Sons, 2005.
- [8] PLATANIOTIS, K.N. & VENETSANOPOULOS, A.N., *Color image processing and applications*, Berlin: Springer, 2011.
- [9] ZADEH, L.A., *Fuzzy sets*, Information and Control., **8(3)**: pp. 338—353, 1965.
- [10] SANTOS, J. & TORRES-MACHI, C. & MORILLAS, S. & CEREZO, V., *A fuzzy logic expert system for selecting optimal and Sustainable Life Cycle Maintenance and rehabilitation strategies for road pavements.*, International Journal of Pavement Engineering, **23(2)**: pp. 425—437, 2020.
- [11] TOMASI, C. & MANDUCHI, R., *Bilateral filter for gray and color images*, Proceedings of IEEE International Conference Computer Vision, pp. 839—846, 1998.

Three mathematical modelling of the glucose-insulin process for Type 1 Diabetes patients. Control and numerical results.

Marcos Llamazares López ¹, Alberto Pérez Galende ² and Álvaro Vargas Moreno ³

- (1) marllalo@alumni.upv.es Universitat Politècnica de Valencia, Universitat de València
- (2) apergal@posgrado.upv.es, Universitat Politècnica de València, Universitat de València
- (3) alvarmo1@etsii.upv.es, Universitat Politècnica de València, Universitat de València

1 Introduction

Type 1 Diabetes is a disease that affects more than 400 million people and it does not allow them to have a normal life. Studies have been made since 1970s to understand this disease and different models to predict the body response have been developed since. The first worldwide accepted model was the Bergman model, developed in 1981 [1], was a model created to measure the glucose in a patient with Type 1 Diabetes. Years later the Hovorka model was created to solve the delay problem provoked by the subcutaneous administration of insulin [5]. Very recently a new model including fractional derivatives was developed to include this same delay but avoiding the complexity of the Hovorka model [10].

In this article the mathematical and control tools needed to treat this model will be introduced. Then each model will be explained and a methodology to solve this models. Finally, we will obtain numerical results that validate the capability to control the glucose concentration in blood function for this three models. At the end a brief comparison of the models and results will be done and we propose future work that can be done to introduce more complex control systems.

2 Models

2.1 Bergman

The first model that was studied in the interaction processes of glucose and insulin was the Bergman model. It is a non-linear model with two coupled differential equations where the aim is to model the interaction between the concentration of insulin in blood $I(t)$ (input of the model) and that of glucose $G(t)$ (output or variable to control).

$$\begin{cases} \dot{X}(t) = -p_2 \cdot X(t) + p_3(I(t) - I_b) \\ \dot{G}(t) = -(p_1 + X(t))G(t) + p_1G_b + G_{meal}(t) \end{cases}$$

Symbol	Quantity
$X(t)$	effect of insulin.
I_b	basal levels of insulin concentration
G_b	basal levels of glucose concentration
G_{meal}	alteration in the glucose concentration due to food intake
p_1, p_2, p_3	kinematic coefficients

Table 1: Variables used in the Fractional Derivative Model

2.2 Hovorka

In 2004, a new non linear model to predict the glucose concentration levels was developed by Roman Hovorka and his collaborators. This model consists in 3 different subsystems, each one focused on modelling one different aspect of the process. This different subsystems can be seen in with all the processes that take place.

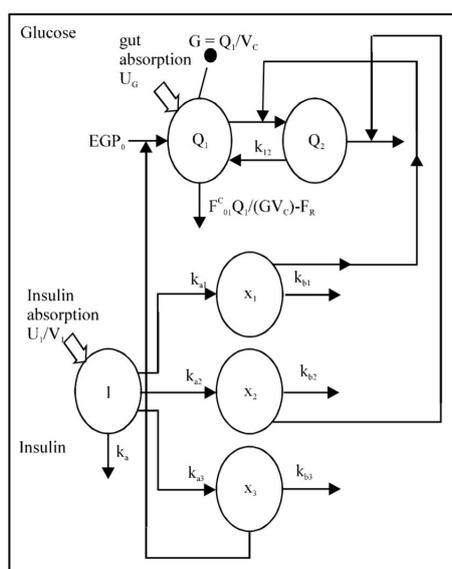


Figure 1: Representation of the entire Hovorka model

Glucose subsystem

$$\frac{dQ_1(t)}{dt} = - \left[\frac{F_{01}^c}{V_G G(t)} + x_1(t) \right] Q_1(t) + k_{12} Q_2(t) - F_R + U_G(t) + EGP_0 [1 - x_3(t)]$$

$$\frac{dQ_2(t)}{dt} = x_1(t) Q_1(t) - [k_{12} + x_2(t)] Q_2(t) y(t) G(t) = Q_1(t) / V_G$$

Insulin subsystem

This subsystem represents how the insulin kinetics works:

$$\frac{dS_1(t)}{dt} = u(t) - \frac{S_1(t)}{t_{\max,I}}$$

$$\frac{dS_2(t)}{dt} = \frac{S_1(t)}{t_{\max,I}} - \frac{S_2(t)}{t_{\max,I}}$$

$$\frac{dI(t)}{d(t)} = \frac{U_I(t)}{V_I} - k_e I(t)$$

Insulin action subsystem

This subsystem represents how the insulin affects the glucose kinetics

$$\frac{dx_1}{dt} = -k_{a1} x_1(t) + k_{b1} I(t)$$

$$\frac{dx_2}{dt} = -k_{a2} x_2(t) + k_{b2} I(t)$$

$$\frac{dx_3}{dt} = -k_{a3} x_3(t) + k_{b3} I(t)$$

Symbol	Quantity
Q_1	Glucose mass in accessible compartment
Q_2	Glucose mass in non-accessible compartment
k_{12}	transfer rate from non-accessible to accessible compartment
V_G	distribution volume of accessible compartment
y, G	Measurable glucose concentration
EGP_0	Endogenous glucose production with zero insulin concentration
S_1	absorption of short-action insulin
S_2	absorption of short-action insulin
$u(t)$	administration of insulin
k_e	fractional elimination rate
$U_I(t)$	total insulin absorption rate
x_1	effecto of insulin on glucose distribution/transport
x_2	effect on glucose disposal
x_3	effect on endogenous glucose production

Table 2: Variables used in the Hovorka model

2.3 Fractional Derivative

The use of fractional-order calculus for control engineering is introduced by Oustaloup [13] in 1995. Since then, it has been shown that most real processes are fractional. Thus, fractional-order model can describe the dynamics of a system more accurately than an integer-order model [10].

We present a non-linear system of three α -order fractional derivative equations for modeling the dynamics of glucose and insulin concentration in blood. [14], [15]

$$\begin{cases} D_0^\alpha g(t) = -[p_1 + x(t)]g(t) + p_1 g_b + m(t) \\ D_0^\alpha x(t) = -p_2 x(t) + p_3 i(t) \\ D_0^\alpha i(t) = -ni(t) + \tau u(t) \end{cases}$$

Symbol	Quantity
D_0^α	α -order fractional time derivative for a starting time $a = t_0 = 0$.
$g(t)$	Blood glucose concentration
g_b	Basal value of blood glucose concentration.
$x(t)$	Dynamic insulin response.
$i(t)$	Blood insulin concentration.
$m(t)$	Glucose disturbance input (meals).
$u(t)$	Exogenous insulin rate input (control function).
p_1	Insulin-independent rate of glucose uptake in muscles.
p_2	Rate for decrease in tissue of glucose uptake.
p_3	insulin-dependent increase of tissue glucose uptake.
n	Decay rate for insulin in blood.
τ	Insulin input conversion factor.
x_b	Basal value of the dynamic insulin response.

Table 3: Variables used in the Fractional Derivative Model

3 Numerical Results

In this section graphical results will be shown. In the Bergman model, the control results are explained and for the Hovorka and fractional models solutions for simple functions will be presented.

3.1 Bergman

Transfer function of the Bergman model

We apply the Laplace transform to both equations of the linearized Bergman system.

$$\begin{cases} s \cdot \mathcal{L}[X](s) - X(0) = -p_2 \cdot \mathcal{L}[X](s) + p_3 \cdot \mathcal{L}[\tilde{I}](s) \\ s \cdot \mathcal{L}[\tilde{G}](s) - \tilde{G}(0) = -p_1 \cdot \mathcal{L}[\tilde{G}](s) - G_b \cdot \mathcal{L}[X](s) + \mathcal{L}[\tilde{G}_{meal}](s) \end{cases}$$

In this way, thanks to the Laplace transform, we have managed to go from a system in differential equations to an algebraic system. We will consider two conditions to apply to the previous system, the first is that the initial conditions are zero ($X(0) = \tilde{G}(0) = 0$), and the second is that the glucose supply due to the meal will be null ($G_{meal} = 0$). The first condition is reasonable since it is simply assumed that the system starts from equilibrium conditions, while the second is assumed because

the function G_{meal} will be considered in the control model as a disturbance of the system. That is, we will calculate the transfer function without it, but we will take it into account in the simulation and we will see how the control algorithm neutralizes its effect.

With the previous conditions and rewriting the equations we obtain:

$$\begin{cases} \mathcal{L}[X](s) = \frac{p_3}{s+p_2} \cdot \mathcal{L}[\tilde{I}](s) \\ s \cdot \mathcal{L}[\tilde{G}](s) = -p_1 \cdot \mathcal{L}[\tilde{G}](s) - G_b \cdot \mathcal{L}[X](s) \end{cases} .$$

And by the substitution method we get the transfer function.

$$\frac{\mathcal{L}[\tilde{G}](s)}{\mathcal{L}[\tilde{I}](s)} = \frac{-p_3 G_b}{(s+p_1)(s+p_2)} .$$

Finally, the numerical values of the parameters are obtained from [2] and are shown on table 4. So the transfer function is:

$$\frac{\mathcal{L}[\tilde{G}](s)}{\mathcal{L}[\tilde{I}](s)} = \frac{-344.4}{s^2 + 0.044s + 0.00039} .$$

p_1	p_2	p_3	G_b	I_b
0.0317	0.0123	4.92	70	7

Table 4: Parameters of the Bergman minimal model

Using the Matlab simulation program Simulink it has been possible to design a PID controller such as in the scheme 2.

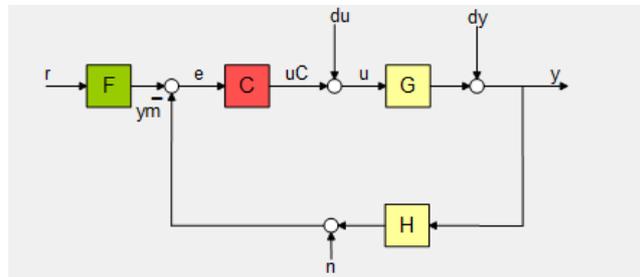


Figure 2: Control system scheme

The Simulink blocks diagram is shown in figure 3, and the coefficients of the designed controller are $K_p = -200$, $K_i = -5$, $K_d = -1$ and $N = 100$.

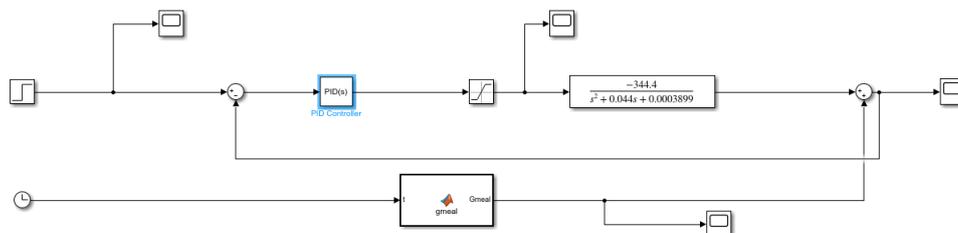


Figure 3: Simulink blocks diagram

3.2 Graphical Representations

Different perturbation signals $G_{meal}(t)$ have been tested, the first being a unit step. Given this signal, the result has been satisfactory, as shown in the figure 4 obtained from the simulation.

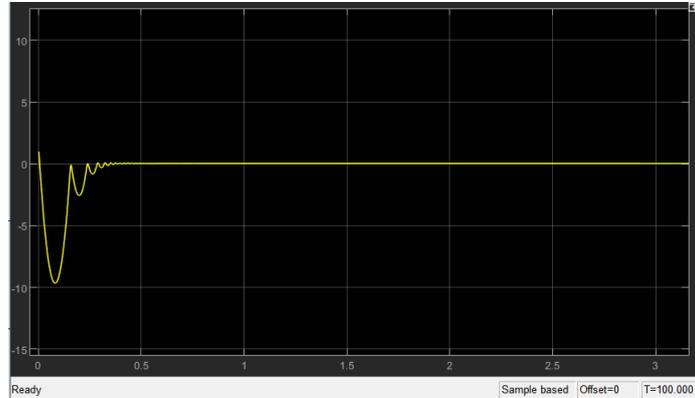
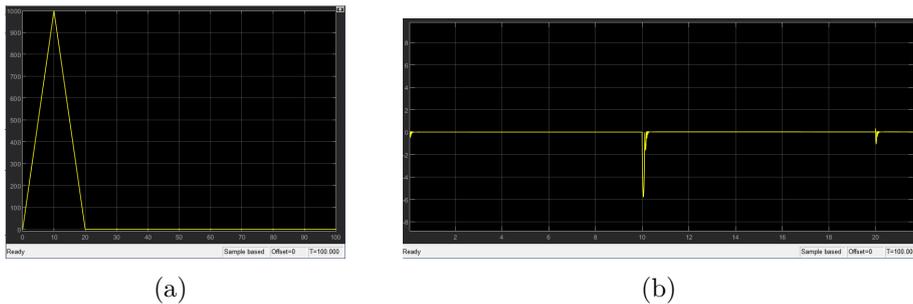


Figure 4: Results when applying unitary step on $G_{meal}(t)$

Another signal of $G_{meal}(t)$ that has been modeled has been a triangular peak generated by the intake of foods with a high glycemic index, as shown in figure 1.5.



(a)

(b)

Figure 5: Peak function on $G_{meal}(t)$ (a) and results when applying a peak function on $G_{meal}(t)$ (b)

The last signal that has been tested has been a sinusoidal with amplitude 100, obtaining as a result figure 6.

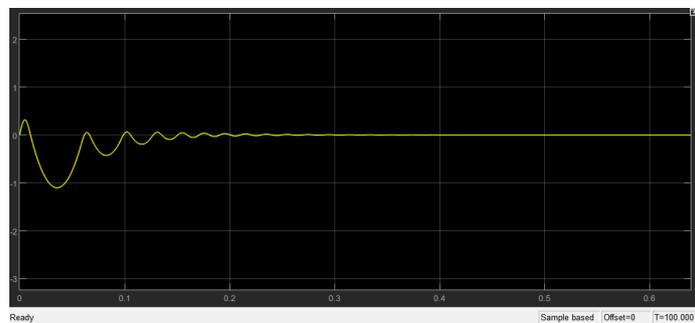


Figure 6: Results when applying a sinus function on $G_{meal}(t)$

Given the previous results one can conclude that the designed PID controller is capable of neutralize the possible perturbation in glucose due to a food input or even to physical exercise.

3.3 Hovorka

Glucose subsystem study

The found solution for the glucose subsystem compartments are:

$$Q_1(t) = e^{\int_0^t \frac{F_{01}^c - V_G x_1 G(t_1)}{V_G G(t_1)} dt_1} \left(Q_b + \int_0^{t_1} \frac{1}{V_G G(t_2)} e^{-\int_0^{t_2} \frac{-F_{01}^c - V_G x_1 G(t_1)}{V_G G(t_1)} dt_1} \cdot EGP_0 V_G G(t_2) - F_R V_G G(t_2) + U_G(t) V_G G(t_2) - EGP_0 V_G x_3 G(t_2) + k_{12} V_G G(t_2) Q_2(t_2) dt_2 \right)$$

$$Q_2(t) = \frac{Q_1(t)}{V_G}$$

and the graphs for this solutions are:

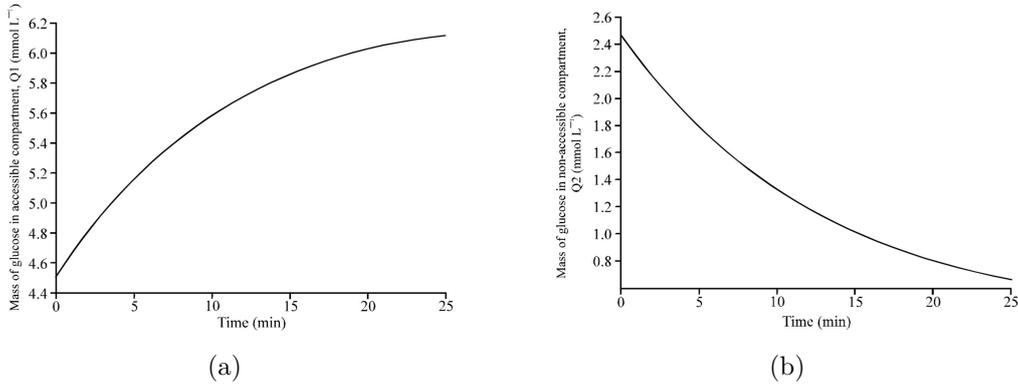


Figure 7: Glucose mass in the accessible compartment(A) and glucose mass in the non-accessible compartment(B)

Insulin subsystem study

Similarly we found the solution for the insulin subsystem compartments and we graph this solutions separately.

$$S_1(t) = e^{-\frac{t}{t_{max,I}}} \int_0^t e^{\frac{t_1}{t_{max,I}}} u(t_1) dt_1$$

$$S_2(t) = e^{-\frac{t}{t_{max,I}}} (1 - e^{\frac{t}{t_{max,I}}}) S_1$$

$$I(t) = \frac{e^{-k_e t} (-1 + e^{k_e t}) U(t)}{k_e V_I}$$

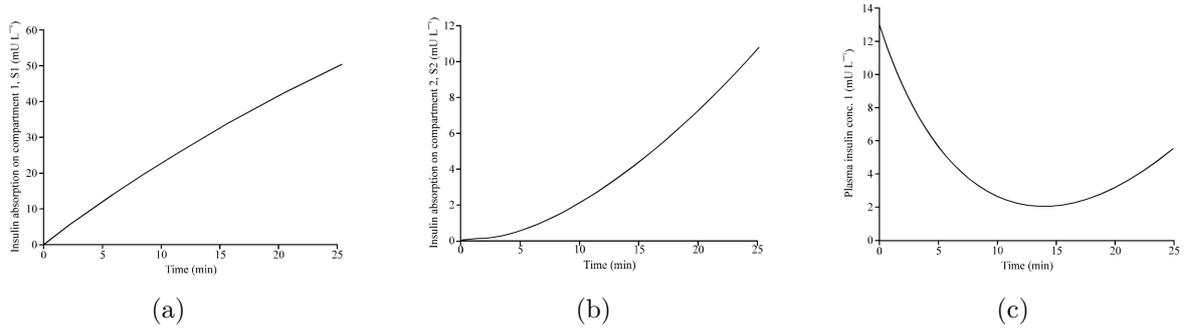


Figure 8: Insulin absorption on the first compartment S_1 (a), insulin absorption on the second compartment S_2 (b) and plasma insulin concentration (c)

Insulin effect subsystem study

Lastly we solve the system for the insulin effect and got the solutions for each compartment.

$$x_1(t) = \frac{e^{-k_{a1}t}(-1 + e^{k_{a1}t})I(t)k_{b1}}{k_{a1}}$$

$$x_2(t) = \frac{e^{-k_{a2}t}(-1 + e^{k_{a2}t})I(t)k_{b2}}{k_{a2}}$$

$$x_3(t) = \frac{e^{-k_{a3}t}(-1 + e^{k_{a3}t})I(t)k_{b3}}{k_{a3}}$$

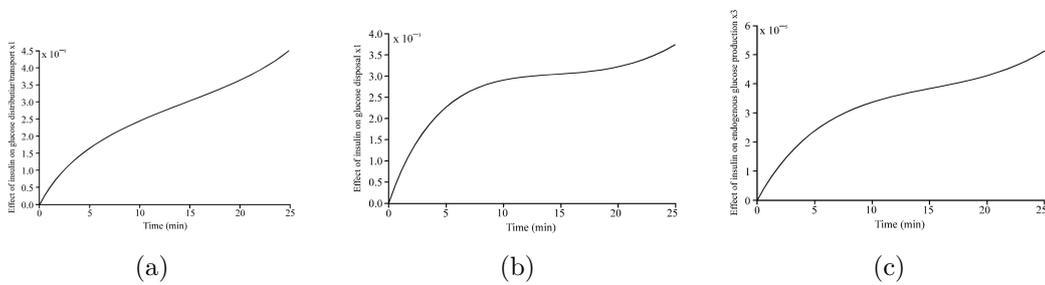


Figure 9: Insulin effect on glucose distribution and transport x_1 (a), insulin effect on glucose disposal x_2 (b) and insulin effect on endogenous glucose production x_3 (c)

3.4 Fractional Derivative

Numerical values of the parameters

We use the numerical values of the parameters presented in [14], [15].

Parameter	Numerical Value
g_b [mg/dL]	81
p_1 [1/min]	0.0337
p_2 [1/min]	0.0209
p_3 [L/(mU · min ²)]	$7.51 \cdot 10^{-6}$
n [1/min]	0.214
τ [1/L]	1/12
x_b [mU/mL]	$5.4 \cdot 10^{-6}$
t_{max} [min]	40
D_g [g]	60
A_g	0.8

Table 5: Numerical values of the parameters from the fraction derivative system.

Selection of functions $m(t)$, $u(t)$

Functions $m(t)$, $u(t)$ are selected, where $m(t)$ is from [14] and $u(t)$ is purposed by the authors.

$$m(t) = \frac{D_g A_g t e^{-t/t_{max}}}{t_{max}^2}$$

Where t_{max} is the time when the absorption is at its peak value, D_g are the carbohydrates in the meal and A_g is the fraction of absorbed glucose.

$$u(t) = k_1 t e^{k_2 t}$$

Where k_1 [mU/min], k_2 [1/min] are adjusting parameters. Function $u(t)$ only applies for t when $g(t) \neq g_b$.

Solution for small deviations

The solution is for small deviations in the basal value, thus we work with the Mittag-Leffler functions truncated to the first member.

$$E_{\alpha, \alpha}^{(0)}((\gamma)(t-s)^\alpha) \approx \frac{1}{\Gamma(\alpha)} - \frac{\gamma}{\Gamma(2\alpha)}(t-s)^\alpha$$

The solution of the system with all previous specifications is shown in the following equation.

$$i(t) = k_1 \tau \int_0^t (t-s)^\alpha e^{k_2(t-s)} \left[\frac{1}{\Gamma(\alpha)} - \frac{n}{\Gamma(2\alpha)}(t-s)^\alpha \right] ds$$

$$x(t) = k_1 \frac{\tau p_3}{\Gamma(2\alpha)} \int_0^t (t-s)^{2\alpha} e^{k_2(t-s)} ds$$

$$g(t) = \frac{D_g A_g}{t_{max}^2} \int_0^t (t-s)^\alpha e^{[-(t-s)/t_{max}]} \left[\frac{1}{\Gamma(\alpha)} - \frac{p_1 + x_b}{\Gamma(2\alpha)}(t-s)^\alpha \right] ds - k_1 \frac{g_b p_3 \tau}{\Gamma(2\alpha)} [A_n + B p_2 + C(p_1 + x_b)] \int_0^t (t-s)^{2\alpha} e^{k_2(t-s)} ds$$

Graphical representation

Finally we can plot the solution of the glucose, which is the most representative function, and find the differences in the control of glucose peaks for different α -orders of the fractional derivative.

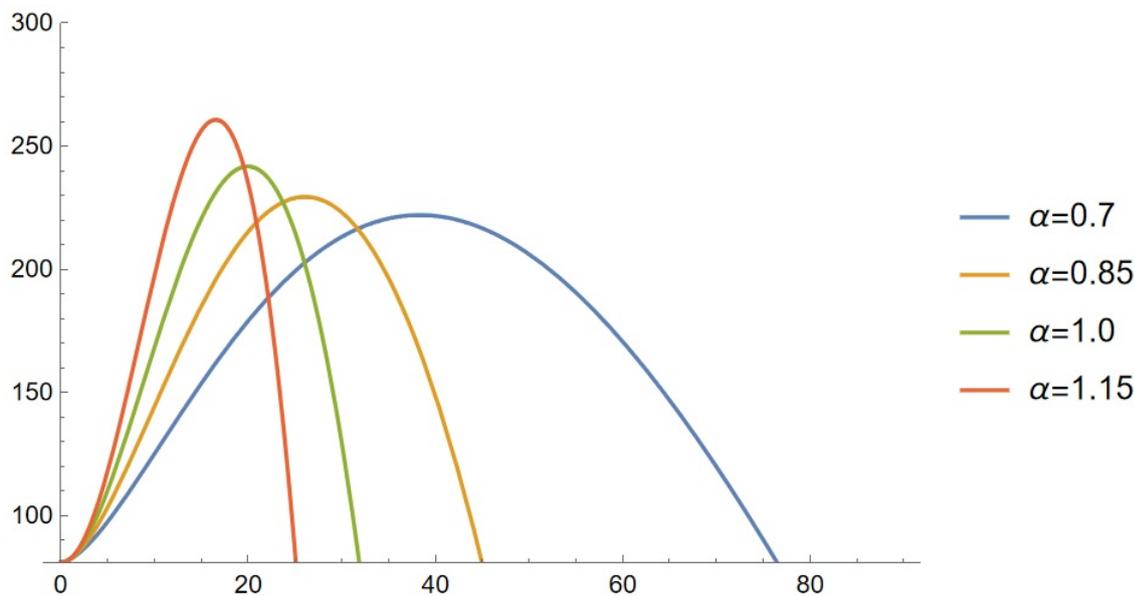


Figure 10: Plot of the dynamics of the glucose function $g(t) \in [81, 300][mg/dL]$, $t \in [0, 80]min$ for an array of α -orders.

4 Conclusions

For the Bergman model satisfactorily results are shown for several ingest functions. Nevertheless, this control has its limitation points. It does not take into account the delays provoked by the subcutaneous in the real insulin pump. This effect is taken into account in the Hovorka model. For the Hovorka model a solution for the system is achieved and a consistent with the reality graphical representation was shown. It is possible to see an improvement from the Bergman model but the added complexity of this model is seen also in the computational costs when solved.

The objective of the fractional model is to improve the results of the Bergman model. It takes into consideration the subcutaneous delays using an array of α -orders. This simplifies the complexity of adding auxiliary equations as in the Hovorka model.

A methodology for solving the system has been shown and a solution for general input functions of glucose and insulin has been obtained. The effect of the α -order in the fractional derivative is shown in the numerical results for inputs of simple functions.

Future work that can be made is an introduction of a PID control for the Hovorka and fractional models in order to obtain results for more complex and real functions.

References

- [1] R. N. BERGMAN ET AL, (1981), *Physiologic evaluation of factors controlling glucose tolerance in man: measurement of insulin sensitivity and beta-cell glucose sensitivity from the response to intravenous glucose.*, 10.1172/jci110398
- [2] KARAM, EKHLAS y JADOO, EMAN y HASSONY, EMAN, (2019), *Design Modified Robust Linear Compensator of Blood Glucose for Type I Diabetes Based on Neural Network and PSO Algorithm*, 29-36, 10.11648/j.cse.20190302.12
- [3] BONDIA, JORGE y ROMERO-VIVO, SERGIO y RICARTE, BEATRIZ y DIEZ, JOSE LUIS, (2018), *IEEE Control Systems Magazine, Insulin Estimation and Prediction: A Review of the Estimation and Prediction of Subcutaneous Insulin Pharmacokinetics in Closed-Loop Glucose Control*, 10.1109/MCS.2017.2766312.
- [4] GUSTAV DOETSCH, (1974) Springer-Verlag Berlin Heidelberg *Introduction to the Theory and Application of the Laplace Transformation*
- [5] ROMAN HOVORKA, VALENTINA CANONICO, LUDOVIC J CHASSIN, ULRICH HAUETER, MASSIMO MASSI-BENEDETTI, MARCO ORSINI FEDERICI, THOMAS R PIEBER, HELGA C SCHALLER, LUKAS SCHAUPP, THOMAS VERING AND MALGORZATA E WILINSKA *Nonlinear model predictive control of glucose concentration in subjects with type 1 diabetes*, *Physiological Measurements*, 25, pp. 905-920, 2004.
- [6] NUR FARHANA MOHD YUSOF, AYUB MD. SOM, AHMMED SAADI IBREHEM AND SHERIF ABDULBARI ALI *A Review of Mathematical Model Describing Insulin Delivery System for Type 1 Diabetes* *Journal of Applied Sciences*, 14, pp. 1465-1468, 2014
- [7] MOUGIAKAKOU, S., PROUNTZOU, K., & NIKITA, K. *A real time simulation model of glucose-insulin metabolism for type 1 diabetes patients*. 2005 *IEEE Engineering in Medicine and Biology 27th Annual Conference*, 2005, pp. 298–301.
- [8] LEE, J. C., KIM, M., CHOI, K. R., OH, T. J., KIM, M. Y., CHO, Y. M., KIM, K., KIM, H. C., & KIM, S. *In silico evaluation of glucose control protocols for critically ill patients*. *IEEE transactions on bio-medical engineering*, 2012, 59, pp. 54–57.
- [9] HEINEMANN L, LINKESCHOVA R, RAVE K, HOMPESCH B, SEDLAK M, HEISE T. *Time-action profile of the long-acting insulin analog insulin glargine (HOE901) in comparison with those of NPH insulin and placebo*. *Diabetes Care*. 2000
- [10] Y. CHEN, I. PETRAS, AND D. XUE, *Fractional Order Control. A tutorial*, *American Control Conference*, Hyatt Regency Riverfront, St. Louis, MO, USA, June 10-12, 2009, pp.1397-1411.
- [11] MARÍA RODRÍGUEZ MARTÍN, ANTONIO LÓPEZ MONTES, *Introducción al cálculo fraccionario y a los modelos de crecimiento tumoral clásicos y fraccionarios*, Universidad Complutense de Madrid, Facultad de Ciencias Matemáticas, 2020.
- [12] ANTÓN LOMBARDEO OZORES, *Fractional Calculus and newtonian dynamics.*, *Revista de investigación GIE Pensament Matemàtic*, Volumen IV, Número 1, pp.077-106 (2014).
- [13] A. OUSTALOUP, *La Dérivation non Entière: Theorie, Synthèse, et Applications*, Hermes, Paris, 1995.

- [14] SIMONA COMAN, CRISTIAN BOLDISOR, LAURA FLOROIAN, *Fractional Adaptive Control for a Fractional – Order Insuline – Glucose Dynamic Model*, 2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP)

- [15] JIMING CHEN, KEJIE CAO, YOUXIAN SUN, YANG XIAO, XU (KEVIN) SU, *Continuous Drug Infusion for Diabetes Therapy: A Closed-Loop Control System Design*, EURASIP Journal on Wireless Communications and Networking, Vol.2008, Article ID 495185, 2008, pp. 1-10.

Graph Neural Network Convolutions: mathematical principles and an application to chemistry

Enric Alberola Boloix ^b, Pablo Merino San José [‡] and Ángel Rolando [#]

(b) Departamento Matemática Aplicada, Universitat Politècnica de València,
ealbbol@posgrado.upv.es

(‡) Departamento Matemática Aplicada, Universitat Politècnica de València,
pmersan1@posgrado.upv.es

(#) Departamento Matemática Aplicada, Universitat Politècnica de València,
anmoquin@alumni.uv.es

1 Introduction

In this article we present a summary of some of the main mathematical principles on which convolutional neural networks in graphs are based, followed by an application to a chemical database. In the first part, we make a concise and general introduction to convolutions in learning theory and to graph neural networks (GNN). In the second part, we present the mathematical framework in which convolutions are extended from the classical domain to the graph domain, making first the distinction between spatial and spectral approaches and focusing on the latter approach. In the third part, we end up relying on the theoretically robust nature of the spectral properties of a graph, based on the eigen-decomposition of its Laplacian matrix, and we deal with its main practical limitations, such as sensitivity to scalability or lack of locality, through a polynomial approximation of the convolutional filter. Nowadays, finding a reliable and easy to handle approximation of such a filter is the key for the efficiency of spectral GNN methods. We provide a powerful candidate based on Chebychev polynomials, as an alternative to a broad range of different approximation schemes. In [6], they experiment with spectral non-parametric and parametric filters, the latter built with cubic splines. In [3], they construct a model through Lanczos algorithm. Another example is [1], where they consider Cayley polynomials in the Laplacian, using more general parametric methods through rational complex functions. Once set up our general setting, we finally design a spectral GNN method using several convolutional layers and the aforementioned Chebychev polynomial approximation for the classification of chemical elements in a database of near 1 billion molecules. This article can be of interest to researchers in the fields of Graph Theory, Signal Processing, Machine Learning, Organic Chemistry and Bioinformatics.

2 Main results

After the exposition and distinction of spatial and spectral approaches, we apply the following model of convolutions with intermediate ReLU nonlinearities and a final softmax activation function, given an initial features matrix X as input:

$$Z_1 = X,$$

$$\begin{aligned}
Z_2 &= \text{ReLU}(\hat{A}Z_1W^{(1)}) + Z_1, \\
Z_3 &= \text{ReLU}(\hat{A}Z_2W^{(2)}) + Z_2, \\
Z_4 &= \text{softmax}(\hat{A}Z_3W^{(3)}).
\end{aligned}
\tag{1}$$

As we see, we add in each layer the embedding information from previous layer, not only through \hat{A} , but also by direct summation. The reason of including such a variant from the proposed model is that we want to take into account residual connections between layers.

In (1), $W^{(i)}$, for $i \in \{1, 2, 3\}$, are weights matrices to train, and the final nonlinearity is

$$\text{softmax}(x_j) = \frac{1}{Z} \exp(x_j), \quad (Z = \sum_{i=1}^N \exp(x_i)), \quad j \in \{1, \dots, N\},
\tag{2}$$

applied row by row. In turn, intermediate nonlinearities are applied component-wise, recalling that $\text{ReLU}(x) = xH(x)$, for H the Heaviside function.

The philosophy of this statistical learning method is semi-supervised, what means that, to penalize misclassified labels, we use the cross-entropy loss function in the following way:

$$\mathcal{L} = - \sum_{l \in \mathcal{Y}_l} \sum_{f=1}^F Y_{lf} \log(Z_{lf}),
\tag{3}$$

where \mathcal{Y}_l is the subset of nodes with known label or feature.

The way we train such matrices $W^{(i)}$ is through gradient descent, using a stochastic optimization procedure called Adam [7]. For such a phase, we use the entire training dataset in each training iteration, obtained from a pre-processing part of our code that gives us training, testing and validation samples. With a sparse representation of A , necessary memory will be $\mathcal{O}(|E|)$.

3 Numerical experiments

With the general method clarified, we apply it to the dataset QM7, a database of nearly 1 billion stable and synthetically accessible organic molecules, composed of all molecules of up to 23 atoms (including 7 heavy atoms C, N, O, and S), totalling 7165 types of molecules, each of them considered as a simple and undirected graph (see <http://quantum-machine.org/datasets/> for more detail). Our objective is to predict which chemical element is located in each of the unlabelled nodes of the graph, after some pre-processing work with the Coulomb matrix (see [8]). Moreover, we present some plots that elucidate how competitive is the proposed GCN model.

4 Conclusions

1. Our model presents sensitivity to imbalanced classes. We see that the chemical element S presents an accuracy score of nearly 1, although its scarce presence in the dataset. It is partially due to the presence of previous layer embeddings Z_l in the propagation to the next layer Z_{l+1} .
2. In general terms, this reference dataset yields an idea of a precise method in semi-supervised prediction.
3. Computational complexity is limited to linear dependencies on $|E|$, given the sparse condition of the adjacency matrix. Notice that we are dealing with 7165 graphs, with 23^2 nodes each one, and a time computation of around 17 minutes.

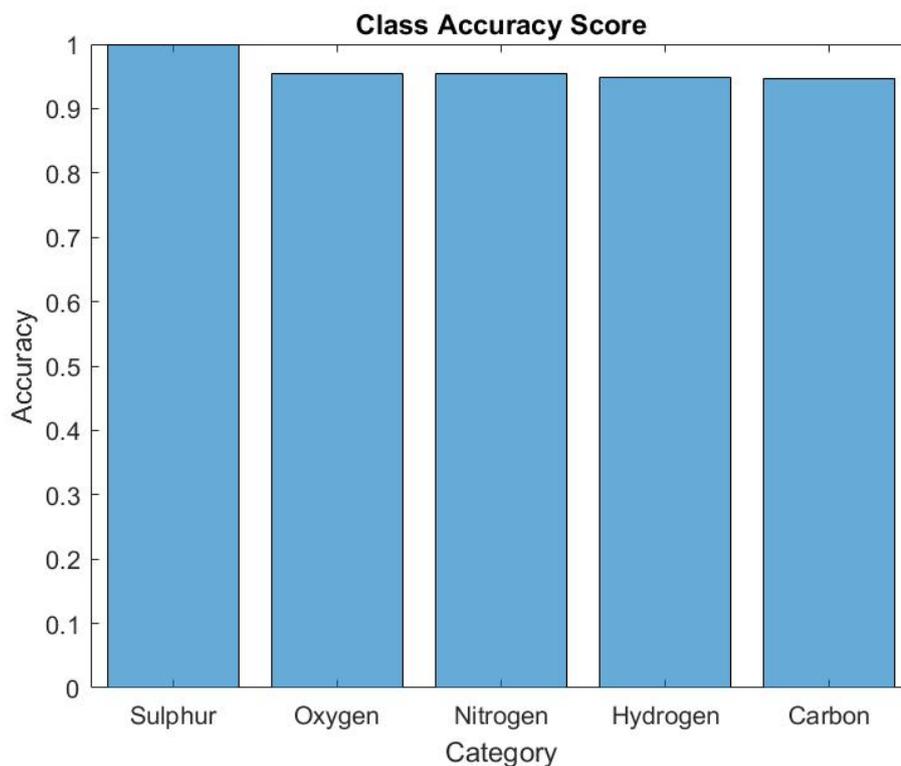


Figure 1: Class accuracy score histogram of the semi-supervised proposed Graph CNN model for QM7.

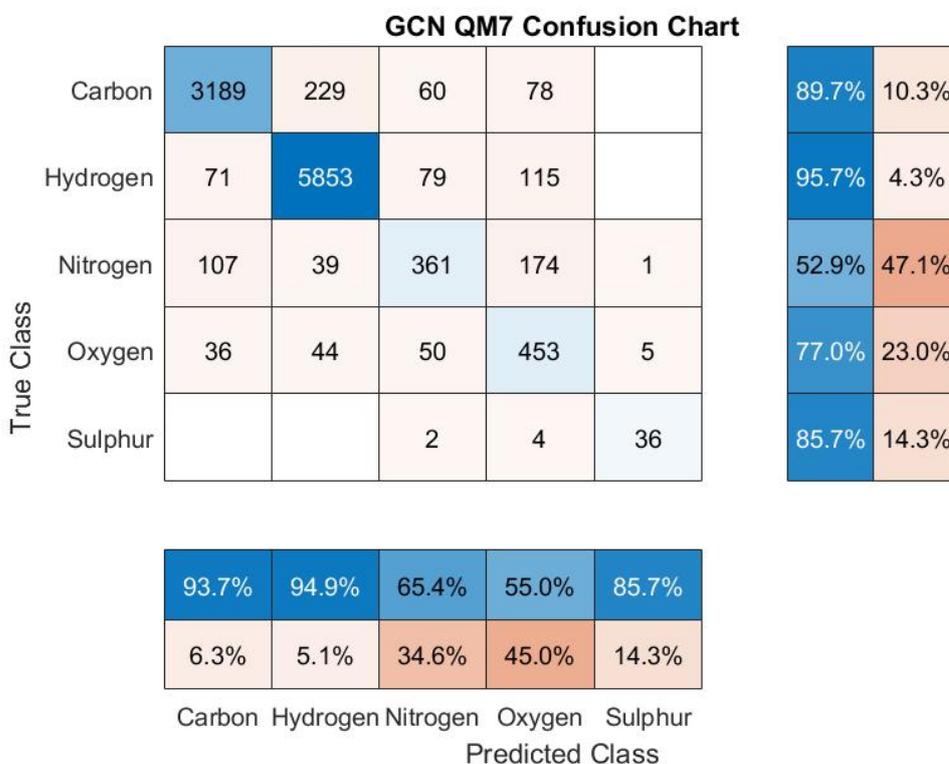


Figure 2: Confusion chart for the semi-supervised proposed Graph CNN model for QM7.

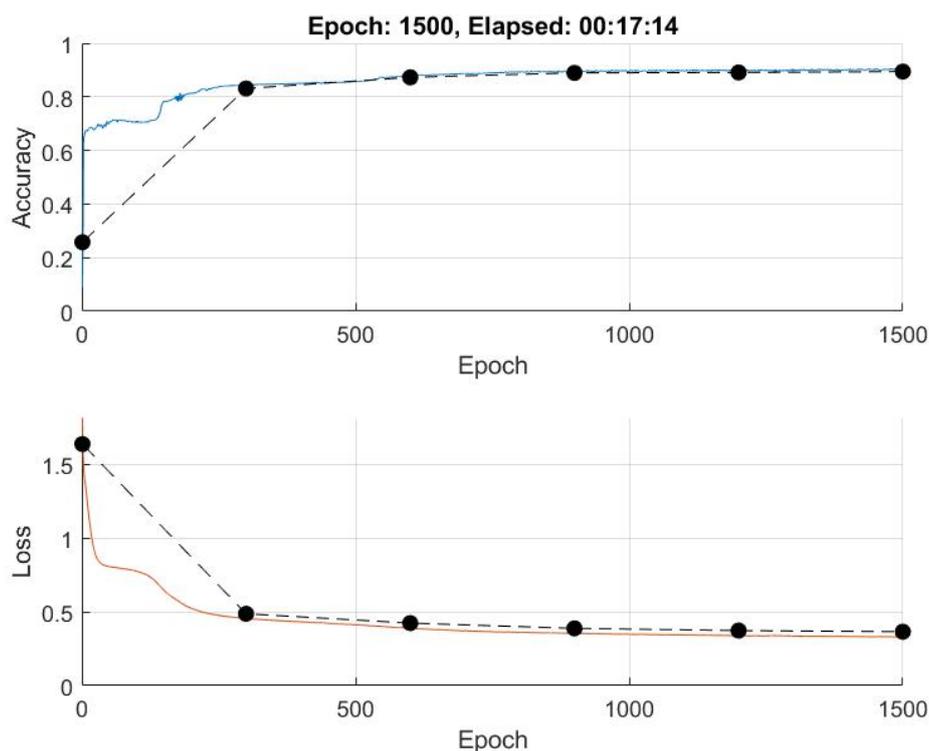


Figure 3: Evolution of accuracy error and loss function (cross-entropy) for QM7 dataset, 1500 epochs of training with gradient descent, learning rate 0.01, accuracy score of 0.900419.

- Moreover, the arbitrariness of the selected graph suggests that this model is powerful against arbitrary simple and undirected graphs.

We imply 1500 epochs for the gradient descent training procedure, and we compute two entities that yield information of carried out predictions: accuracy score and confusion chart. This practice is possible because, as we saw, the proposed method is semi-supervised.

The former is computed with known-label samples from a subset of the dataset employed for validation. Using the cross-entropy loss function from (3), we can obtain a final error value over the forementioned subset of samples. According to the latter entity, we give a matrix with the number of correctly and incorrectly predicted labels over the subset of validation samples. This is called *confusion chart*.

In the presented graphics, we show the following:

- In figure 3, we represent accuracy score and loss function values in each epoch of the training phase.
- In figure 2, we represent the confusion chart. On the right and below the matrix, we see a summary of the percentages of correctly and incorrectly predicted labels, per chemical element (observe that, in the matrix, diagonal elements are correctly predicted, and non-diagonal elements are uncorrectly predicted).
- In figure 1, we represent, through an histogram, the value of the accuracy score for each chemical element that constitute the studied molecules.

Financial disclosure

This research was partially supported by Spanish Ministerio de Ciencia, Innovación y Universidades PGC2018-095896-B-C22, by the internal research project ADMIREN of Universidad Internacional de La Rioja (UNIR) and was partially supported by Universitat Politècnica de València Contrato Predoctoral PAID-01-20-17 (UPV).

References

- [1] M. BRONSTEIN, *Deriving Convolution from first principles*, <https://towardsdatascience.com/deriving-convolution-from-first-principles-4ff124888028>, 2020.
- [2] M. DEFFERRARD ET AL, *Convolutional Neural Networks on Graphs with Fast Localized Spectral Filtering*, International Conference on NIPS, **30** : 3844–3852, 2016.
- [3] R. LIAO ET AL, *LanczosNet: Multi-Scale Deep Graph Convolutional Networks*, ICLR, 2019.
- [4] T.N. KIPF AND M. WELLING, *Semi-Supervised Classification with Graph Convolutional Networks*, ICLR, 2017.
- [5] D.K. HAMMOND ET AL, *Wavelets on graphs via spectral graph theory*, Applied and Computational Harmonic Analysis, **30(2)** : 129–150, 2011.
- [6] J. BRUAN ET AL, *Spectral Networks and Locally Connected Networks on Graphs*, arXiv preprint arXiv:1312.6203., 2013.
- [7] KINGMA D.P. ET AL, *Adam: A method for stochastic optimization*, arXiv preprint arXiv:1412.6980, 2014.
- [8] RUPP M. ET AL, *Fast and Accurate Modeling of Molecular Atomization Energies with Machine Learning*, Physical review letters, **108(5)**, 2012.

Cryptographic systems: a mathematical review

Pérez-Diukina, C.^{1*}, Sabater-García, P.^{1**} and Zaragoza-Chichell, J.^{1***}

(1) Universitat Politècnica de València, València, Spain.

(1*) cperdiu@posgrado.upv.es

(1**) psabgar@posgrado.upv.es

(1***) juazachi@inf.upv.es

1 Introduction

With the ever increasing amount of information stored online, it is critical to securely maintain sensitive data. Mathematics has played a central role in ensuring that this information cannot be accessed by unwanted third parties. In this work we introduce how algebra rudiments, hand in hand with computation, can help us encode data and restrict readability of such data to only those provided with specific insight into the mathematical model. Among some of the most studied are the discrete logarithm problem, Elliptic Curve Cryptography (ECC), the Rivest–Shamir–Adleman public-key cryptosystem (RSA), and hash functions. In this article we introduce these algorithms as well as the cryptanalysis of RSA.

2 Discrete logarithm problem

The discrete logarithm problem arises in an cyclic subgroup of an abelian group where we do not know the integer to which we must raise a certain element of the group to get to another one. The elements of the group encode messages, their discrete logarithms are the key to decipher them.

Suppose we have a group G , an element $g \in G$ such to $o(g) = n \in \mathbb{N}$, we have another element $h \in G$ and we want find a number $m \in \mathbb{Z}$ such to $g^m = h$. Since the problem of finding this number is sufficiently difficult, messages are encrypted in such a way that to decrypt them it must be solved.

A particular case of the discrete logarithm problem is when the working group is an elliptic curve, which is a subset of the product of a field with itself, to which is added an infinite point on the

vertical axis, and has defined on it a summation operation, for which this infinite point is the neutre.

The elliptic curve is $E = \{(x, y) \in \mathbb{F}_q : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ where $\mathbb{F}_q = \mathbb{Z}_p / \langle f(x) \rangle$, being p a prime number, $q = p^m$, $m \in \mathbb{Z}$ and $f(x) = x^3 - x \in \mathbb{Z}_p[x]$. $E = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. An additive law is defined and the discrete logarithm problem over E is posed.

3 Hash Functions

Regarding internet's security, password management is one of the most important topics. In the olden days, websites that required user authentication would store every user's password in their database. However, time proved that such thing was not a good idea and that is where hash functions come in handy.

Hash functions are nothing else but maps that take an arbitrary size binary array into a fixed size binary array. There are many different hash functions and they satisfy different properties depending on what they are meant to be used for. Anyway, we are only interested in the so called *cryptographic hash functions*. Every cryptographic hash function must satisfy three properties: Denote by $\{0, 1\}^* = \cup_{n \in \mathbb{N}} \{0, 1\}^n$ the set of arbitrary long binary arrays. So, let $h : \{0, 1\}^* \rightarrow \{0, 1\}^M$ be a hash function. Then we say that it is a cryptographic hash function if:

- It is preimage resistant, i.e., if given a $y \in \{0, 1\}^N$ it is hard to find a $x \in \{0, 1\}^*$ such that $h(x) = y$.
- It is second preimage resistant, i.e., if given a $x_1 \in \{0, 1\}^*$ and $y = h(x_1)$ it is hard to find another $x_2 \in \{0, 1\}^*$ such that $y = h(x_2)$.
- It is collision resistance, i.e., if it is hard to find any two $x_1, x_2 \in \{0, 1\}^*$ such that $h(x_1) = h(x_2)$.

Any good hash function should be fast to compute, safe and, of course, deterministic. However, in real life problems, fastness is usually preferred over safety. In that sense, hash functions are usually asked to verify what is known as the avalanche effect: if only one bit in an input is changed, each output bit will have 50% chance of changing.

Among the many hash functions that have been published, perhaps SHA-1 [4] has a special place in history. Although its use is not recommended today, it is predecessor to SHA-256 [5] and SHA-512, which are still in use today.

Another widely use of hash functions is that of digital signatures, a procedure to ensure the

authenticity of a document. Typical implementations come from an extension of RSA cryptosystem [7].

However, one should keep in mind that the use of cryptographic hash functions does not only apply to the previously specified scenarios. For example, they are the grounding stone to Bitcoin and Ethereum and the block-chain technology by extension.

4 The RSA algorithm

Before introducing the RSA algorithm it is important to understand the concept of public key cryptosystems. Such a cryptosystem can be described by a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where \mathcal{P} is the set of plaintexts, \mathcal{C} is the set of ciphertexts produced by an encryption function $E \in \mathcal{E}$, \mathcal{K} is the set of keys, and \mathcal{D} is the set of decryption functions. $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ must also verify that for each $K \in \mathcal{K} \exists E_K \in \mathcal{E}, D_K \in \mathcal{D} : D_K(E_K(P)) = P, \forall P \in \mathcal{P}$.

The RSA algorithm was first introduced by Rivest, Shamir, and Adleman in 1977 and then described in detail in their 1978 paper [7]. The algorithm can be summarized as follows: Let $d, e, n \in \mathbb{Z}_+$ be positive integers such that $n = pq$ where p and q are large primes. We have $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, the integers modulo n . Then the keyspace is defined as follows:

$$\mathcal{K} := \{(n, p, q, e, d) : ed \equiv 1 \pmod{\phi(n)}\}$$

where ϕ is Euler's totent function, $\phi(n) = (p-1)(q-1)$.

The security of the RSA algorithm depends on the level of difficulty of the RSA problem. This problem consists in computing the plaintext given only the public key and ciphertext. Solving this problem is equivalent in difficulty to inverting the RSA function. Currently, there exist no efficient algorithms to invert the RSA function. Determining how difficult it is to invert is an open problem. There have been many algorithms proposed but none have achieved a total break if n is large enough and the algorithm is correctly implemented [3].

RSA is a very popular algorithm, but data analysis has showed that ECC outperforms RSA in both implementation time, storage requirements, and security [1, 2]. This makes ECC a great way to encrypt data on devices with low computational power or for businesses that process large amounts of customer data [8, 9]. In its 2020 report the National Institute of Standards and Technology (NIST) has warned that when quantum computing becomes a practical consideration, the security-strength estimates for RSA and ECC algorithms will be significantly affected [6].

5 Conclusion

With the great computational advance the cryptosystems currently used have also greatly gained in complexity. We have reviewed the mathematical structure of a few popular cryptosystems (RSA,ECC,SHA) and how they are used in everyday life. We also documented the security features of RSA and ECC. We concluded that both RSA and ECC are extremely hard to break without the decryption key but RSA needs larger key sizes than ECC to achieve the same security level. It is important to remark that the emergence of quantum computing the security of these cryptosystems will be greatly compromised.

References

- [1] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmud and Zurina Mohd Hanapi, *Comparison of ECC and RSA algorithm in resource constrained devices*, In 2013 International Conference on IT Convergence and Security (ICITCS),, 1–3. IEEE, 2013.
- [2] Dindayal Mahto and Dilip Kumar Yadav., *Performance analysis of rsa and elliptic curve cryptography*, International Conference on NIPS, 20(4):625–635, 2018.
- [3] Majid Mumtaz and Luo Ping, *Forty years of attacks on the rsa cryptosystem: A brief survey*, Journal of Discrete Mathematical Sciences and Cryptography, 22(1):9–29, 2019.
- [4] National Institute of Standards and Technology, *FIPS PUB 180-1: Secure hash standard*, April 2002.
- [5] National Institute of Standards and Technology, *FIPS PUB 180-2: Secure hash standard*, August 2002.
- [6] Patrick O'Really, Kristina Rigopoulos, Larry Feldman, Greg Witte, et al, *2020 Cybersecurity and privacy annual report*, NIST SPECIAL PUBLICATION, 800:214, 2021. August 2002.
- [7] Ronald L Rivest, Adi Shamir, and Leonard Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21(2):120–126, 1978.
- [8] Olufunke R. Vincent, Olusegun Folorunso and AD Akinde, *Improving e-payment security using elliptic curve cryptosystem*, Electronic Commerce Research, 10(1):27–41, 2010.
- [9] Eun-Jun Yoon and Kee-Young Yoo. *Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc*, In 2009 International Conference on Computational Science and Engineering, volume 2, 633–640. IEEE, 2009

Partial Differential Equations in Random Walk Spaces

Álvaro González Cortés ^b, Daniel Isert Sales [‡] and Eduardo Sena Galera [#]

(b) algoncor@alumni.uv.es

(‡) isada@alumni.uv.es

(#) segae@alumni.uv.es

1 Introduction

The digital world has brought with it many different kinds of data of increasing size and complexity. Indeed, modern devices allow us to easily obtain images of higher resolution, as well as to collect data on internet searches, healthcare analytics, social networks, geographic information systems, business informatics, etc. Consequently, the study and treatment of these big data sets is of great interest and value. In this respect, weighted discrete graphs provide a natural and flexible workspace in which to represent the data. In this context, a vertex represents a data point and each edge is weighted according to an appropriately chosen measure of “similarity” between the corresponding vertices. Historically, the main tools for the study of graphs came from combinatorial graph theory. However, following the implementation of the graph Laplacian in the development of spectral clustering in the seventies, the theory of partial differential equations on graphs has obtained important results in this field. This has prompted a big surge in the research of partial differential equations on graphs. Moreover, interest has been further bolstered by the study of problems in image processing. In this area of research, pixels are taken as the vertices and the “similarity” between pixels as the weights. The way in which these weights are defined depends on the problem at hand.

On another note, let $J: \mathbb{R}^N \rightarrow \mathbb{R}$ be a nonnegative, radially symmetric and continuous function with $\int_{\mathbb{R}^N} J(z) dz = 1$. Nonlocal evolution equations of the form

$$u_t(x, t) = \int_{\mathbb{R}^N} J(y - x) u(y, t) dy - u(x, t) \quad (1)$$

and variations of it, have naturally arisen in various scientific fields as a means of modelling

a wide range of diffusion processes. An intuitive reasoning for the wide applicability of this model comes from thinking of $u(x, t)$ as the density of a “population” at a point x at time t and of $J(y - x)$ as the probability distribution of moving from y to x in one “jump”. Then, $\int_{\mathbb{R}^N} J(y - x)u(y, t)dy$ is the rate at which “individuals” are arriving at x from anywhere else and $-u(x, t) = -\int_{\mathbb{R}^N} J(y - x)u(y, t)dy$ is the rate at which they are leaving location x . Therefore, in the absence of external or internal sources, we are lead to equation 1 as a model for the evolution of the population density over time. In the previous two paragraphs, we have brought forward two instances in which there is great interest in the study of partial differential equations in a nonlocal (or discrete) setting. Further interest has arisen following the analysis of the peridynamic formulation of the continuous mechanic, the study of Markov jump processes and other nonlocal models.

The aim of this article is to unify into a broad framework the study of many of the previously mentioned problems. In order to do so, we note that there is a strong relation between some of these problems and probability theory, and it is in this field in which we find the appropriate spaces in which to develop this unifying study. Let (X, \mathcal{B}) be a measurable space and $P : X \times \mathcal{B} \rightarrow [0, 1]$, a transition probability kernel on X . Then, a Markovian transition function can be defined as follows: for any $x \in X$, $B \in \mathcal{B}$, let

$$P_t(x, B) := e^{-t} \sum_{n=0}^{\infty} \frac{t^n}{n!} P^n(x, B), \quad t > 0,$$

where P^n denotes the n -step transition probability kernel.

In this setting, particular choices of the measurable space (X, \mathcal{B}) and of P will lead to some of the previous problems. For example, if $X = \mathbb{R}^N$ and $P(x, dy) = J(y - x)dy$, we will recover equation 1. Moreover, taking X to be the set of vertices of a weighted discrete graph and appropriately defining the transition probability function in terms of the weights we are also able to recover the heat equation on graphs.

The previous remarks suggest that the appropriate setting in which to fulfill our goals of unifying a wide variety of nonlocal models into broad framework is provided by random walk spaces. These spaces are constituted by a measurable space (X, \mathcal{B}) and a transition probability kernel P on X which encodes the jumps of a Markov process. We will adopt the notation $m_x = P(x, \cdot) \in \mathcal{P}(X, \mathcal{B})$ for each $x \in X$ (here $\mathcal{P}(X, \mathcal{B})$ denotes the space of probability measures on (X, \mathcal{B})). Additionally, we will require a kind of stability property to hold for these spaces, that is, the existence of an invariant measure ν . Then, we will say that $[X, \mathcal{B}, m, \nu]$ is a random walk space. Owing to the generality of these spaces, the results that we obtain will have a wide range of applicability to a large spectrum of evolution problems arising in a variety of scientific fields. Unfortunately, this framework does not cover problems related with the fractional kernel due to its singular nature.

During the last years and with the aforementioned goal in mind, we have studied some gradient flows in the general framework of a random walk space. In particular, we have studied the heat flow, the total variation flow and the ROF Model. Specifically, together with the existence and uniqueness of solutions to these problems and the asymptotic behavior of its solutions, a wide variety of their properties have been studied, as well as the nonlocal diffusion operators involved in them.

1.1 Structure of the article

Let us shortly describe the contents of the article. To start with, in Section 1, we introduce the general framework of a random walk space. We relate it to classical notions in Markov chain theory and provide a list of results which we hope aid the reader in getting a good idea about the properties which these spaces enjoy. After introducing a stability property for random walk spaces, called m -connectedness, we continue exploring the characteristics enjoyed by this notion and we relate it to known concepts of ergodicity. We then provide a list of examples of random walk spaces of particular interest, as those that were mentioned at the beginning of the introduction. The rest of the section is dedicated to introducing the nonlocal counterparts of classical notions like those of gradient, divergence, boundary, perimeter, mean curvature and Ricci curvature, as well as of the Laplace operator. In doing so, we obtain results which mimic classic results in the local case and, moreover, obtain further characterizations of the m -connectedness of a random walk space. We also spend some time in finding sufficient conditions for Poincaré type inequalities to hold and relate them both to the gap of the Laplace operator and to isoperimetric inequalities.

Section 2 focuses on the study of the heat flow in random walk spaces. In our context, associated with the random walk $m = \{m_x\}_{x \in X}$, the Laplace operator Δ_m is defined as

$$\Delta_m f(x) = \int_X (f(y) - f(x)) dm_x(y).$$

Assuming that the invariant measure ν satisfies a reversibility condition with respect to the random walk, the operator $-\Delta_m$ generates in $L^2(X, \nu)$ a Markovian semigroup $\{e^{t\Delta_m}\}_{t \geq 0}$ called the heat flow in the random walk space. Moreover, we are able to characterise the infinite speed of propagation of the heat flow in terms of the m -connectedness of the random walk space. In addition, in Subsection 2.4, we study the asymptotic behaviour of the semigroup $\{e^{t\Delta_m}\}_{t \geq 0}$ and with the help of a Poincaré inequality we obtain rates of convergence of $\{e^{t\Delta_m}\}_{t \geq 0}$ as $t \rightarrow \infty$.

In Section 3 we study the total variation flow. For this purpose, we introduce the 1- Laplacian operator associated with a random walk space and obtain various characterizations of it. We then proceed to prove existence and uniqueness of solutions of the total variation flow in random walk spaces and to study its asymptotic behaviour with the help of some Poincaré type inequalities.

Section 4 is dedicated to the study of the (BV, L^p) -decomposition, $p = 1$ and $p = 2$, of functions in random walk spaces. This is done by studying the Rudin-Osher-Fatemi model both with L^2 and with L^1 fidelity terms. We obtain the Euler-Lagrange equations of these minimization problems and proceed to obtain a wide range of results on the properties enjoyed by the minimizers.

2 Main Results

The main results that appear in the work are the following.

2.1 The heat Flow

First result is an adaptation of a well know formula to the theory of random walk spaces. It will be helpful several times along the work.

Proposition 1. (*Integration by parts formula*) *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. Then,*

$$\int_X f(x) \Delta_m g(x) d\nu(x) = -\frac{1}{2} \int_{X \times X} \nabla f(x, y) \nabla g(x, y) d(\nu \otimes m_x)(x, y) \quad (2)$$

for $f, g \in L^1(X, \nu) \cap L^2(X, \nu)$.

Next characterization is also important for further results.

Theorem 1. *Let $[X, \mathcal{B}, m, \nu]$ be a random walk space and suppose that ν is a probability measure. Then,*

$$[X, \mathcal{B}, m, \nu] \text{ is } m\text{-connected} \Leftrightarrow \Delta_m \text{ is ergodic}$$

To see some examples of random walk spaces we recommend the reader to visit chapter 2 of [13].

The first important result concerning the heat flow is the following. In this result we claim that the closed symmetric form that we define before is a Dirichlet form.

Theorem 2. *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. Then, $-\Delta_m$ is a non-negative self-adjoint operator in $L^2(X, \nu)$ with associated closed symmetric form \mathcal{E}_m . In fact, \mathcal{E}_m is Markovian and, therefore, a Dirichlet form.*

As a consequence of an important result in semigroup theory we know that $e^{t\Delta_m} u_0$ is the unique solution of the heat equation. In the next Theorem we introduce a form of representing this solution by means of power series.

Theorem 3. *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. Let $u_0 \in L^1(X, \nu) \cap L^2(X, \nu)$. Then,*

$$e^{t\Delta_m} u_0(x) = e^{-t} \sum_{n=0}^{+\infty} \int_X u_0(y) dm_x^{*n}(y) \frac{t^n}{n!} \quad \text{for every } x \in X \text{ and } t > 0. \quad (3)$$

In particular, for $D \in \mathcal{B}$ with $\nu(D) < +\infty$, we have

$$e^{t\Delta_m} \chi_D(x) = e^{-t} \sum_{n=0}^{+\infty} m_x^{*n}(D) \frac{t^n}{n!} \quad \text{for every } x \in X \text{ and } t > 0.$$

Starting from the solution of the heat equation, we can characterize the m -connected random walk spaces. This is known as the infinite propagation speed.

Theorem 4. Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. $[X, \mathcal{B}, m, \nu]$ is m -connected if, and only if, for any non- ν -null $0 \leq u_0 \in L^1(X, \nu) \cap L^2(X, \nu)$, we have that $e^{t\Delta_m} u_0 > 0$ for ν -a.e. $x \in X$ and all $t > 0$.

As for the last important result, we study the asymptotic behaviour of the semigroup $\{e^{t\Delta_m} u_0\}_{t \geq 0}$.

Proposition 2. Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. For every $f \in L^2(X, \nu)$,

$$\lim_{t \rightarrow \infty} e^{t\Delta_m} f = f_\infty \in \{u \in L^2(X, \nu) : \Delta_m u = 0\}.$$

Suppose that $[X, \mathcal{B}, m, \nu]$ is m -connected, then,

(i) if $\nu(X) = +\infty$, $f_\infty = 0$ ν -a.e.

(ii) if ν is a probability measure, $f_\infty = \int_X f(x) d\nu(x)$ ν -a.e.

2.2 Total Variation Flow

Since its introduction as a means of solving the denoising problem in the seminal work by Rudin, Osher and Fatemi ([12]), the total variation flow has remained one of the most popular tools in Image Processing. Furthermore, the use of neighbourhood filters by Buades, Coll and Morel in [5] has led to an extensive literature in nonlocal models in image processing. Consequently, there is great interest in studying the total variation flow in the nonlocal context. Moreover, a different line of research considers an image as a weighted discrete graph, where the pixels are taken as the vertices and the “similarity” between pixels as the weights. Therefore, the study of the 1-Laplacian operator and the total variation flow in random walk spaces has a potentially broad scope of application. The main results from this section will be, essentially, auxiliary to prove theorems from section 4:

Theorem 5 (Coarea formula). Let $[X, \mathcal{B}, m, \nu]$ be a random walk space. For any $u \in L^1(X, \nu)$, let $E_t(u) := \{x \in X : u(x) > t\}$. Then,

$$TV_m(u) = \int_{-\infty}^{+\infty} P_m(E_t(u)) dt. \quad (4)$$

Theorem 6. Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space. Let $u \in L^2(X, \nu)$ and $v \in L^2(X, \nu)$. The following assertions are equivalent:

(i) $v \in \partial\mathcal{F}_m(u)$;

(ii) there exists $\mathbf{z} \in X_m^2(X, \nu)$ with $\|\mathbf{z}\|_{L^\infty(X \times X, \nu \otimes m_x)} \leq 1$ such that

$$v = -\operatorname{div}_m \mathbf{z} \quad (5)$$

and

$$\int_X u(x)v(x)d\nu(x) = \mathcal{F}_m(u); \quad (6)$$

(iii) there exists $\mathbf{z} \in X_m^2(X, \nu)$ with $\|\mathbf{z}\|_{L^\infty(X \times X, \nu \otimes m_x)} \leq 1$ such that (5) holds and

$$\frac{1}{2} \int_{X \times X} \nabla u(x, y) \mathbf{z}(x, y) d(\nu \otimes m_x)(x, y) = \mathcal{F}_m(u); \quad (7)$$

(iv) there exists $\mathbf{g} \in L^\infty(X \times X, \nu \otimes m_x)$ antisymmetric with $\|\mathbf{g}\|_{L^\infty(X \times X, \nu \otimes m_x)} \leq 1$ such that

$$v(x) = - \int_X \mathbf{g}(x, y) dm_x(y) \quad \text{for } \nu\text{-a.e } x \in X, \quad (8)$$

and

$$- \int_X \int_X \mathbf{g}(x, y) dm_x(y) u(x) d\nu(x) = \mathcal{F}_m(u). \quad (9)$$

(v) there exists $\mathbf{g} \in L^\infty(X \times X, \nu \otimes m_x)$ antisymmetric, satisfying (8) and

$$\mathbf{g}(x, y) \in \text{sign}(u(y) - u(x)) \quad \text{for } (\nu \otimes m_x)\text{-a.e. } (x, y) \in X \times X. \quad (10)$$

2.3 The ROF-model

Let us recall the classic problem in image restoration. Given a corrupted image $f : \Omega \rightarrow \mathbb{R}$ on, for example, a rectangle Ω in \mathbb{R}^2 , the aim is to remove the noise or corruption in order to obtain the desired “clean” image $u : \Omega \rightarrow \mathbb{R}$, which is related to the original one by

$$f = u + n,$$

when n is the additive noise. Unfortunately, the problem of recovering u from f is ill-posed. To handle this problem, Rudin, Osher and Fatemi (see [12]) proposed to solve the following constrained minimization problem over $BV(\Omega)$:

$$\text{Minimize } \int_\Omega |Du| \quad \text{subject to } \int_\Omega u = \int_\Omega f \quad \text{and} \quad \int_\Omega |u - f|^2 = \sigma^2. \quad (11)$$

The first constraint corresponds to the assumption that the noise has zero mean, and the second that its standard deviation is σ . Problem (11) is naturally linked to the following unconstrained problem (called the ROF-model):

$$\min \left\{ \int_\Omega |Du| + \frac{\lambda}{2} \|u - f\|_2^2 : u \in BV(\Omega) \right\}, \quad (12)$$

for some Lagrange multiplier $\lambda > 0$. It has been proved an existence and uniqueness result for (11), as well as the link between (11) and (12). The constant λ in (12) plays the role of a “scale parameter”. By tweaking λ , we can select the level of detail desired in the reconstructed image.

The use of neighborhood filters by Buades, Coll and Morel in [5] has led to an extensive literature of nonlocal models in image processing. This nonlocal ROF-model, in a simplified version, has the form

$$\min \left\{ \int_{\Omega \times \Omega} J(x-y)|u(x) - u(y)| dx dy + \frac{\lambda}{2} \|u - f\|_2^2 : u \in L^2(\Omega) \right\}. \quad (13)$$

On the other hand, an image can be seen as a weighted graph where the pixels are taken as the vertices, and the weights are related to the similarity between pixels. The ROF-model in a weighted graph $G = (V(G), E(G))$ reads as follows:

$$\min \left\{ \frac{1}{2} \sum_{x \in V(G)} \sum_{y \in V(G)} |u(y) - u(x)| w_{xy} + \frac{\lambda}{2} \sum_{x \in V(G)} |u(x) - f(x)|^2 \sum_{y \sim x} w_{xy} : u \in L^2(G, \nu_G) \right\}. \quad (14)$$

Problems (13) and (14) are particular cases of the following ROF-model in a random walk space $[X, \mathcal{B}, m, \nu]$:

$$\min \left\{ \frac{1}{2} \int_X \int_X |u(y) - u(x)| dm_x(y) d\nu(x) + \frac{\lambda}{2} \int_X |u(x) - f(x)|^2 d\nu(x) : u \in L^2(X, \nu) \right\}, \quad (15)$$

which is one of the motivations for this chapter and we call the m -ROF-model.

Another problem in which we are interested is the (BV, L^1) -decomposition in a random walk space $[X, \mathcal{B}, m, \nu]$, that reads as

$$\min \left\{ \frac{1}{2} \int_X \int_X |u(y) - u(x)| dm_x(y) d\nu(x) + \lambda \int_X |u(x) - f(x)| d\nu(x) : u \in L^1(X, \nu) \right\}, \quad (16)$$

which has as a particular case the (BV, L^1) -decomposition in graphs.

Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space, $f \in L^2(X, \nu)$ and $\lambda > 0$. Our aim in this section is to study the m -ROF-model:

$$\min \left\{ TV_m(u) + \frac{\lambda}{2} \int_X |u(x) - f(x)|^2 d\nu(x) : u \in L^2(X, \nu) \right\}. \quad (17)$$

We will start by proving existence and uniqueness of the minimizer of problem (17) as well as a characterization of this minimizer.

Theorem 7. *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space and assume that ν is a probability measure. For any $f \in L^2(X, \nu)$ and $\lambda > 0$, there exists a unique minimizer u_λ of problem (17). Moreover, u_λ is the unique solution of the problem*

$$\lambda(u - f) \in \Delta_1^m(u). \quad (18)$$

Consequently, $u_\lambda \in L^2(X, \nu)$ is the solution of problem (17) if, and only if, there exists $\mathbf{g} \in L^\infty(X \times X, \nu \otimes m_x)$ antisymmetric such that

$$\lambda(u_\lambda - f) = \operatorname{div}_m \mathbf{g} \quad (19)$$

and

$$g(x, y) \in \operatorname{sign}(u_\lambda(y) - u_\lambda(x)) \quad \text{for } (\nu \otimes m_x)\text{-a.e. } (x, y) \in X \times X.$$

In [12], to solve problem (11), the gradient descent method was used, which required to solve numerically the parabolic problem

$$\begin{cases} u_t = \operatorname{div} \left(\frac{Du}{|Du|} \right) - \lambda(u - f) & \text{in } (0, \infty) \times \Omega, \\ \frac{Du}{|Du|} \eta = 0 & \text{on } (0, \infty) \times \partial\Omega, \\ u(0, x) = v_0(x) & \text{in } x \in \Omega. \end{cases} \quad (20)$$

Then, the denoised version of f is approached by the solution of (20) as t increases. The concept of solution for which this problem is well-posed was given in [1]. We will see here that a non-local version of (20) can be used to approach the solutions of the ROF-model in the workspace of metric random walk spaces.

As in [12], we can see that problem (17) is well-posed by using the gradient descent method. For this, one needs to solve the Cauchy problem

$$\begin{cases} v_t \in \Delta_1^m v(t) - \lambda(v(t) - f) & \text{in } (0, T) \times X, \\ v(0, x) = v_0(x) & \text{in } x \in X, \end{cases} \quad (21)$$

with v_0 satisfying

$$\int_{\Omega} v_0 = \int_{\Omega} f.$$

Now, problem (21) can be rewritten as the following abstract Cauchy problem in $L^2(X, \nu)$:

$$v'(t) + \partial \mathcal{G}_m(v(t), f, \lambda) \ni 0, \quad v(0) = v_0. \quad (22)$$

Then, since $\mathcal{G}_m(\cdot, f, \lambda)$ is convex and lower semi-continuous, by the theory of maximal monotone operators ([3]), we have that, for any initial data $v_0 \in L^2(X, \nu)$, problem (22) has a unique strong solution. Therefore, if we define a solution of problem (21) as a function $v \in C(0, T; L^2(X, \nu)) \cap W_{loc}^{1,1}(0, T; L^2(X, \nu))$ such that $v(0, x) = v_0(x)$ for ν -a.e. $x \in X$ and satisfying

$$\lambda(v(t) - f) + v_t(t) \in \Delta_1^m(v(t)) \quad \text{for a.e. } t \in (0, T),$$

we have the following existence and uniqueness result.

Theorem 8. *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space and assume that ν is a probability measure. For every $v_0 \in L^2(X, \nu)$ there exists a unique strong solution of the Cauchy problem (21) in $(0, T)$ for any $T > 0$. Moreover, we have the following contraction and maximum principles in any $L^q(X, \nu)$ -space, $1 \leq q \leq \infty$:*

$$\|(v(t) - w(t))^+\|_{L^q(X, \nu)} \leq \|(v_0 - w_0)^+\|_{L^q(X, \nu)} \quad \forall 0 < t < T, \quad (23)$$

for any pair of solutions v, w of problem (21) with initial data $v_0, w_0 \in L^2(X, \nu)$ and noisy images $f, \hat{f} \in L^2(X, \nu)$, with $f \leq \hat{f}$, respectively.

Finally, we will study the m -ROF-model with L^1 -fidelity term, that is, given $f \in L^1(X, \nu)$ and $\lambda > 0$, we will study the minimization, over $L^1(X, \nu)$, of the energy given by the sum of the total variation and the L^1 -fidelity term:

$$\min \left\{ TV_m(u) + \lambda \int_X |u - f| d\nu : u \in L^1(X, \nu) \right\}. \quad (24)$$

In the next result we characterise the minimizers of (24):

Theorem 9. *Let $[X, \mathcal{B}, m, \nu]$ be a reversible random walk space and assume that ν is a probability measure. Let $f \in L^2(X, \nu)$, $\lambda > 0$ and $u_\lambda \in L^2(X, \nu)$. Then, $u_\lambda \in M(f, \lambda)$ if, and only if, there exists $\xi \in \text{sign}(u_\lambda - f)$ such that*

$$\lambda \xi \in \Delta_1^m(u_\lambda).$$

3 Conclusions

The article has introduced a new framework who unifies different branches of PDE and let us to study this equations in a new general way. Moreover, specifically, the main conclusions are the following.

- The random walk sapces allow us to study the heat flow in nonlocal models associated to a nonginular kernel in \mathbb{R}^N .
- The m -connexion of the random walk sapace is caracterized by the infinity propagation speed.
- If a Poincaré inequality is satisfied, we can determine the convergence of the heat flow.
- We have introduced the Euler-Lagrange equations associated to the ROF minimization problems for $p = 1, 2$
- We have seen the importance of the correct election of λ .

References

- [1] Fuensanta Andreu, Coloma Ballester, Vicent Caselles, and José M Mazón. Minimizing total variation flow. *Differential and integral equations*, 14(3):321–360, 2001.
- [2] Dominique Bakry, Ivan Gentil, and Michel Ledoux. *Analysis and geometry of Markov diffusion operators*, volume 348. Springer Science & Business Media, 2013.
- [3] H Brézis. Opérateurs maximaux monotones et semi-groupes de contractions dans les espaces de hilbert. number 5 in north holland math. *Studies. North-Holland, Amsterdam*, 1973.
- [4] Ronald E Bruck Jr. Asymptotic convergence of nonlinear contraction semigroups in hilbert space. *Journal of Functional Analysis*, 18(1):15–26, 1975.
- [5] Antoni Buades, Bartomeu Coll, and Jean-Michel Morel. A review of image denoising algorithms, with a new one. *Multiscale modeling & simulation*, 4(2):490–530, 2005.
- [6] TF Chan and S Esedoglu. Aspects of total variation regularized l1 function approximation. ucla cam report 04-07, to appear in *siam j. Appl. Math.*

- [7] Vincent Duval, Jean-François Aujol, and Yann Gousseau. The tvl1 model: a geometric point of view. *Multiscale Modeling & Simulation*, 8(1):154–189, 2009.
- [8] Masatoshi Fukushima, Yoichi Oshima, and Masayoshi Takeda. *Dirichlet forms and symmetric Markov processes*. de Gruyter, 2010.
- [9] Jose M Mazon, Marcos Solera, and Julián Toledo. The heat flow on metric random walk spaces. *Journal of Mathematical Analysis and Applications*, 483(2):123645, 2020.
- [10] Yves Meyer. Oscillating patterns in image processing and nonlinear evolution equations, volume 22 of university lecture series. *American Mathematical Society, Providence, RI*, 364, 2001.
- [11] Themistocles M Rassias. On the stability of the linear mapping in banach spaces. *Proceedings of the American mathematical society*, 72(2):297–300, 1978.
- [12] Leonid I Rudin, Stanley Osher, and Emad Fatemi. Nonlinear total variation based noise removal algorithms. *Physica D: nonlinear phenomena*, 60(1-4):259–268, 1992.
- [13] Marcos Solera Diana. Gradient flows in random walk spaces. 2021.
- [14] Wotao Yin, Donald Goldfarb, and Stanley Osher. The total variation regularized l^1 model for multiscale decomposition. *Multiscale Modeling & Simulation*, 6(1):190–211, 2007.