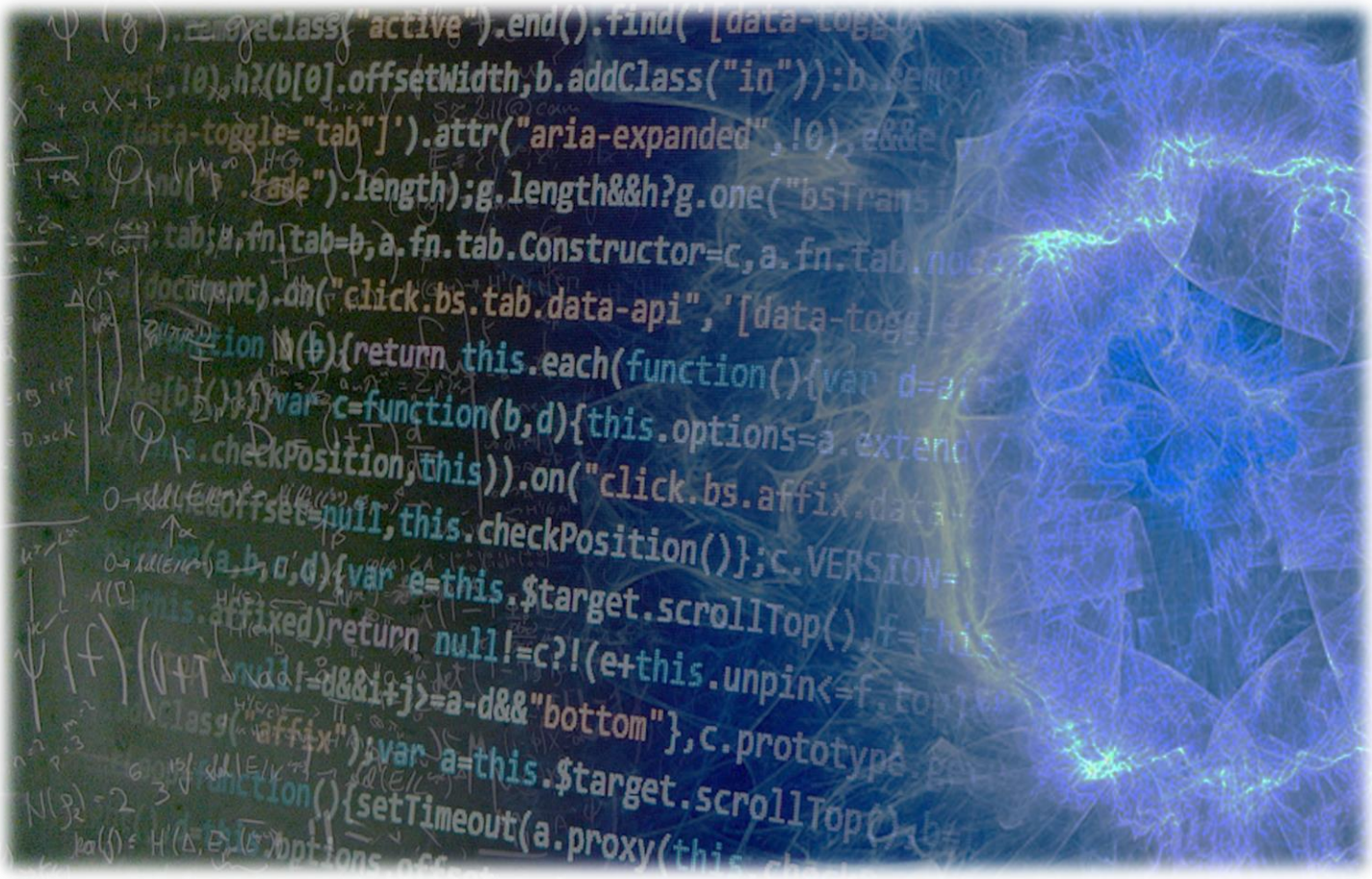
StudMath-IT



International Student Conference StudMath-IT 2021

Extended Abstracts Volume

Mathematics & Computer Science **NOVEMBER, 18-19** **"Aurel Vlaicu" University of Arad**

Extended Abstracts Volume of the International Student Conference StudMath-IT

organized by

Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad,

with support of

Romanian Ministry of Education and Research

November 18th-19th, 2021

StudMath-IT 2021

Mathematics & Computer Science

"Aurel Vlaicu" University of Arad, Faculty of Exact Sciences
Address: **2 Elena Drăgoi St., 310330, Arad, Complex M (Micalaca, 300 area)**
***Tel./ Fax*: +40 257.219.000**
***e-mail*: stiinte.exacte@uav.ro,**
***Web*: studmathit.uav.ro**

Edited by:
Crina Anina Bejan, Antonio Marius Flavius Lupuți and Dominic Bucerzan

Table of Contents

Extended Abstract of accepted papers for presentation

Elaboration of the Graph Type Model for the Analysis of Biological Data

Ion Ganea[1*]

Scientific Advisor: Prof. Gheorghe Căpățână, PhD[1]

[1]*Moldova State University, Chișinău, Republic of Moldova*

The evolution of human society generates a number of problems such as: population growth, food and limited resources, climate change. As a result, the need to increase agro-industrial production and its quality increases. These issues need to be analyzed and addressed through a cross-disciplinary approach to problem families.

Based on the data resulting from the research in the biology laboratory of USM, a data model is elaborated. It is an integrated collection of concepts needed to describe the data, the relationships between them and the existing constraints on the data of the analyzed system. The implementation of this model is done by creating a graph database using the Neo4j DBMS .

The initial objective of this database is to obtain the necessary knowledge on the influence of certain compounds on the development of plants and their degree of influence. Graphs are created to answer important questions in the field. The data model has the following components: nodes, labels, relationships, and properties:

- Nodes and associated labels: Proteins, N2, P2, Root length, weight 100 grains, P2O5, S1 , S2 , S3 , Control, Prep1 , Prep2 .
- *Identifying connections (relationships) between entities: Contains, Measures, Weighs.*

The implementation of the data model in the *Neo4j* DBMS is done through the *Cypher* language.

Example of realization of entities: *Varieties (S1) and Compounds (P1).*

create (S1: Varieties {variety: 'S1'}),
(Prep1: Compound {prep: 'Prep1'})

An instruction is made to create the relationship " Untreated " between nodes of variety " S1 " and " Control (m) ":

```
match (s1: Variety), (m: Treatment)
where id (s1) = 2 and id (m) = 1
create (s1) - [rel: Untreated] -> (m)
return s1, m
```

Keywords: databases, problems, problem families, graph, neo4j , models.

* Corresponding author, Ion Ganea, e-mail adress: iganea9@gmail.com

A Fixed-Point Approach for the Semi-Linear Stokes System from Fluid Mechanics

David Brumar[1*]

Scientific Advisor: Prof. Radu Precup, PhD[1]

[1] *Babeș-Bolyai University, Department of Mathematics, Cluj-Napoca, Romania*

This paper is concerned with the study of semi-linear Stokes problem using the operator method approach based on abstract results of nonlinear functional analysis. More precisely, using the Banach's contraction principle, we prove the existence and uniqueness of the solution. Then, under weaker conditions and using Schauder's fixed point theorem we obtain an existence result for the problem.

The slow flow of an incompressible homogeneous fluid is described by its pressure (x) and its velocity (x). For a stationary regime, the problem is to find such a pair of functions in order that the following conditions hold:

$$\begin{cases} -\mu\Delta u + \nabla p = f(x) & in\ \Omega \\ \nabla \cdot u = 0 & in\ \Omega. \\ u = 0 & on\ \partial\Omega \end{cases} \qquad (1)$$

Here $\Omega \subset \mathbb{R}^n$ is a bounded open set, $\mu > 0$ is the kinematic viscosity $f \in (L^2(\Omega))^n$ is the external force. Now, if we denote $V := (H_0^1(\Omega))^n$ and $V_{div} = \{v \in V: \nabla \cdot v = 0\}$, then if a pair $(u(x), p(x))$ is a solution to the problem (1), then $u \in V_{div}$ and for every $v \in V_{div}$ we have

$$\mu \int_\Omega \nabla u \cdot \nabla v = \int_\Omega f \cdot v\,. \qquad (2)$$

This gives the variational form of the problem (1).

In this paper we consider the semi-linear Stokes system

$$\begin{cases} -\mu\Delta u + \nabla p = h(x, u(x)) & in\ \Omega \\ \nabla \cdot u = 0 & in\ \Omega\,, \\ u = 0 & on\ \partial\Omega \end{cases} \qquad (3)$$

where h: $\Omega \times \mathbb{R}^n \to \mathbb{R}^n$. The idea is to rewrite the problem (3) as a fixed-point equation $u = S \circ (u)$, $u \in V_{div}$ where $S = (-\Delta)^{-1}$ and B is the Nemytskii operator.

Theorem Let $\Omega \subset \mathbb{R}^n$ be a bounded open set, and h: $\Omega \times \mathbb{R}^n \to \mathbb{R}^n$ satisfying the following:

1. h is a Caratéhodory function;
2. there exists a constant $a \in \mathbb{R}_+$ such that $|h(x, u) - h(x, u)| \le a|u - u|$ for any $u, u \in \mathbb{R}^n$ and a.e. $x \in \Omega$;
3. $\frac{a}{\mu\lambda_1} < 1$, where by λ_1 is denoted the smallest eigenvalue of the Dirichlet problem

Then the semi-linear Stokes system (1) has a unique solution with $u \in V_{div}$. Moreover, u is the limit in V_{div} of the sequence of successive approximations $u_k := (u_0)$ for $k \ge 0$ and $u_0 \in V_{div}$.

Finally, under weaker conditions, we use Schauder´s fixed point theorem and obtain the existence of a solution.

Keywords: Stokes system, Semi-linear problems, Operator method, Weak solution, Fixed point theorems, Sobolev spaces.

[*] Corresponding author, David Brumar, e-mail adress: brumardavid97@gmail.com

On the Finite Subgroups of $\mathrm{PGL}_2(\boldsymbol{C})$

Alexandru-David Abrudan[1*]

Scientific Advisor: Prof. Andrei Mărcuș, PhD[1]

[1] *Babeș-Bolyai University, Department of Mathematics, Cluj-Napoca, Romania*

We give results regarding the finite order elements and finite subgroups of the projective linear group of degree two over the field extension $\mathrm{Q}(i)$ and ring extension $\mathrm{Z}[i]$.

Let K be a field or ring. Consider the general linear group of degree two over K, $\mathrm{GL}_2(K) = \{A \in \mathrm{M}_2(K) \mid \det A \in \mathrm{U}(K)\}$. We consider the projective linear group of degree two over K, denoted $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^*$.

The works of Dresden and others touch on the topic of the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{R})$, $\mathrm{PGL}_2(\boldsymbol{Q})$ and $\mathrm{PGL}_2(\boldsymbol{Z})$, giving a classification of these subgroups.

The following results are a study on the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$ and $\mathrm{PGL}_2(\boldsymbol{Z}[i])$, where $\boldsymbol{Q}(i) = \{a + bi \mid a, b \in \boldsymbol{Q}\}$ and $\boldsymbol{Z}[i] = \{a + bi \mid a, b \in \boldsymbol{Z}\}$. They have been proved using similar and adapted ideas found in Dresden's work.

The main results of this paper are classifications of the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$ and $\mathrm{PGL}_2(\boldsymbol{Z}[i])$. Our first main theorem states that the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$ are cyclic, dihedral or isomorphic to A_4. This has been proved based on the fact that $\mathrm{PGL}_2(\boldsymbol{C})$ has finite subgroups C_n, D_n, A_4, S_4 and A_5, then systematically removing S_4 and A_5 with the help of certain counter examples. The next main theorem concretely lists the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$ - C_2, C_3, C_4, C_6, D_2, D_3, D_4 and A_4. This result has been proved by coupling the aforementioned theorem with a lemma that lists the finite order elements of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$. Lastly, the final main result is a theorem that lists all the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Z}[i])$ - C_2, C_3, C_4, D_2, D_3 and A_4. Analogously, this result has been proved by giving certain limiting conditions to the finite subgroups of $\mathrm{PGL}_2(\boldsymbol{Q}(i))$.

In this paper we have classified the finite subgroups of the projective linear group of degree 2 over the complex-extended field $\boldsymbol{Q}(i)$ and ring $\boldsymbol{Z}[i]$. Some of the classifications are proved to be unique up to conjugacy, given their limited choice of generators.

Keywords: projective general linear group; finite subgroups; fractional linear transformations; dihedral group.

* Corresponding author, Alexandru-David Abrudan, e-mail: alexandru.david.abrudan@stud.ubbcluj.ro

A rtificial Intelligence in Medicine

Rares Danut Patcas[1]

[1] *Babeș-Bolyai University, Department of Mathematics, Cluj-Napoca, Romania*

Breast cancer is one of the most common and leading causes of cancer among women. Currently, it has become a common health issue, and its incidence has increased recently. Prior identification is the best way to manage breast cancer results. Computer-aided detection or diagnosis (CAD) systems play a major role in the prior identification of breast cancer and can be used for the reduction of the death rate among women. The main intention of this paper is to make use of the recent advances in the development of CAD systems and related techniques. The mainstay of the project is to predict whether the person is having breast cancer or not. Machine learning is nothing but training the machines to learn and perform by themselves without any explicit program or instruction. So here, predicting whether a person is suffering from breast cancer or not is done with the help of the trained data. We need trained data for many other types of cancer as well.

In other words, machine learning can be used to make diagnostic for all types of cancer and many other diseases like skin cancer because it is still a classification based on images as you can see.

Developments in automation and artificial intelligence are set to revolutionize the workplace - in May 2017, McKinsey estimated that 50% of activities currently carried out by workers have the potential to be automated. Many of us are wondering how our fields may be impacted by this societal shift. Artificial intelligence in medicine and healthcare has been a particularly hot topic in recent years. While there is a sense of great potential in the application of AI in medicine, there are also concerns around the loss of the 'human touch' in such an essential and people-focused profession. Artificial intelligence (AI) is the technological new trend currently providing more options for businesses to strive for. Just like any other profession, medicine is also having a taste of Artificial

intelligence. According to various medical researches, about 50 percent of activities carried out by workers can be automated. How medical practitioners respond to the use of AI is important to its success. For instance, 25 years ago, certain medical innovations were almost impossible. As a matter of fact, AI has contributed immensely to medicine but what does the future hold for medicine. The reason for the increasing use of AI in healthcare is because quite a number of the above may be automated. Don't forget, these processes mentioned above form part of the 50 percent of workers' activities that can be automated. Besides, automation of these processes will ensure that tasks are completed more efficiently. It gives the medical professional more time to handle other activities.

Keywords: Artificial Intelligence, Machine Learning, Medical Images

* Corresponding author, Rares Danut Patcas, e-mail: patcasrares2@gmail.com

Human Tracking and Profiling for Risk Management

Ranjith K.H.V.S.[1*], Jayasekara A.S.[1], Ratnasooriya K.A.L.L.[1], J.L Thilini Randika[1], Dr. Lakmal Rupasinghe[1] and Ms. Chethana Liyanapathirana[1]

Dept. of Computer Software Engineering, Sri Lanka Institute of Information Technology. Malabe, Sri Lanka

Infectious viruses are conveyed via respiratory droplets produced by an infected person when they speak, sneeze, or cough. So, to combat virus transmission, the World Health Organization (WHO) has imposed severe regulations such as mandatory face mask use and social segregation in public spaces.

The 'Human Tracking and Profiling for Risk Management System (HTPRM)' is an online application that identifies the risk associated with failing to follow proper health practices. This proposed approach, which is divided into four components, utilizes 'You Only Live Once YOLO(V3)' to detect face-mask danger, which would be determined based on two factors: wearing the face mask properly and the type of mask (Surgical, k95, homemade, and bare).

The second phase is to use OpenCV and SSD-Mobilenet to evaluate the value of a one-meter space(Social Distance) between people. The system recognizes the maximum number of individuals that can be in the vicinity of the specific hall that uses YOLO(V3) and image processing as the third procedure. In the last processing, the system identifies each person's behavior, classifies it as uncommon or not, and calculates the risk associated with each category.

Finally, the system computes the overall risk and generates a warning alarm to notify the user that they are in a dangerous scenario. Index Terms—YOLO (V3), SSD (Single shot detector), Mobilenet, Open-CV, Image Processing, Open pose, Tenser-flow.

Keywords: Human Tracking, Risk Management

* Corresponding author, Ranjith K.H.V.S., e-mail: it18126020@my.sliit.lk

Iterative Shepard Operator of Least Squares Thin-Plate Spline Type

Andra Malina[1*]

[1] *Babeș-Bolyai University, Cluj-Napoca, Romania*

The Shepard operator, introduced by D. Shepard in 1968, is one of the best suited methods for interpolating scattered data. One way for overcoming its drawbacks is by considering a quadratic modification of the method, depending on a radius of influence, obtaining the so-called *modified Shepard operator*.

T. Cătinaș and A. Malina introduced in 2021 a new Shepard operator, based on the classical and the modified Shepard methods and the least-squares thin-plate spline function.

The least squares thin-plate spline is defined as

$$F_i(x,y) = \sum_{j=1}^{i} C_j d_j^2 \log(d_j) + ax + by + c, \quad i = 1, \dots, N' \qquad (1)$$

where the coefficients C_j, a, b, c are found such that to minimize the expression

$$E = \sum_{i=1}^{N'} [F_i(x_i,y_i) - f(x_i,y_i)]^2 \qquad (2)$$

Considering $N'=N$, where N is the number of initial nodes and also $N'=k$, where k is the cardinal of a smaller set of knot-points, that represents the initial set, provides better results and is based on an algorithm described by J. R. McMahon in 1986.

We consider an *iterative modification of the Shepard operator of least squares thin-plate spline type*, following an idea presented by A. Masjukov and V. Masjukov in 2005. The operator, denoted by u_L, is defined as

$$u_L(x,y) = \Sigma_{k=0}^{K} \Sigma_{j=1}^{N'} \left[u_{F_j}^{(k)} w\left((x-x_j, y-y_j)/\tau_k\right) \Sigma_{p=1}^{N'} w\left((x_p-x_j, y_p-y_j)/\tau_k\right) \right], \quad (3)$$

where the weight function w is continuously differentiable and has the properties

$$w(x,y) \geq 0, w(0,0) = 0, w(x,y) = 0 \text{ if } ||(x,y)|| > 1 \qquad (4)$$

and $u_{Fj}^{(k)}$ denote the interpolation residuals at the step k. The method is completed by the choice of τ_k which is defined as $\tau_k=\tau_0\gamma^k$, with τ_0 an initial parameter and $\gamma\in(0,1)$, varying values, inspired from multiscale analysis.

We introduced an iterative modification of the Shepard operator of least squares type, using two sets of nodes, the second one being representative for the first one. Numerical experiments showed the improvements made by this method compared to the classical Shepard operator and situations when it is comparable to the modified operator.

Keywords: Shepard operator, least squares thin-plate spline, knot points, iterative multiscale method.

* Corresponding author, Andra Malina, e-mail: andra.malina@ubbcluj.ro

On Starlike Univalent Mappings in One and Several Complex Variables

Eduard Ștefan Grigoriciuc[1*]

[1] *Faculty of Mathematics and Computer Science, Babeș-Bolyai University, Cluj-Napoca, Romania*

Dedicated to the memory of Professor Dr. Gabriela Kohr

In this paper we discuss about starlike univalent mappings (i.e. holomorphic and injective mappings which maps the unit disc/Euclidean unit ball onto a starlike domain with respect to the origin) on the unit disc in the complex plane $\mathbb{C}$, respectively on the Euclidean unit ball in the case of n-dimensional complex space $\mathbb{C}^n$. Recall that a domain $D\subset\mathbb{C}^n$ is called starlike with respect to the origin if $0\in D$ and for all $z\in D$, we have that the segment between 0 and z is contained in D. Also, notice that we denote

$$S=\{f:U\to\mathbb{C}: f(0)=0, f'(0)=1 \text{ and } f \text{ is univalent}\}$$

the family of all univalent functions on the unit disc U and

$$S^*=\{f\in S: f(U) \text{ is a starlike domain with respect to the origin}\}$$

the class of all starlike function on the unit disc U. For $n\geq 2$, we denote $S(B_n)$ and $S^*(B_n)$ the class of univalent (respectively, starlike) mappings on the Euclidean unit ball B_n.

It is known that the family of univalent functions S is not a convex set, hence it will be interesting to study the properties of a convex combinations of the form $(1-\lambda)f+\lambda g$, where $\lambda\in(0,1)$ and f, g are univalent functions.

In particular, in this paper, we consider the particular case when f and g are starlike mappings on the Euclidean unit ball (i.e. $f,g\in S^*(B_n)$). We discuss about both cases of one, respectively several complex variables, but our main results are given for the case of several complex variables.

Keywords: Univalent function, Starlike function, Starlike domain, Convex combination, Biholomorphic mapping.

* Corresponding author, Eduard Ștefan Grigoriciuc, e-mail: eduard.grigoriciuc@ubbcluj.ro

Image Processing - A Mathematical Perspective

Rajat Rai[1], Tanvi Patil[1] and Shreya Katole[1]

Scientific Advisor: Dr. Avinash J. Kamble[1]

[1]*Pillai HOC College of Engineering & Technology, Rasayani- 410207, INDIA*

Image Processing is the study of modifying an image, to get an enhanced quality image or to extract some useful information from it. An Image is defined as a two-dimensional signal F(x,y), where x and y are coordinates in the graph. Linear Algebra plays a vital role in changing the properties of an image. One of the methods used in image processing is Singular Value Decomposition (SVD) which involves factorizing a matrix into three small matrices. The objective of the paper is to highlight the mathematical concept, singular value decomposition which plays a significant role in Image processing.

Linear Algebra is a branch of mathematics that is widely used in the fields like Computer Graphics, Cryptography, Signal Processing, Coding Theory, etc.

The Singular Value Decomposition method used in image processing is based on the concept of matrix factorization. It is a typical way of representing an $m \times n$ matrix M into three matrices.

$$\mathbf{M = USV^T}$$

Here,

M is the input matrix,

U is an $m \times m$ unitary matrix representing the left singular vectors,

S is an $m \times n$ diagonal matrix representing singular values/eigenvalues of approximated matrix and

V is an $n \times n$ unitary matrix representing the right singular vectors. VT is a conjugate transpose of V.

The singular values in the matrices are arranged in the descending order of their magnitude so that the initial values contain more information than the other.

Understanding the working of Singular Value Decomposition by geometrically representing it gives us an insight into the other matrix properties and also helps us in understanding and writing the algorithms based on Singular Value Decomposition. Digital images are represented in matrix form describing the color and color intensities of the image which undergoes various mathematical operations for enhancement of the same.

Among various mathematical tools, singular value decomposition proves to be a significant method in image processing. It helps to retain the important singular values and avoids redundant data which results in preserving the quality of the image intact.

Keywords: Singular Value Decomposition, Image Processing, Matrix Decomposition, Unitary Matrix.

Rajat Rai, e-mail: rajatjr20comp@student.mes.ac.in
Tanvi Patil, e-mail: tanviap20comp@student.mes.ac.in
Shreya Katole, e-mail: shreyak20comp@student.mes.ac.in
DR. Avinash J. Kamble, e-mail: avinashkamble@mes.ac.in

Graph Neural Network – An Effective Framework for Neural Network

Utkarsha Chaudhari[1], Nihar Pasi[1] and Shivam Modhave[1]
Scientific Advisor: Dr. Avinash J. Kamble[1]

[1]*Pillai HOC College of Engineering and Technology, Rasayani-410207, INDIA*

A neural network system is a computational learning system that works similar to a human brain allowing the computer to recognize and understand patterns or images and connect similar aspects in the field of Artificial Intelligence, Deep Learning and Machine Learning. Neural network is classified into 4 types: Artificial Neural Network (ANN), Convolution Neural Network (CNN), Recurrent Neural Network (RNN) and Graph Neural Network (GNN). GNN is based on Graph theory, which is study of graph using structured datatype that has **nodes** and **edges**. The defining feature of a GNN is that it uses a form of neural message passing in which messages are exchanged between nodes in the graph and updated using neural networks. Neural Network uses graph theory which is based on the concpets of aggregation and propagation of features of a node. Aggregation is the process of computing a single output from various inputs which are collected from the neighbouring nodes. The aggregation process is expressed in 4 different types. The main aggregation function among them, also called as *sum of products* function, is mathematically expressed:

$$s = w_0x_0 + w_1x_1 + \cdots + w_nx_n = \sum_{i=0}^{n} w_i\, x_i$$

where, w_i represents the weight of the i^{th} node and x_i represents the node .
Each node associates(aggregates) its value with its neighbouring nodes regardless of whether they lie in front or behind the node in the graph. These aggregated values on each layer of the graph is further passed to next layer using propogation function, also called as *message passing* function, mathematically expressed as

$$h_v^k = \sigma\left(W_k \sum \frac{h_u^{k-1}}{|N(v)|} + B_k h_v^{k-1}\right) where\ k = 1, \ldots\ldots, k-1$$

where, v is a certain node, k is layers of aggregation, σ is the non-linearity coefficient, $W_k \sum \frac{h_u^{k-1}}{|N(v)|}$ averages the neighbors of node and $B_k h_v^{k-1}$ is a trainable weight matrix.

There are many neural networks in use but GNN proves to be an effective framework for the study of Neural Networks. It provides a better way for node level, edge level and graph level prediction tasks. Aggregation and propagation function plays a vital role in GNN as in their absence the user won't be able to extract updated information from any specific node.

Keywords: Neural Network, Graph Theory, Graph Neural Network, Aggregation Function and Propagation Function

Utkarsha Chaudhari, e-mail: utkarshavc20comp@student.mes.ac.in
Nihar Pasi, e-mail: niharmp20comp@student.mes.ac.in
Shivam Modhave, e-mail: rajendrams20comp@student.mes.ac.in
Dr. Avinash J. Kamble, e-mail: avinashkamble@mes.ac.in

Applications of Partial Derivatives of Composite Functions of Several Real Variables

Alexandra Nicoleta Dagău [1*] and Paula Ioana Barna [1]

Scientific Advisor: Prof. Ghiocel Moț, PhD[1]

[1] *"Aurel Vlaicu" University of Arad, Romania.*

In this article we make applications of partial derivatives of first order and second order of real composite functions with *m* functions and *n* variables:

$$f(x_1, x_2, \dots, x_n) = \varphi(u_1(x_1, x_2, \dots, x_n),\ u_2(x_1, x_2, \dots, x_n), \dots, u_m(x_1, x_2, \dots, x_n)).$$

We choose to approach this subject because includes a fundamental material for every mathematician or scientist, which needs basic calculus aspects in his daily routine. The beginning of this article has a short theoretical part, which contains basic notions used in solving problems and accomplishing proofs, chosen specifically for this theme.

In the first part we compute the partial derivatives of second order for:

$$f(x_1, x_2) = \varphi(u_1(x_1, x_2), u_2(x_1, x_2), u_3(x_1, x_2)) \ ;$$
$$f(x_1, x_2, x_3) = \varphi(u_1(x_1, x_2, x_3), u_2(x_1, x_2, x_3)).$$

In the second part we generalize the results for *m* functions and *n* variables and in the last part we present some representative examples.

Keywords: real functions, composite functions, partial derivatives, higher order partial derivatives, Jacobi's matrix, the Jacobian

*Corresponding author,Alexandra Nicoleta Dagău, e-mail: dagaualexandra99@yahoo.com

A Classification of Groups of Order $pq2$

Cristian-Aurel Rafiliu[1*]
Scientific Advisor: Prof. Andrei Mărcuș, PhD[1]

[1]*Babeș-Bolyai University, Faculty of Mathematics and Computer Science,*
1 Mihail Kogălniceanu St., 400084, Cluj-Napoca, Romania

In this paper we present a classification of groups of order $pq2$, where $p<q$ are prime numbers. The method used is an elementary method and we don't use very abstract notions from algebra. The results which lead to this classification, and also the results on automorphism groups can be adapted to find classifications of groups in other cases.

We made a classification of groups of order $pq2$, where $p<q$ are primes, using an elementary method. From the proved results we see how we can construct such of groups and how we can enumerate them. Of course, the results of this classification or about automorphism groups can be adapted to another classification of groups.

Keywords: classification groups, automorphism group, semidirect product, split extensions.

* Corresponding author, Cristian-Aurel Rafiliu – e-mail: cristianrafiliu2@gmail.com

Approaching Real Phenomena Through Differential Equations

Mihaela Sterp[1*]

[1] *"Aurel Vlaicu" University of Arad, Romania*

This paper aims to emphasize some of the real world phenomena, at the base of many of them being the differential equations and the systems of differential equations.

The study of differential equations is a wide field in pure and applied mathematics, physics, and engineering. All of these disciplines are concerned with the properties of differential equations of various types.

Pure mathematics focuses on the existence and uniqueness of solutions, while applied mathematics emphasizes the rigorous justification of the methods for approximating solutions.

Differential equations play an important role in modelling virtually every physical, technical, or biological process, from celestial motion, to bridge design, to interactions between neurons.

Differential equations such as those used to solve real-life problems may not necessarily be directly solvable, i.e. do not have closed form solutions. Instead, solutions can be approximated using numerical methods. The study of the stability of solutions of differential equations is known as stability theory.

The theory of ordinary differential equations is one of the most powerful methods that humans have invented or discovered and continuously improved for describing the natural phenomena whose investigation is fundamental for the progress of humanity. But its power is not limited to the natural phenomena, such as physical, biological or chemical, it is also fundamental for the study and the construction of mechanical systems from engineering, as well as for the study and the prediction of the economical or social behavior of our real world.

A natural extension of the theory of ordinary differential equations is the theory of partial differential equations, which is certainly more suitable for describing those phenomena whose space-dependence is not negligible. However, most of the results about partial differential equations were not be obtainable without a good theory for the ordinary differential equations.

This paper presents several mathematical models for real world phenomena, such as: the evolution of some bacteria, the growth of trees, the equations of plane curves, the movement of a rocket, the "birth" of a substance in a bimolecular chemical reaction, transient phenomena in a circuit consisting of a capacitor and a resistor, decreasing the salinity of a salt solution in water, etc.

Keywords: Differential equations, real world phenomena, mathematical models.

*Corresponding author, Mihaela Sterp – e-mail: sterpmihaela98@yahoo.com

Cycloidal Curves

Alexandra Florea[1*]

Scientific Advisor: Lect. Lorena Camelia Popa, PhD[1]

[1] *"Aurel Vlaicu" University of Arad, Romania*

This paper approach a special class of plane curves, named cycloidal curves: cycloid, hypocycloid, epicycloid and pericycloid, and presents a unitary way in which they can be studied.

This cycloidal curves have various applications in life, being often used in multiple technical applications, in construction, in design and even in mechanics.

Cycloidal curves are obtained by rolling a moving curve without friction on a fixed curve (in the plane).

The cycloid is a plane curve generated by a point which belongs to a circle, that rolls along a straight line. In the case of a circle rolled outside the contour of another circle, a plane curve called an epicycloid is formed. And in the case of a circle rolled inside the contour of another circle, the hypocycloid plane curve is formed.

In the case of the hypocycloid and the epicycloid, starting from their parametric equations we will explore their representation according to the ratio between the radius of the moving circle and the radius of the fixed circle and we will present some particular cases using the GeoGebra mathematical software.

Also, using the MathCad software we will calculate the length of such curves and the area bounded by them.

Keywords: cycloid, hypocycloid, epicycloid, pericycloid.

[*] Corresponding author, Alexandra Florea, e-mail: flr_alexandra@yahoo.com

Decreasing Monomial Codes

Andreea Sz¨ocs[1*]

[1]*"Aurel Vlaicu" University of Arad, Romania*

Motivation

Today's security of digital information mainly relies on two algorithms - the RSA cryptosystem and the DH key exchange. Both of these rely on the hardness of solving descrete logarithms using classical algorithms. (Factorising large numbers can be reduced to the descrete logarithm problem.) In 1994, Shor's algorithm, a quantum algorithm, presented a polynomial-time solution to the descrete logarithm problem. Thus, with the construction of quantum computers, the cryptosystems used thus far can no longer solely be relied upon. In preparation, intense research has been made into post-quantum cryptography. This science aims to study cryptosystems that would remain secure when faced with both classical and quantum computers, and which could be deployed without major changes to present communication networks and protocols. The main new candidates are code-based, lattice-based and multivariate polynomial-based cryptosystems.

Code-based cryptosystems

Code-based cryptosystems are ones where the underlying one-way function makes use of an error-correcting code C. This function may consist of adding an error to a codeword of C or in computing a syndrome using a parity-check matrix of C.

The first such cryptosystem is a PKC proposed by Robert J. McEliece in 1978. Apart from having a large public key, the McEliece cryptosystem has many strong features: the security reductions are tight, both encryption and decryption are very fast as the procedures have low complexity. Extensive research has been made into reducing the key size for this cryptosystem. This produced numerous variants to the original McEliece.

Decreasing monomial codes

Due to its structure, a self-dual decreasing monomial code has a large permutation group. Moreover, because of the underlying algebraic structure, very little information is needed to fully determine a certain code. This makes them memory-efficient.

For these reasons, this paper provides an introduction into self-dual decreasing monomial codes.

Keywords: Monomial codes, Code-based cryptosystems.

*Corresponding author, Andreea Sz¨ocs – e-mail: andreea.szocs@uav.ro

Conditional Empirical Process Involving Functional Data

Salim Bouzebda[1], Fethi Madani[2] and Souddi Youssouf[2*]

[1]*Alliance Sorbonne University, University of Technologie de Compiègne, L.M.A.C., Compiègne, France*
[2]*University Dr Tahar Moulay de Saida, Alegria*
Laboratoire of Modèles Stochastiques, Statistique et Applications

The purpose of this work is to establish the invariance principle for the conditional setindexed empirical process formed by strong mixing random variables when the covariates are functional. We establish our results under some assumptions on the richness of the index class C of sets in terms of metric entropy with bracketing. We apply our main result for testing the conditional independence, that is, testing whether whether two random vectors Y_1 and Y_2 are independent, given X.

The theoretical results of the present paper are (or will be) key tools for many further developments in functional data analysis.

Keywords: Conditional distribution, Nadaraya-Watson regression estimator, Empirical process, Functional data, Strong mixing.

Salim Bouzebda, e-mail: Bouzebda@gmail.com
Madani Fethi, e-mail: fethi.madani@univ-saida.dz
Youssouf Souddi, e-mail: souddioucef@yahoo.fr

Remarks Related to the Rotation Surfaces

Paula Ioana Barna [1*] and Alexandra Dagău[1]

Scientific Advisor: Lect. Lorena Camelia Popa, PhD[1]

[1] *"Aurel Vlaicu " University of Arad, Romania*

This article offers both students and those passionate about mathematics a content that includes theoretical aspects and various examples of rotation surfaces. For this purpose, we approached three rotation surfaces to highlight the generation mode, their surface area, but also capacity. The surfaces studied are: Gabriel's horn (known as the Painter's paradox), the surface of number 8 and the astroidal ellipsoid. We generated these surfaces using: Mathcad and GeoGebra.

I chose to approach this subject due to the fact that geometry is find everywhere in the environment being everything we can perceive and everything we can not, because the imagination does not stop dealing with geometric figures. In other words, geometry is an essential and indispensable tool for people's daily lives.

Keywords: Gabriel's horn, generation, capacity, surface area.

[*]Corresponding author, Paula Ioana Barna – email: paula.barna@yahoo.com

On Differential Equations Involved in the Study of Scientific Processes

Pavel Păun[1*]

[1] *"Aurel Vlaicu" University of Arad, Romania*

As most of the dynamical systems that describe scientific processes issued from economics, engineering, biology, chemistry or physics are extremely complex, identifying the corresponding mathematical models might usually be difficult. Many of the phenomena drawn from actual events or situations are modelled through ordinary differential equations, integral equations or partial derivative equations.

Differential equations had a major impact on the history of science, they are one of the main and necessary factor for describing and explaining the use of differential equations, primarily in general terms, then in the context of specific equations. The primary origin in Newtonian mechanics is based on differential equations, which he applies with an intuitive ability to study nature. Differential equations provide one of the few sources of significant nonlinear problems for which simple solutions are available.

Differential equations are an important factor that is impossible to ignore; and this importance increases in proportion to the computational speed of modern technology. Through all the diversity of applications, we meet several principles and calculation methods very often, among them is the principle of superposition for the theorems of linear problems of existence and uniqueness of solutions, which will be presented in the first chapter. The derivative of a function represents a rate of change, and an equation involving derivatives is called a differential equation.

Many natural laws give a relationship between the rates of change of different quantities, rather than between the quantities themselves. It should come as no surprise that differential equations have had a major impact on the history of science and are one of the ways in which mathematical methods are applied in everyday life. The problems of differential mathematical and scientific equations are classified using the words "linear" and "nonlinear".

Linear problems lend themselves to comprehensive and satisfying theories, while nonlinear problems often require special devices. Both types are encountered in applications. Starting with biomathematics problems, the theory epidemics, (the) ecology, the spiral form of a shell snail, including military strategy, all of these lead immediately to the simple ordinary linear equation.

The issue presented in this paper is very topical and with significant applicability. Thus, phenomena from biology and ecology are modeled, such as plant growth, bacterial spread and environmental pollution, as well as from physics, highlighting processes in mechanics, thermodynamics, electricity and wave theory.

Keywords: Dynamical systems, differential equations, scientific processes

* Corresponding author, Pavel Păun, e-mail: paun.pavel91@gmail.com

Evading the Chip Shortage Handling Secure Cryptographic Tokens Using Consumer-Grade Micro-Controllers

Alexandru Kiraly[1*]

Scientific Advisor: Lect. Darius Bufnea, PhD[1]

[1]*Babes-Bolyai University of Cluj-Napoca, Romania*

Recent years have put more strain on online activities than ever. With pandemics around one corner, audacious yet innovative software releases behind another, it raises the question: How do we handle the security of this fine ballet? Are passwords enough? How can we better protect our online persona? This paper aims to answer these questions, summarize and document the implementation of a few key concepts about hardware-based cryptographic security in relation to the current global situation.

It has been observed that while many adopt new ways to secure their data, few understand the implications and compromises of the different methods involved. Unfortunately, it's usually strong authentication that gets traded in exchange for convenience.

Finding the perfect balance can prove to be a challenge, which is why the existence and wide integration of said hardware tokens was investigated in the first part. Starting with the usual ways people use them in the second part, we looked for how and why dedicated security devices went out of stock and what can be done about it.

The proposed idea revolves around using the abundance of cheap user programmable microcontrollers for generating, storing and authenticating pairs of public key cryptographic tokens. More specifically, the process of handling RSA keypairs in the context of Secure Shell (SSH) authentication, the computational limitations they implied and the essential, general knowledge behind the semicentennial algorithm.

Overcoming the restrictive instructions of 8-bit processors, the single-digit amount of kilobyte-sized memory and the excruciating speed of computing large numbers at 16 million cycles per second, one question remains: Is it worth it? Results show that by simply factoring the ratio between price and processing speed, it absolutely is. Ultimately, when comparing the number of features available, the proposed method is not particularly the best, yet. However, while being cost-effective and relatively secure, this method manages to strike, in our opinion, a perfect balance between accessibility, comfort and security.

Keywords: Security, SSH, Public Key Cryptography, Resource Limits, Signature, Authentication, Hardware

Corresponding author, Alexandru Kiraly, e-mail: alexandru.kiraly@ubbcluj.ro

Conference Agenda

"Aurel Vlaicu" University, Faculty of Exact Sciences
Str. Elena Drăgoi, nr. 2, 310330 Arad, Complex M
Zoom Platform

Thursday, 18.11.2021		
UTC -Time	**RO -Time**	
06:00 – 07:15	**08:00 - 9:15**	**Registration**
07:15 – 07:45	**09:15 - 09:40**	**StudMath-IT 2020 Opening Ceremony**
07:40 – 08:00	**09:40 – 09:50**	**Coffee Break**
07:50 – 08:20	**09:50 – 10:20**	**Plenary Presentation**
08:20 – 08:30	**10:20 - 10:30**	**Coffee Break**
08:30 – 10:00	**10:30 – 12:00**	**Corporate Presentation**
10:00 – 12:00	**12:00 – 14:00**	**Lunch Break**
12:00 – 14:20	**14:00 - 16:00**	**Parallel Sessions – Papers Presentation**
12:00 – 14:00	**14:00 - 16:00**	**Parallel Sessions – Papers Presentation**
12:00 – 14:00	**14:00 - 16:00**	**Parallel Sessions – Papers Presentation**
16:30 – 17:30	**18:30 – 19:30**	**Workshop – TOSTMASTERS** **Limited number of participants.** **Please contact the organizers**
Friday, 19.11.2021		
07:00 – 09:00	**09:00 - 11:00**	**Workshop on "Scientific Writing"** **Limited number of participants.** **Please contact the organizers**

Special thanks to our Sponsors:

MINISTERUL EDUCAȚIEI

UNIVERSITATEA AUREL VLAICU *din* ARAD
Facultatea de Științe Exacte

The conference is also visible on:

information
an Open Access Journal by MDPI

Invited Partners: