MathDigest

Research Bulletin of Institute for Mathematical Research

VOLUME 8 NUMBER 1 ISSN 1985 – 2436 JULY 2017 SYAWAL 1438

Research Articles

Gondran Algebra and Complex Network Analysis

Hidup : Suatu Sifat Keselanjaran

The Role of Hermite Polynomials in Physics

Public Key Encryption Explained

Effects of Problem Posing on Mathematics Performance of Secondary School Students

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

Math Digest

Research Bulletin of Institute for Mathematical Research

VOLUME 8 NUMBER 1
ISSN 1985 – 2436

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

EDITORIAL NOTES

MathDigest ia a research bulletin of INSPEM that publishes a set of articles in Mathematics and other fields related to Mathematics. In this eight edition, MathDigest has moved forward by publishing this bulletin online. This is the strategy and aspiration of INSPEM to see that this bulletin can be easily accessed and read everywhere.

The content of the displayed articles is lighter and simple with new images in the form of magazines that would be more appealing to the readers' interest in attaining the essence of the article. In line with the development of technology and social media, INSPEM intends to make **MathDigest** an informative research bulletin and a source of referrals.

Finally, hopefully **MathDigest** will move forward and gets a place in the hearts of all readers. Any inquiries or submissions can be sent to the Chief Editor by email to n_sumirah@upm.edu.my.

Prof. Dr. Noor Akma Ibrahim
Chief Editor

TINTA EDITOR

MathDigest merupakan buletin penyelidikan INSPEM yang menghimpunkan pelbagai artikel dalam bidang Matematik dan bidang yang berkaitan dengan Matematik. Pada edisi ke lapan ini, ***MathDigest*** telah mengorak langkah dengan menerbitkan buletin ini secara atas talian. Penerbitan secara atas talian ini merupakan strategi dan hasrat INSPEM untuk melihat buletin penyelidikan ini dapat diakses dengan lebih mudah dan dibaca di mana-mana sahaja.

Kandungan artikel yang dipamerkan adalah lebih ringan dan santai, dengan imej baharu berbentuk majalah yang akan menarik lebih perhatian dan minat pembaca untuk meneliti intipati artikel tersebut. Sejajar dengan perkembangan teknologi dan media sosial hari ini, INSPEM berhasrat menjadikan ***MathDigest*** ini sebuah buletin penyelidikan yang informatif dan sumber rujukan pelbagai pihak.

Akhir kata, semoga ***MathDigest*** terus maju jaya dan mendapat tempat di hati semua pembaca. Sebarang pertanyaan atau kiriman artikel bolehlah dihantar kepada Ketua Editor melalui emel ke n_sumirah@upm.edu.my.

Prof. Dr. Noor Akma Ibrahim
Ketua Editor

CONTENTS

Gondran Algebra and Complex Network Analysis 1
Maman Abdurachman Djauhari

Hidup: Suatu Sifat Keselanjaran 7
Ismail Mohd

The Role of Hermite Polynomials in Physics 12
Nurisya Mohd Shah, Chan Kar Tim, Hishamuddin Zainuddin

Public Key Encryption Explained 17
Muhammad Asyraf Asbullah

Effects of Problem Posing on Mathematics Performance of Secondary School Students 22
Kanageshvary Sinnathamby, Rosnaini Mahmud, Rohani Ahmad Tarmizi

Abstract of Theses 29

*

Gondran Algebra and Complex Network Analysis

Maman Abdurachman Djauhari

ABSTRACT

Gondran algebra is introduced. Its algebraic structure is unusual in the way we do arithmetic. People have to change the way they do addition and multiplication of two non-negative real numbers before using this algebra in applications such as in statistics, data analysis especially clustering analysis, finance, linguistic, network analysis, taxonomy, etc. An application in filtering the information contained in a complex network will be demonstrated.

INTRODUCTION

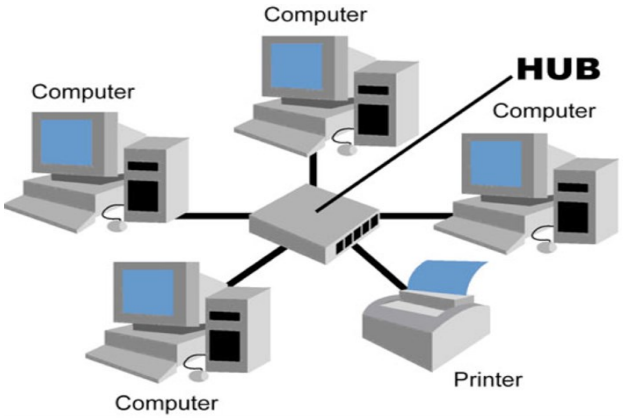
There is no axiomatic system which covers all aspects of mathematics [1]. Thus, there is no well-defined definition about mathematics. Instead, we have so many descriptions of this special field of study. The most famous one is what Gauss said that mathematics is the queen of sciences. This shows the special role of mathematics in all sciences. This statement of Gauss had received an echo where, in 1961, appeared a book entitled "*Mathematics, queen and servant of science*" written by Eric Temple Bell. When Galileo said

* The real world is as small as small world network
Image source:
http://computernetworkingtopics.weebly.com/star-topology.html

that the universe is written in the language of mathematics, he seemingly wanted to say that mathematics is the only language to communicate effectively and efficiently with Nature in quantitative manner.

In France, mathematics has a very special position in culture. In an interview with Journal of Science, June 2008, French Minister of National Education said that "*La France est la terre des mathématiciens* (France is the land of mathematicians)." He was right. Many Fields medalists were French mathematicians or mathematicians who were originally came from France. We witness that France has long tradition where elite politicians have to have a good background in mathematics. It is not exaggerated if we say that, for French mathematicians, mathematics is the science of all possible worlds. This is to distinguish this field of study from other sciences. If Physics, for example, is the science of physical objects, biology is the science of living creatures. The name of these two disciplines, like all other ones, implicitly reflects the object of study. It is not so with mathematics. This is the reason why it is not rare that mathematicians were/are doing research without thinking about its immediate applications.

Look at the history of the irrational number Pi, for example. Human civilization needs more than 35 centuries to find the exact value of Pi; ancient Egyptian mathematician Ahmos had tried to find Pi in 18 century BC and its exact value was discovered by French mathematician named Viette in 17 century CE. What is this exact value for if not for human civilization itself? There is no immediate application of this exact value.



Our society is as small as small world network

Image source: http:// www.csestack.org/ importance-of- network-topology/

Another example is what now called the most famous determinantal inequality. In late 19 century, Jacques Hadamard proved this inequality theorem. It was formulated just for the sake of his intellectual adventure and curiosity and nothing to do with application. Surprisingly, as reported in [2], until present there are hundreds of proofs of this theorem. Currently, the author uses this theorem in multivariate analysis especially for measuring multivariate dispersion.

There are so many mathematical discoveries like that one. In this article, Gondran algebra will be introduced as an example of mathematics as the science of all possible worlds. Then, its role in complex network analysis will be demonstrated.

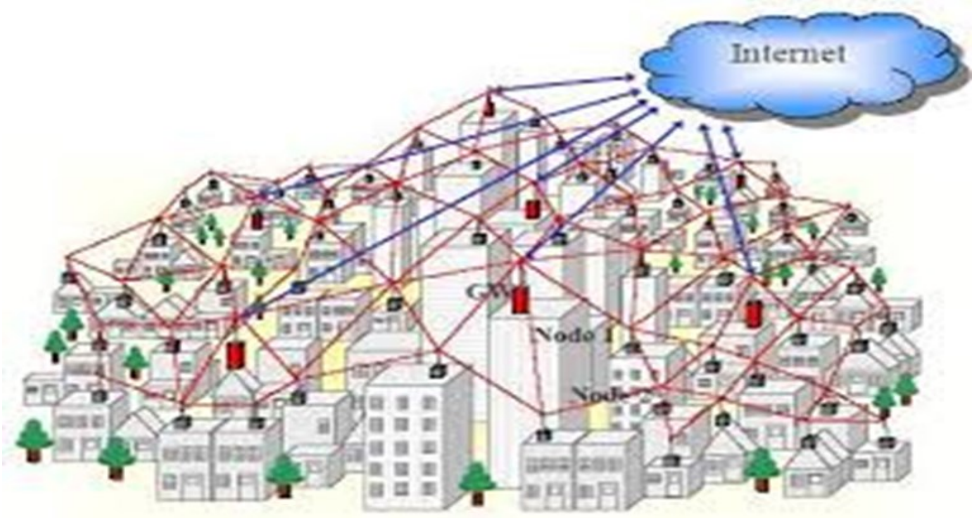
Gondran algebra is an abstract algebra. For those who use to work with the field of real numbers, this is seemingly a strange algebra with unusual addition and multiplication of two non-negative real numbers. In fact, we are not working with the set of all non-negative real numbers R_+ as a subset of the field of all real numbers. Instead, we consider R_+ as subset of the *dioid* $R_+ \dot{E} \{+\infty\}$ with two operations that will be defined later on. As we will show in this paper, its role in complex network analysis is very surprising and its application in econophysics is very advantageous when graph theoretical approach is used.

To begin our discussion, in the second section we recall the algebraic structure of Gondran algebra. Then, by considering a complex network as a dissimilarity matrix D on this dioid, the problem of complex network filtering is discussed in the third section. In the fourth section two examples will be delivered and to end this paper, concluding remarks will be highlighted in the last (fifth) section.

GONDRAN ALGEBRA

Look at this classical problem. Suppose Malaysian government plans to construct the network of gas pipe such that all big cities in Peninsular are connected. How to find the minimum length of pipe to fulfill this construction? The network with minimum length of pipe is called minimum spanning tree (MST) of the complex network consisting all big cities and the distance among them. This is a typical problem in complex network analysis.

Nowadays, there are so many algorithms to solve this problem. As can be seen, for example, in [3], [4], [5], and [6], the most two adopted ones are Kruskal's algorithm and Prim's. See, for example, [7] for a nice historical background and [8] for recent discussion on this algorithm. However, they only give one MST among all possible MSTs that might exist. Consequently, when MST is



Small world network of buildings connected by the internet but ... who own internet?

Image source: http://www.wi-man.net/wi-man-wireless-network-topology/

used to filter the information in a complex system such as practiced in financial market, the filtered information might be misleading. It is not robust. This is the first problem among three encountered in this paper. The second one is about the algorithm to find the robust filtered network and the last one is to find an MST. For this purpose, Gondran algebra will be employed.

Algebra is a branch of mathematics where people study mathematical symbols together with the rules how to manipulate these symbols. We learn in this branch, for example, the so-called algebraic structure, i.e., a system consisting of a set and one or more operations defined on it satisfying a list of axioms. Gondran algebra is an algebraic structure introduced by Michel Gondran (French mathematician) in the middle of 1970s. It consists of a set $S = P_+ \cup \{+\infty\}$, the union of P_+ and {+∞}, and two operations ∨ called addition and ∧ called multiplication of two elements of S where for al x and y in S, $x \vee y =$ the smallest of x and y, denoted by min{x, y}, and $x \vee y =$ the largest of x and y, denoted by max{x, y}.

Thus, in this algebraic structure, the addition of 5 and 11 is not equal to 16 but 5 and the multiplication of 17 and 6 is not 102 but 17. The operations ∨ and ∧ on $S'S$ satisfy all axioms of a dioid [9, p. 233-237]. Gondran algebra is a dioid. We simply denote it as the triplet (S, ∨, ∧). An interesting thing reveals when we consider a dissimilarity matrix defined on this dioid. Since this matrix is a numerical representation of complex network, we can make addition and multiplication of two networks. Here, the dissimilarity of two objects measures how far those objects are dissimilar to each other.

Let us consider a complex network of n actors as a connected undirected weighted graph of n nodes. The weight of the link between nodes i and j is a numerical representation of the complex relationship between i and j. It is then a dissimilarity or, equivalently, similarity score of nodes i and j. If there is no relationship between the k-th and m-th actors, just let the link between them have the weight $d(k,m) = +\infty$. Therefore, this complex network can be represented as a dissimilarity matrix D of size $(n \times n)$. It is a symmetric matrix.

In econophysics, the most widely useddissimilarity is the one constructed based on Pearson correlation coefficient (PCC). See, for example, [10] and [11] and some references therein for the details. Very recently, [12] and [13] define dissimilarity based on Escoufier vector correlation (EVC). EVC is to measure the dissimilarity among stocks where each stock is represented as a multivariate time series. We can find other dissimilarities, including non-Euclidean distances, in [14].

ROBUST INFORMATION FILTERING

Suppose we are to filter the important information contained in a network D consisting of n actors. As mentioned in [10] and [9], the standard practice is as follows.

i. Find an MST of D to get the filtered network.
ii. Determine the sub-dominant ultrametric (SDU) of D from MST. SDU provides the taxonomy among actors and is usually visualized in the form of dendogram.

Once MST has been determined, the network topology representing it is then analysed and numerically summarized, for example, by using centrality measures. See [15], [16] and [17] for the most adopted centrality measures.

As mentioned earlier, when MST is not unique, this practice leads to non-robust filter. Thus, it provides

misleading information. See Djauhari [6] for further details. Unfortunately, in practice, it is very often that D contains more than one MST. To overcome the robustness problem, in this paper we propose to use the forest of all MSTs (Forest, in short) instead of an MST. Forest is unique and therefore the Forest-based filter is robust. More interestingly, if MST is not unique in D, all MSTs and the Forest have the same SDU.

In what follows, we introduce the procedure to find SDU, Forest and an MST. Let us denote D^+ the SDU of D and Δ the adjacency matrix of the Forest. Due to the limited space, the theoretical justification of this procedure cannot be delivered here. However, those who are interested in it could contact the author.

Sub-dominant ultrametric

1) Let $D^{*2} = D \otimes D$ represent matrix multiplication of D with itself in usual manner but $x \vee y = \min\{x, y\}$, and $x \vee y = \max\{x, y\}$ for all elements x and y of D. If $D^{*2} = D$, then $D^+ = D^{*2}$. Otherwise, go to 2).
2) Compute $D^{*4} = D^{*2} \otimes D^{*2}$. If $D^{*4} = D^{*2}$, then $D^+ = D^{*4}$. Else, go to 3).
3) Compute $D^{*8} = D^{*4}$. If $D^{*8} = D^{*4}$, then $D^+ = D^{*8}$. Else, go to 4).
4) The process is repeated until k-th iteration where $D^{*2k} = D^{*2(k-1)}$. Then, $D^+ = D^{*2k}$.

This procedure needs k iterations where $k \neq \frac{\ln(n)}{\ln(2)}$. This is a significant contribution in terms of computational advantage where the number of iterations could be predetermined.

Forest

Once D^+ has been determined, Δ an be derived in simple manner. Let $\Delta^+ = D - D^+$ (usual matrix subtraction). Then, the adjacency matrix Δ is obtained from Δ^+ by changing all zero off diagonal elements by 1 and all non-zero elements by 0.

MST

This is the procedure to find an MST.

1) Construct H_1 the sub-graph of Forest obtained by removing all leaves. If H_1 has no leaf and M_1 is an MST of H_1, then the union of M_1 and all removed leaves is an MST of D. Otherwise, go to 2).

2) Construct H_2 the sub-graph of H_1 obtained by removing all leaves in H_1. If H_2 has no leaf and M_2 is an MST of H_2, then the union of M_2 and all previously removed leaves is an MST of D. Else, go to 3).

i. The removal process of leaves is continued until k-th iteration where H_k has no leaf. The union of an MST of H_k and all previously removed leaves is an MST of D.

Example

Two hypothetical examples will be presented to illustrate the advantages of Gondran algebra approach. The first example is for the case where MST is unique and the second one is where MST is not unique.

Example 1. Consider the following network D discussed in Example 1 in [9, p. 235].

$$D = \begin{pmatrix} 0 & 7 & 5 & 8 & 10 & 8 & 10 \\ 7 & 0 & 2 & 10 & 9 & 9 & 10 \\ 5 & 2 & 0 & 7 & 11 & 10 & 9 \\ 8 & 10 & 7 & 0 & 8 & 4 & 11 \\ 10 & 9 & 11 & 8 & 0 & 9 & 5 \\ 8 & 9 & 10 & 4 & 9 & 0 & 10 \\ 10 & 10 & 9 & 11 & 5 & 10 & 0 \end{pmatrix}$$

It is a complete connected undirected weighted graph of seven objects. By using their algorithm, these authors of [9] come up with this MST in Fig. 1.

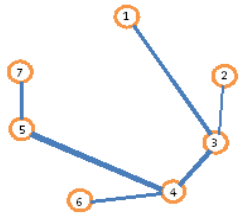


Fig 1. An MST of D

From this MST, they get the following SDU,

$$D^+ = \begin{pmatrix} 0 & 5 & 5 & 7 & 8 & 7 & 8 \\ 5 & 0 & 2 & 7 & 8 & 7 & 8 \\ 5 & 2 & 0 & 7 & 8 & 7 & 8 \\ 7 & 7 & 7 & 0 & 8 & 4 & 8 \\ 8 & 8 & 8 & 8 & 0 & 8 & 5 \\ 7 & 7 & 7 & 4 & 8 & 0 & 8 \\ 8 & 8 & 8 & 8 & 5 & 8 & 0 \end{pmatrix}$$

For example, the element of this matrix at the first row and sixth column is,

$$d^+(1,6) = \max\{d(1,3), d(3,4), d(4,6)\}$$
$$= \max\{5, 6, 7\} = 7$$

One thing must be underlined in this example. According to this method we do not know whether MST is unique or not. However, by using the

results in the third section, after 3 iterations we get $D^{+} = D^{*8}$ and $\Delta$is

$$\Delta = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

This adjacency matrix shows that MST in Fig. 1 is unique; the Forest consists of one MST.

Example 2. Consider this network

$$D = \begin{pmatrix} 0 & 0.1 & 0.3 & 0.2 & 0.1 \\ 0.1 & 0 & 0.3 & 0.4 & 1.7 \\ 0.3 & 0.3 & 0 & 0.6 & 0.5 \\ 0.2 & 0.4 & 0.6 & 0 & 0.2 \\ 0.1 & 1.7 & 0.5 & 0.2 & 0 \end{pmatrix}$$

We show that if we use the standard practice, the information issued from MST might be misleading. In fact, we need 2 iterations to get the SDU D^{+} and the adjacency matrix Δ

$$D^{+} = D^{*4} = \begin{pmatrix} 0 & 0.1 & 0.3 & 0.2 & 0.1 \\ 0.1 & 0 & 0.3 & 0.4 & 1.7 \\ 0.3 & 0.3 & 0 & 0.6 & 0.5 \\ 0.2 & 0.4 & 0.6 & 0 & 0.2 \\ 0.1 & 1.7 & 0.5 & 0.2 & 0 \end{pmatrix}$$

and

$$\Delta = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

This matrix corresponds to the Forest in Fig. 2. We see that this Forest contains a circuit $(1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 1)$ which means that MST is not unique in D

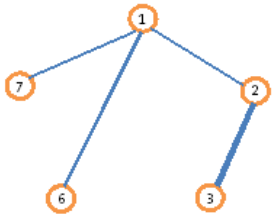
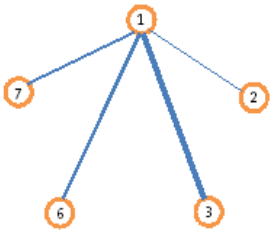
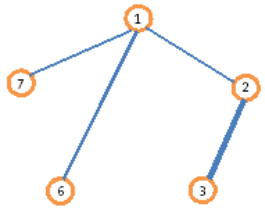


Fig. 2. The Forest in D

This Forest consists of two MSTs as can be seen in Fig. 3.



(a)



(b)

Fig. 3. Two possible MSTs (a) and (b)

In terms of weights sum, the two MSTs are the same. However, in terms of network analysis, they are totally different. For example, their degree distributions are different from each other.

Gondran algebra has simplified the search for SDU and MST in one single step, namely, the construction of the sequence $D^{*2}, D^{*4}, D^{*8}, \ldots$, until it converges. Since the number of iterations is predetermined, it is not necessary to test whether the convergence is achieved or not. Moreover, this sequence gives us Forest.

Once SDU has been obtained, Forest and an MST can be found in a simple manner. However, in network analysis, the problem to find an optimal MST is still open.

AFFILIATION

Maman Abdurachman Djauhari

Professor of Statistics
Director,
Centre for Research in Statistics and Data Analysis
Tjahaja Bina Statistika Indonesia, Ltd.P. (Commanditaire Ven nootchap)
Jl. Kanayakan A-15, Bandung 40135, Indonesia

REFERENCES

[1] Cassacuberta, C. and Castelet, M. 1999, *Mathematical Research Today and Tomorrow: Viewpoint of seven fields mwdallists*. Berlin: Springer-Verlag.

[2] Suzuki, J. 2002, *A history of mathematics*. New Jersey: Prentice Hall.

[3] Roux, M. 1975, Classification automatique. École d'eté d'analyse numérique, Paris: IRIA.

[4] Benzecri, J.P. 1980, *L'Analyse des données: 7. La taxinomie*. Paris: Dunod.

[5] Mantegna, R.N. 1999, Hierarchical structure in financial markets. *European Physical Journal*, B11, p. 193.

[6] Djauhari, M.A. 2012, A robust filter in stock networks analysis. *Physica A: Statistical Mechanics and its applications*, 391, p. 5049.

[7] Graham, R.L. and Hell, P. 1985, On the history of the minimum spanning tree problem. *Annals of the History of Computing*, 7, p. 43.

[8] Djauhari, M.A. and Gan, S.L. 2013, Minimal spanning tree problem in stock networks analysis: An efficient algorithm. *Physica A: Statistical mechanics and its applications*, 392, p. 2226.

[9] Gondran, M. and Minoux, M. 2008, *Graphs, dioids and semirings*: New models and algorithms. New York: Springer Science+Business Media, LLC.

[10] Mantegna, R.N. and Stanley, H.E. 2000, *An introduction to econophysics: Correlation and complexity in finance*. London: Cambridge University Press.

[11] Djauhari, M.A. and Gan, S.L. 2015a, Optimality problem of network topology in stocks market analysis. *Physica A: Statistical mechanics and its applications*, 419, p. 108.

[12] Djauhari, M.A. and Gan, S.L. 2015b, New York Stock Exchange performance: Evidence from the Forest of multidimensional minimum spanning trees. *Journal of Statistical Mechanics -Theory and Experiments*, 2015, p. 12005.

[13] Kazemilari, M. and Djauhari, M.A. 2015, Correlation network analysis for multi-dimensional data in stocks market. *Physica A: Statistical mechanics and its applications*, 429, p. 62.

[14] Cailliez, F. and Pages, J.P. 1976, *Introduction à l'analyse des données*. Paris: Societé de Mathematiques Appliquées et de Science Humaines (SMASH).

[15] Freeman, L.C. 1979, Centrality in social networks. I. Conceptual clarification. *Social Networks*, 1, p. 215.

[16] Borgatti, S.P. 2005, Centrality and network flows. *Social Networks*, 27, p. 55.

[17] Bonacich, P. 2007, Some unique properties of eigenvector centrality. *Social Networks*, 29(2), p. 5554.

Hidup: Suatu Sifat Keselanjaran

Ismail Mohd

ABSTRAK

Setiap kegiatan manusia pada setiap masa boleh disekutukan dan dilakarkan sebagai satu graf yang disebut fungsi. Oleh sebab kegiatan manusia kepunyaan satu set takterbilangkan, geraf itu adalah selanjar di sepanjang hidup seseorang. Oleh hal yang demikian, kegiatan mempunyai hubungan erat dengan keselanjaran dan kehidupan di akhirat. Melalui takrifan keselanjaran, maksud kehidupan boleh difahami secara matematik. Keselanjaran boleh membantu fungsi untuk membina beberapa rantau tarikan berasaskan pensifar fungsi tersebut.

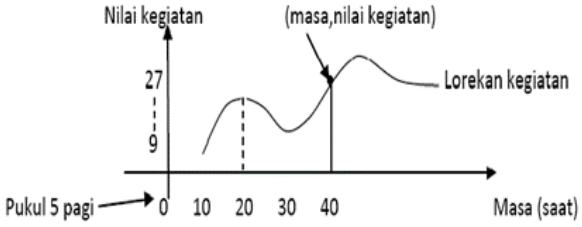
ABSTRACT

Each human activity at each time can be associated and plotted as a graph so-called function. Since human activities belong to the uncountable set, the graph is continuous along life of every one. Therefore activity has a strong relationships with continuity and life in the hereafter. Through the definition of continuity, the meaning of life can be understood mathematically. Continuity can help function to build several regions of attraction based on the zeroes of its function.

PENGENALAN

Ketika sarapan pagi terfikirkah kita akan kegiatan kita sebelum dan selepas sarapan itu? Adakah wujud kegiatan antara dua kegiatan yang berlainan sama ada sebelum, semasa dan selepas sarapan itu? Pepatah agung mengatakan "dalam kalangan dua orang berlainan jenis di dalam satu bilik, pasti terdapat yang ketiga." Jadi di antara dua titik berlainan pasti ada titik di tengahnya.

Jika setiap kegiatan disekutukan dengan satu nilai, maka setiap saat terdapat satu nilai sehingga jika diplotkan wujud satu graf seperti dalam Rajah 1. Namanya ialah lorekan

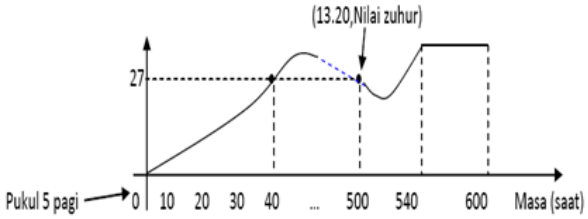


Rajah 1: Ketika (5.40 pagi,27 pahala Subuh berjamaah).

Untuk mendapatkan lorekan kegiatan yang unik, hendaklah setiap saat hanya dikaitkan dengan satu kegiatan. Jadi tidak mungkin lorekan menjadi unik jika ada garis mencancang memotong lorekan lebih daripada satu kali. Jika dalam beberapa saat sebelum dan selepas minit ke-20 kita tidur atau tiada kegiatan yang bererti, maka tiada garis memotong lorekan pada minit ke-20. Lorekan akan diberikan pentakrifan khusus dalam matematik seperti dalam perenggan berikut.

KONSEP FUNGSI

Fungsi ialah suatu konsep yang amat penting. Ia merupakan pungutan kegiatan atau ibadah dan sudah tentu yang memenuhi fitrah manusia (Rajah 2).



Rajah 2: Ketika (13.20, Nilai Zuhur berjamaah)

Dalam selang (0,40), semua kegiatan berlainan dan nilai kegiatan diandaikan berlainan sehingga terhasil lorekan 1-ke-1. Mulai dari 40 hingga 500 wujud sebanyak-banyaknya dua kegiatan yang berlainan tetapi nilai kegiatan adalah sama seperti nilai sholat subuh dan solat zuhur berjamaah, yakni 27. Jadi terbentuk lorekan paling banyak 2-ke-1. Untuk selang (540,600) lorekan bersifat banyak (≥2)-ke-1. Selanjutnya diberikan satu pernyataan yang mewakili Lorekan 1-ke-1 dan Lorekan banyak-ke- 1 yakni fungsi.

Takrif 1 : Lorekan $L : D_L \to R_L$ disebut fungsi jika untuk setiap $x, y \in D_L$, $x = y$ mengimplikasikan $L(x) = L(y)$.

Sebagai ringkasan, digantikan ungkapan "mengimplikasikan" dengan "$\Rightarrow$" .

Perbahasan A :
Ada dua kumpulan sahaja :

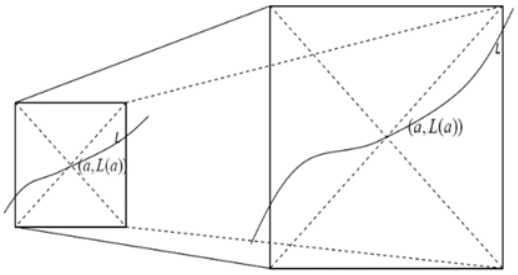
Kumpulan a :
(i) "$x = y \Rightarrow L(x) \neq L(y)$ ",tiada dalam Rajah 2
(ii) "$x \neq y \Rightarrow L(x) = L(y)$", ada dalam selang (40,500),
(iii) "$x \neq y \Rightarrow L(x) \neq L(y)$", lihat selang (0,40)

dan

Kumpulan b :
(iv) " $L(x) \neq L(y) \Rightarrow x \neq y$ ",Contoh [0,40],
(v) "$L(x) \neq L(y) \Rightarrow x = y$", tiada dalam Rajah 6, dan
(vi) " $L(x) = L(y) \Rightarrow x = y$", lihat [540,600].

(i)–(iii) tidak boleh menggantikan "$x = y \Rightarrow L(x) \neq L(y)$". Akan tetapi (iv) boleh menggantikan "$x = y \Rightarrow L(x) = L(y)$".

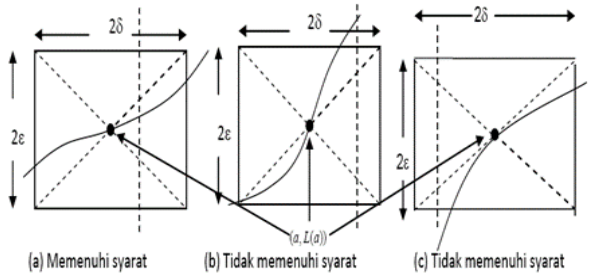
Perbahasan B : Tetapkan $(a, L(a)) \in L$. Periksa bahagian geraf L di sekitar $(a, L(a))$ dengan membuat sisi empat tepat berpusat di $(a, f(a))$ (Rajah 3).



Rajah 3: Sisi empat berpusat

Jika sisi empat itu kecil, maka besarkan (guna mikroskop) sehingga nampak lebih jelas. Khusus lihat lebar dan tinggi sisi empat sehingga L masih merupakan **fungsi**.

Secara geometri, syarat fungsi ialah setiap garis mencangcang di dalam sisi empat, memotong lorekan L di dalam sisi empat itu sendiri. (Rajah 4).



Rajah 4: Pelbagai sisi empat. Hanya (a) memenuhi syarat fungsi (memotong kiri-kanan sisi empat)

Syarat sisi empat: Jika tinggi sisi empat ialah 2ε, dan lebarnya ialah $,2\delta$ maka syarat sisi empat ialah

$$\forall\ x \in [a-\delta, a+\delta]$$
$$L(x) \in [L(a)-\varepsilon, L(a)+\varepsilon] \text{ atau } \forall\ x \ni$$

$$|x-a| < \delta\ ,\ |L(x)-L(a)| < \varepsilon$$

kerana

$$L(x) \in [L(a)-\varepsilon, L(a)+\varepsilon] \Rightarrow$$
$$L(a)-\varepsilon \le L(x) \le L(a)+\varepsilon \Rightarrow$$
$$-\varepsilon \le L(x)-L(a) \le \varepsilon \Rightarrow$$
$$|L(x)-L(a)| \le \varepsilon \ \vee\ |L(x)-L(a)| < \varepsilon$$

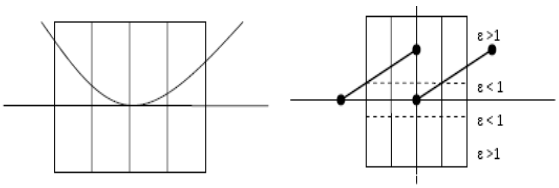
PROSES KESELANJARAN

Proses peneropongan graf fungsi di sekitar $(a, L(a))$ hanya boleh dilaksanakan apabila ada sisi empat yang cukup kecil berpusat di $(a, L(a))$ dan memenuhi syarat. Ada dua pertanyaan yang perlu dijawab secara bertahap.

Pertanyaan 1

Pilih $\varepsilon > 0$ tertentu, dapatkah dibuat sisiempat berpusat , $(a, L(a))$ tinggi 2ε dan memenuhi syarat terhadap L?

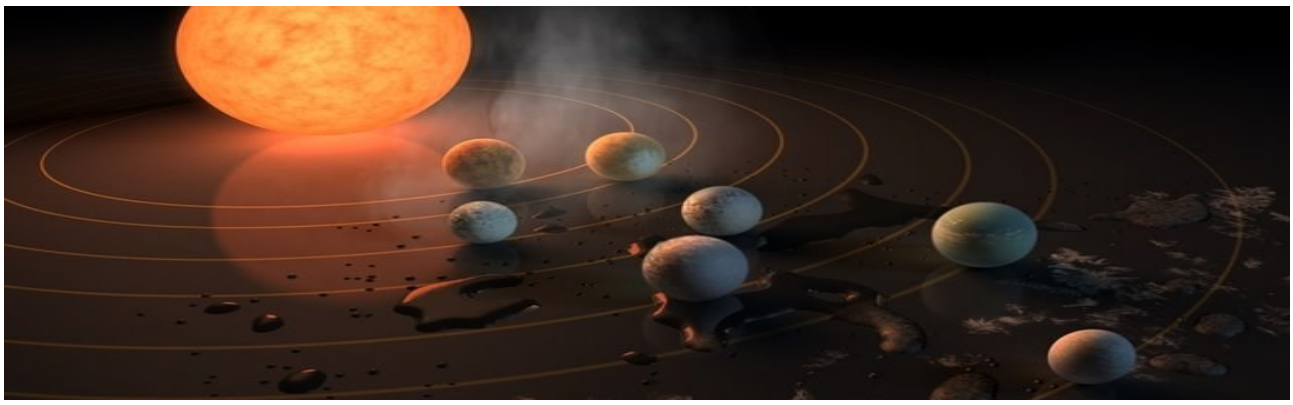
Jika sisi empat itu ada, maka wujud banyak sekali sisi empat yang memenuhi syarat. Misalnya, sisiempat dengan tinggi yang sama (lihat Rajah 5(a)).



(a) (b)

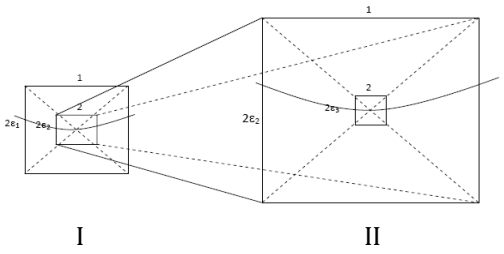
Rajah 5: Tinggi yang sama

Dapat dikatakan, jika ada sisi empat yang memenuhi syarat ε untuk tersebut, maka setiap sisi empat yang lebih tinggi dan lebar yang sama akan memenuhi syarat (Rajah 5(b)).



Pertanyaan 2
Apabila dapat dibuat sisi empat yang memenuhi syarat dengan tinggi ε , maka tahap berikutnya adalah buat sisi empat baru dengan ketinggian ε_1 (misalnya $\varepsilon_1 = \varepsilon/2$).

Kemudian **Pertanyaan 1** diulangi lagi bagi sisi empat dengan tinggi ε_1 itu. Perlaksanaan menjawab **Pertanyaan 1** dan secara beruntum, dilukiskan seperti dalam Rajah 6.



Rajah 6: Pelaksanaan Pertanyaan 1.

Pelaksanaan proses (memilih ε yang semakin kecil, menjawab **Pertanyaan 1**, sesudah itu **Pertanyaan 2**) tersebut, akan memunculkan dua **kemungkinan**.

Dalam Rajah 6, ada dua pasang sisi empat **I** dan **II**. Setiap pasang terdiri dari sisi empat **besar 1** dan sisi empat **kecil 2**. Sisi empat **1** dan sisi empat **2** menggambarkan apabila sisi empat **1** dengan tinggi $2\varepsilon_1$ memenuhi syarat, maka buatkan sisi empat **2** berketinggian $2\varepsilon_2 < 2\varepsilon_1$ yang memenuhi syarat. Apabila tiada sisi empat berketinggian $2\varepsilon_2$ yang memenuhi syarat, pemeriksaan **dihentikan**.

Sekiranya wujud sisi empat berketinggian $2\varepsilon_2$ yang memenuhi syarat (digambarkan sebagai sisi empat 2), maka pemeriksaan **diteruskan** dengan peneropongan (pembesaran melalui mikroskop).

Dari sisi empat **2** dalam **I** menjadi sisi empat **1** dalam **II** menggambarkan peneropongan (pembesaran). Di sini, pembesaran meliputi ukuran sisi empat dan lengkungannya.

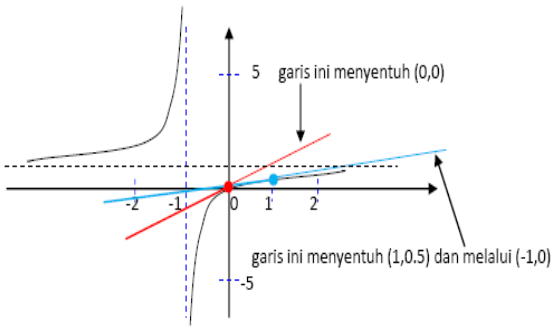
Kemungkinan 1 bahawa pada suatu tahap (setelah pemilihan ε tertentu), tidak ada sisi empat ketinggian 2ε yang memenuhi syarat sehingga fungsi dikatakan **tak selanjar** (proses peneropongan **terhenti**) di $x = a$.

Kemungkinan 2 betapapun kecilnya ε, sentiasa ada sisi empat yang memenuhi **syarat** ketinggian 2ε. Fungsi dikatakan **selanjar** (proses peneropongan **diteruskan**) di $x = a$.

PEMANFAATAN KESELANJARAN

Pencarian akar
Bagaimana akar fungsi $f : R \to R$ untuk $f(x) = x \div (x+1)$ $x \neq -1$ ditentukan.

Apabila dilukis, graf hampirannya adalah seperti dalam Rajah 7.



Rajah 7 : Graf fungsi f pada selang (-5,5)

Akar fungsi f ialah 0. Adakah wujud akar lain? Gunakan lelaran Newton $x_{k+1} = x_k - f(x_k) \div f'(x_k)$ asalkan $f'(x_k) \neq 0$ dan x_0 sebarang, untuk menentukan akar lain jika ada. Dengan menggunakan ungkapan fungsi f secara bebas diperoleh lelaran

$$x_{n+1} = -x_n^2 \quad n = 0,1,2,\ldots . \qquad (1)$$

Beberapa pilihan x_0 memberikan jawapan kepada persoalan ini seperti dalam Jadual 1.

Daripada graf fungsi, kelihatan akar fungsi f ialah 0 sahaja (unik), tetapi apabila digunakan persamaan (1) diperoleh akar -1 dan –M dengan M ialah nombor yang sangat besar dan nombor ini selalu ada selagi komputer boleh mengira.

Soalan: Di manakah salah atau silapnya penggunaan lelaran Newton $x_{k+1} = x_k - f(x_k) \div f'(x_k)$?

Jadual 1: Akar fungsi f menerusi pelaksanaan lelaran Newton: $x_{n+1} = -x_n^2$ $(n = 0,1,2,...)$

x_0	x_1	x_2	x_3	...	x_k	Akar	Betulkah?	Kenapa ?
0	0	0	0	...	0	0	Betul	Lihat rajah 7
1	-1	-1	-1	...	-1	-1	Palsu	Persamaan (1)
1.1	-1.21	-1.4641	-2.14359	...	-M	-M	Palsu	Persamaan (1)
-2	-4	-16	-256	...	-M	-M	Palsu	Persamaan (1)
-1.5	-2.25	-5.0625	-25.62891	...	-M	-M	Palsu	Persamaan (1)
0.5	-0.25	-0.0625	-0.00391	...	0	0	Betul	Selang Tarikan
0.9	-0.81	-0.0561	-0.00315	...	0	0	Betul	Selang Tarikan
-0.9	-0.81	-0.0561	-0.00315	...	0	0	Betul	Selang tarikan
-1.1	-1.21	-1.4641	-2.14359	...	-M	-M	Palsu	Persamaan (1)

Selang Tarikan ([1, 2, 3])

Pemilihan nombor $x_0 \in (-0.9,0.9)$ sebagai nombor awal lelaran Newton selalu memberikan 0 sebagai akar fungsi f. Lebih tepat lagi, nombor $x_0 \in (-1,1)$ menemukan akar 0 bagi fungsi f. Selang $(-1,1)$ dinamakan selang tarikan bagi akar 0 kerana apa-apa nombor dalam selang tersebut yang dipilih sebagai nombor awal bagi lelaran Newton, selalu sahaja menuju atau menumpu ke akar zero.

KESIMPULAN

Sesungguhnya pembelajaran dan penyelidikan dalam matematik (kalkulus) bukan untuk matematik itu sendiri sahaja bahkan untuk manusia itu sendiri. Pemahaman tentang fungsi memberi fahaman bahawa tiada tempat bagi kegiatan yang berlainan pada satu masa. Keselanjaran memberi gambaran tentang hubungan antara suatu kegiatan dengan kegiatan lain yang menghasilkan pungutan lorekan atau tanggungjawab seseorang terhadap kehidupannya.

AFFILIATION

Ismail Mohd

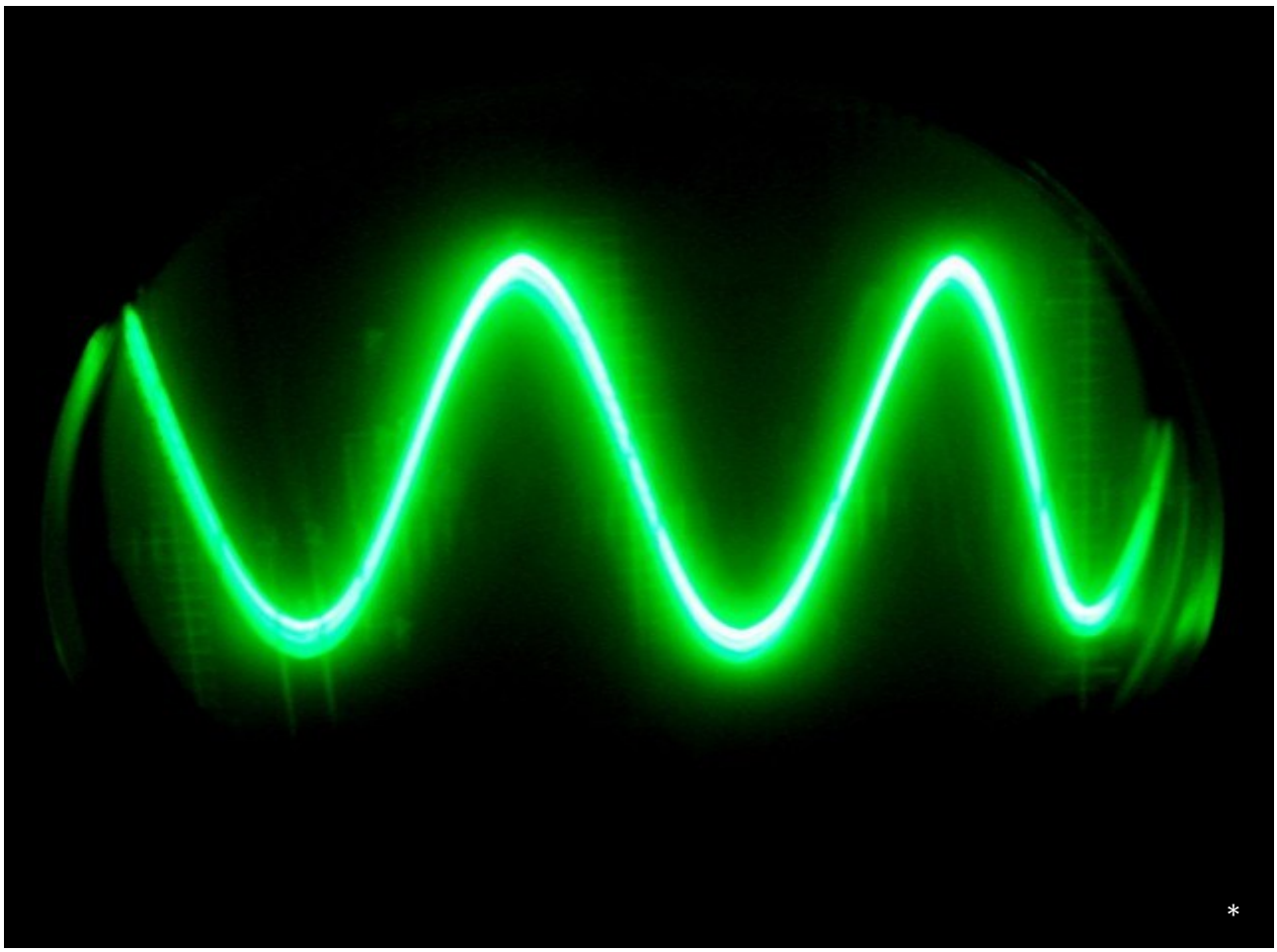
Research Fellow
Laboratory of Statistical Computational Operation Research,
Institute for Mathematical Research,
Universiti Putra Malaysia,
43000 UPM Serdang,
Selangor,
Malaysia.

RUJUKAN

[1] Wolfe, M. A., (1978). *Numerical Methods for Unconstrained Optimization: An Introduction*, Van Nostrand Reinhold Company, London,

[2] Mohd, I. B. (2000). *Identification of Region of Attraction for Global Optimization Problem Using Interval Symmetric Operator*, Journal of Applied Mathematics and Computation. 110, 121 – 131.

[3] Dennis, J. E., and R. B. Schnabel (1983). *Numerical Methods for Unconstrained Optimization and Nonlinear* Equations, Prentice-Hall.



The Role of Hermite Polynomials in Physics

Nurisya Mohd Shah,
Chan Kar Tim,
Hishamuddin Zainuddin

ABSTRACT

Polynomials is an expression in mathematics with certain conditions that have significant contribution in the area of mathematics and science. Even though polynomials is originally a pure mathematical language, they arise quite naturally in various problems in physics. In this note, we discussed the role of one of the many types of polynomials called the Hermite polynomials. This polynomials appear almost in each physics textbooks and provide an importance insight towards solving physical problems.

* *Image source:*
https://arstechnica.com/science/2014/07/quantum-state-may-be-a-real-thing/

INTRODUCTION

Polynomials is an expression in mathematics consisting of variables and coefficients which only employs the operations of addition, subtraction, multiplication, and nonnegative integer exponents. In mathematics, they are many types of the so-called classical orthogonal polynomials. Historically, these polynomials were discovered as solutions to differential equations arising in various physical problems. The classical orthogonal polynomials are a group of polynomials having certain properties that is also can be related to various problems in physics and also chemistry.

To name a few, they are collectively called Hermite, Laguerre, Legendre, Gegenbaur, Chebyshev polynomials and many others, see for example Boas (2006) and Chihara (1978). Each of the polynomials has been actively discussed in many scientific literatures.

The focus of this writing is to discuss explicitly the role of Hermite polynomials which arise in physics, particularly in quantum mechanics model. We give an overview of the simple case of quantum mechanical systems in one and two-dimensional space, namely the quantum harmonic oscillator. We also introduce the notion of noncommutative quantum mechanics which we denote as NCQM. This model is of current interest as more general type of families of Hermite polynomials arise from it.

Then we show a variousconnecting line between the Hermite polynomials in quantum mechanics and in NCQM for the case of Landau model of Hamiltonian in two dimensions. This type of families of polynomials has also connections to the study of quantum optics.

BACKGROUND

Series solutions of differential equations have been widely discussed in most of standard mathematical textbooks which have always been proven to have connections with various physical problems. The usual method in applied mathematics or mathematical physics research, is to find solutions to the associated differential equations which described certain physical models. These solutions are usually known to be the exact solvable potentials. The most simple quantum mechanics model for which every physics student should be able to solve is called the quantum harmonic oscillator problem. The solution to the time-independent Schrodinger equation which described the wave function can be written in terms of the Hermite polynomials, Tannoudji et.al (1977). This can be done up to *d*-dimension of the Schrodinger, which also give rise to the higher order solution in terms of the Hermite polynomials in n-variables.

For example, if one considers a two-dimensional system of non-interacting charged particles in the magnetic field, and look at the associated exactly solvable potentials, this is a very well-known physical problem namely Landau quantization. The solution is in terms of the two-dimensional time-independent Schrodinger equation, for which one could obtained a discrete energy values for charged particles to occupy the orbits, Landau et.al (1977). The corresponding eigenfunction is represented by the two-variables Hermite polynomials. One can refer to Balogh et.al (2015) forfurther works on the more generalized family of Hermite polynomials for which the physical problem associated to it is the non-commutative quantum mechanics model. This model specifically being introduced is motivated by problems found in string theory and high energy physics. Among other orthogonal polynomials which has become an active discussed area are the Laguerre polynomials which describe the hydrogen atom, Griffith (2014). The associated Laguerre for example, has also been proven to properly describe the vibrations of diatomic molecules which is very important in the field of quantum chemistry, called the Morse oscillator, see Shi-Hai Dong (2002).

QUANTUM HARMONIC OSCILLATOR

The one-dimensional quantum harmonic oscillator (qhos) is an analog to the simple harmonic oscillator for which the time-independent Schrodinger equation takes the following form,

$$H_{osc}\psi(x) = -\frac{\hbar^2}{2m}\frac{d^2}{dx^2}\psi(x) + \frac{1}{2}m\omega^2 x^2\psi(x). \quad (1)$$

H_{osc} is called the Hamiltonian of the system (oscillator), m is the particle mass with angular frequency, ω and at position x with the reduced Planck constant, $\hbar$. If we were to find the energy values E and also the corresponding eigenfunction, then we solve,

$$H_{osc}\psi(x) = E\psi(x), \quad (2)$$

which is just the eigenvalue equation.

The usual computation is by an algebraic method i.e. ladder operator method to find the exact solutions of Eq. (1) and thus (2) by rewriting H_{osc} in terms of the lowering operator, a and raising operator, $a^\dagger$

$$a = -i\hbar\frac{d}{dx} - im\omega x \;;\; a^\dagger = i\hbar\frac{d}{dx} + im\omega x$$

with the only survive commutation relation $[a, a^\dagger] = 1.$

Image source:

https://www.nyas.org/podcasts/media/podcast/a-quantum-state-of-mind/

Using Dirac notation, theeigenfunctions, are obtained by, $\langle x|n\rangle := \psi_n(x)|n\rangle$, $n = 1,2,3,$ are obtained by,

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$$

and

$$a|0\rangle = 0$$

where |0> is called a vacuum state. Therefore the coordinate space representation of these vectors, by functions on $L^2(x, dx)$, is the normalized,

$$\psi_n(x) = \left(\frac{m\omega}{\pi\hbar}\right)^{\frac{1}{2}} H_n(x')e^{-\frac{x'^2}{2}}$$

With $x' = \sqrt{\frac{m\omega}{\pi\hbar}}x$. Extending (qhos) for the two-dimensional case is straight forward. One writes the Hamiltonian as,

$$H_{2D} = \frac{\hbar^2}{2m}\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) + \frac{1}{2}m\omega^2(x^2 + y^2).$$

This time, defining the operators,

$$a_1 = i\hbar\frac{\partial}{\partial x} - im\omega x \ , \quad a_2 = -i\hbar\frac{\partial}{\partial y} - im\omega y$$

and their adjoints $a_1^\dagger$, $a_2^\dagger$ on $L^2\left(\mathbb{R}^2, dxdy\right)$,one obtains the eigenfunctions,

$$|n,m\rangle = \frac{(a_1^\dagger)^n(a_2^\dagger)^m}{\sqrt{n!m!}}|0,0\rangle \qquad (3)$$

and $a_i = |0,0\rangle = 0$ for $i = 1,2.$

Again, in the coordinate space representation, these appear as products of two Hermite polynomials,

$$\langle x, y|n,m\rangle := \psi_{n,m}(x,y)$$
$$= \frac{m\omega}{\pi\hbar}H_n(x')H_m(y')e^{-\frac{x'^2+y'^2}{2}},$$

with

$$x' = \sqrt{\frac{m\omega}{2\hbar}}x \ , \quad y' = \sqrt{\frac{m\omega}{2\hbar}}y$$

These polynomials, and also some of their variants, have also been used in quantum optical studies using beam-splitters.

LANDAU PROBLEM IN QUANTUM MECHANICS

For the Landau quantization problem of an charged particle (for e.g. electron) placed in a constant magnetic field, the Hamiltonian (in some conveniently chosen units) can be written as,

$$H_{\text{elec}} = \frac{1}{2}\left(\vec{p} - \vec{A}\right)^2$$
$$= \frac{1}{2}\left(p_x + \frac{y}{2}\right)^2 + \frac{1}{2}\left(p_y + \frac{y}{2}\right)^2 \quad , (4)$$

where $\vec{A}$ is the vector potential together with the position x, y and momentum p_x, p_y operators. On the Hilbert space $L^2(\mathbb{R}^2, dxdy)$ of our problem, we make the replacements,

$$p_x + \frac{y}{2} \to Q_1 = -i\frac{\partial}{\partial x} + \frac{y}{2} \ , \ p_y - \frac{x}{2} \to P_1 = -i\frac{\partial}{\partial y} + \frac{x}{2} \ .$$

Then, $[Q_1, P_1] = iI$ and the Hamiltonian becomes,

$$H_{\text{elec}} = \frac{1}{2}\left(P_1^2 + Q_1^2\right) \qquad (5)$$

The eigenvalues of this Hamiltonian, the so-called *Landau levels,* are

$$E_\ell = \left(\ell + \frac{1}{2}\right), \quad \ell = 0,1,2,\ldots\infty$$

each level being infinitely degenerate. There is a second set of operators that one can define,

$$Q_2 = -i\frac{\partial}{\partial y} + \frac{x}{2}$$

$$P_2 = -i\frac{\partial}{\partial x} + \frac{y}{2}$$

and $[Q_2, P_2] = iI$. The two sets of operators $\{Q_1, P_1\}$ and $\{Q_2, P_2\}$ are mutually commute namely,

$$[Q_2, Q_1] = [P_2, Q_1] = [Q_2, P_1] = [P_2, P_1] = 0$$

Similarly, we defined the operators,

$$A_1 = \frac{1}{\sqrt{2}}(iQ_1 - P_1) \ , \ A_2 = \frac{1}{\sqrt{2}}(Q_2 - iP_2)$$

and their adjoints, which then satisfy the only survive commutation relations, $[A_i, A_i^\dagger] = 1 \ , \quad i = 1, 2.$

The eigenstates of the Hamiltonian are thus given by,

$$\psi_{\ell,n} := \frac{1}{\sqrt{n!\ell!}}\left(A_1^\dagger\right)^n \left(A_2^\dagger\right)^\ell \psi_{00}$$

where $n, \ell = 0, 1, 2, \ldots,$ and $A_1\psi_{00} = A_2\psi_{00} = 0$

The solutions also give rise to the Hermite polynomials as for the case of two-variables. In addition, only available occupied orbits by the electron, are those with discrete energy levels.

NON-COMMUTATIVE QM MODEL

The notion of NCQM can be understood by the extra feature added to the original quantum mechanics model. NCMQ can only be realized in two and higher dimensional system. The algebra which described noncommutative model is,

$$[x_i, x_j] = i\Theta_{ij} \ ; \quad [p_i, p_j] = i\zeta_{ij} \ ,$$
$$[x_i, p_j] = i\hbar\delta_{ij} \ . \quad (6)$$

In literature, this algebra is called the deformed Heisenberg algebra. For $i, j = 1, 2, \ldots,$ both Θ_{ij}, ζ_{ij} are antisymmetric non-commutative parameter which measure the non-commutativity between two spatial and momentum coordinates.

A concrete physical example of a situation where the introduction of non-commutativity makes a difference in the observed energy spectrum of a quantum system is given as follows.

We go back to the problem of the electron in a constant magnetic field, for which we had earlier obtained the energy levels using the Hamiltonian (4).

We now rewrite this Hamiltonian, by replacing the standard position operators by the non-commutative ones.

We denote the non-commutative operators with a hat. Thus, we get the Hamiltonian,

$$H_{elec}^{nc} = \frac{1}{2}\left(\vec{\hat{P}} - \vec{\hat{A}}\right)^2$$
$$= \frac{1}{2}\left(\hat{P}_1 + \hat{Q}_2\right)^2 + \left(\hat{P}_2 + \frac{\hat{Q}_1}{2}\right)^2 \ , (7)$$

where

$$\hat{Q}_1 = q_x - \frac{\Theta}{2}p_y \ , \quad \hat{Q}_2 = q_y + \frac{\Theta}{2}p_x \ , \quad \hat{P}_1 = p_x \ , \quad \hat{P}_2 = p_y$$

Substituting in (7),

$$H_{elec}^{nc} = \frac{1}{2}\left(p_x + \frac{q_y}{2} + \frac{\Theta}{4}p_x\right)^2 + \frac{1}{2}\left(p_y + \frac{q_x}{2} + \frac{\Theta}{4}p_y\right)^2$$
$$= \frac{1}{2}\left[\left(1 + \frac{\Theta}{4}\right)p_x + \frac{q_y}{2}\right]^2$$
$$= \frac{1}{2}\left[\left(1 + \frac{\Theta}{4}\right)p_y - \frac{q_x}{2}\right]^2$$

Let $\gamma = \left(1 + \frac{\Theta}{4}\right)$ and introduce the operators,

$$\tilde{Q}_1 = \sqrt{\gamma}\,p_x + \frac{1}{\sqrt{\gamma}}\frac{q_y}{2} \quad , \quad \tilde{P}_1 = \sqrt{\gamma}\,p_y - \frac{1}{\sqrt{\gamma}}\frac{q_x}{2} \qquad (8)$$

Then,

$$\left[\tilde{Q}_1, \tilde{P}_1\right] = -\frac{1}{2}[p_x, q_x] + \frac{1}{2}[q_y, p_y] = i$$

Finally we get the Hamiltonian:

$$H_{elec}^{nc} = \frac{1}{2}\gamma\left[\left(\sqrt{\gamma}\,p_x + \frac{1}{\sqrt{\gamma}}\frac{q_y}{2}\right)^2 + \left(\sqrt{\gamma}\,p_y - \frac{1}{\sqrt{\gamma}}\frac{q_x}{2}\right)^2\right] + \frac{1}{2}\left(1 + \frac{\Theta}{4}\right)\left(\tilde{P}_1^2 + \tilde{Q}_1^2\right)$$

We conclude that the effect of non-commutativity is to shift all the energy levels by the amount $\frac{\Theta}{8}$:

$$\Delta E = \frac{\Theta}{8}.$$

As can be easily seen, introducing an additional noncommutativity, where the two observables of momentum also do not commute, would just shift the energies by an additional amount.

The deformed generalized Hermite polynomials arise from this model is biorthogonal as was shown in Balogh (2015).

CONCLUSION

As a conclusion, we have properly discussed and highlight how Hermite polynomials play a significant role in computing the exact solvable potentials in quantum mechanical problems. We show that there is a one-to-one correspondence of the d-dimensional schrodinger equation with associated potentials with the n-variables of the Hermite polynomials. As one goes towards higher order of the polynomials and also study its more generalized version, other important discoveries in physical science can also be realized.

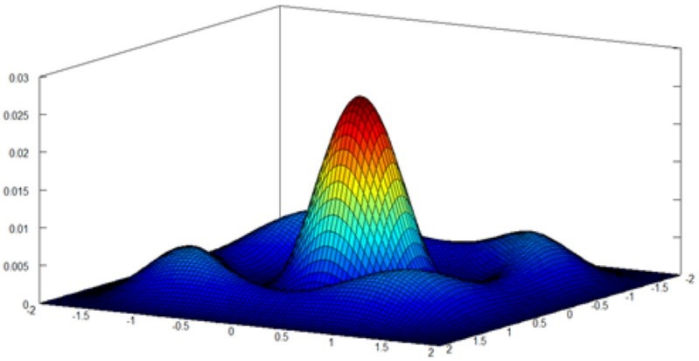


Image source: https://commons.wikimedia.org/wiki/File:6th_Eigenfunction_of_the_2D_Simple_Harmonic_Oscillator_2nd_perspective_view.jpeg

AFFILIATION

Nurisya Mohd Shah

Senior Lecturer,
Department of Physics,
Faculty of Science,
Universiti Putra Malaysia,
43400 UPM Serdang,
Selangor,
Malaysia.

Chan Kar Tim

Senior Lecturer,
Department of Physics,
Faculty of Science,
University Putra Malaysia,
43400 UPM Serdang,
Selangor,
Malaysia.

Hishamuddin Zainuddin

Associate Professor,
Deputy Director,
Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang,
Selangor,
Malaysia.

REFERENCES

[1] Balogh, F., Nurisya M. Shah and Ali, S.T. (2015). On Some Families of Complex Hermite Polynomials and their Applications to Physics. Operator Theory: Advances and Applications, Vol. 247, 157-171.

[2] Chihara, T.S. (1978). An Introduction to Orthogonal Polynomials, Gordon & Breach, Science Publishers, Inc.

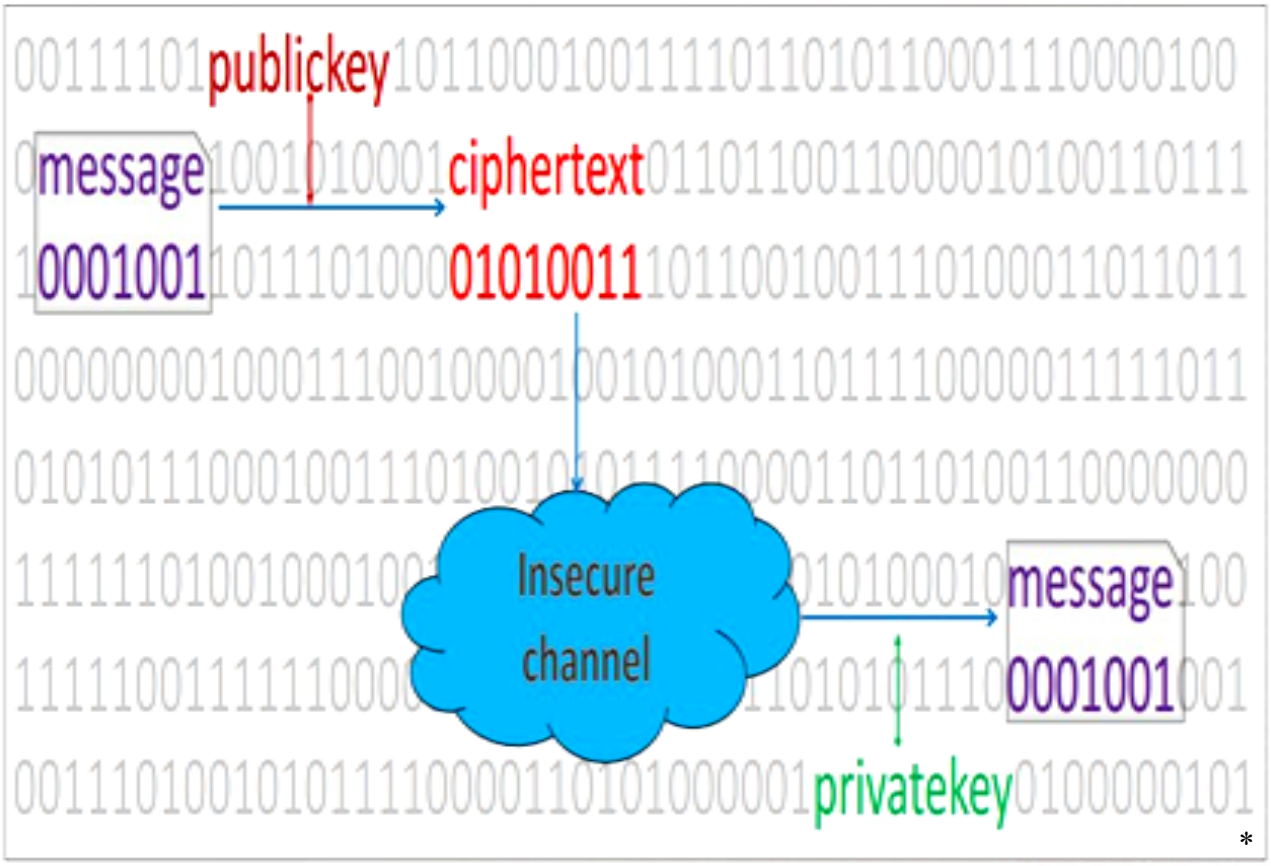
[3] Cohen-Tannoudji, C., Diu, B. and Laloë,, F. (1977). Quantum Mechanics Wiley, Vol. I, Complement EIII.

[4] Griffiths, D.J., (2014). Introduction to Quantum Mechanics Pearson New Int. Ed., pg 154.

[5] Landau, L. D. and Lifschitz, E. M. (1977). Quantum Mechanics: Non-relativistic Theory. Course of Theoretical Physics. Vol. 3, 3rd ed. London: Pergamon Press.

[6] Mary, L. Boas (2006). Mathematical Methods in The Physical Sciences, John-Wiley & Sons. pg 562.

[7] Shi-Hai Dong, Lemus, F. & Frank, A. (2002). Ladder Operators for the Morse Potential. Int. Journal of Quantum Chemistry, Vol. 86, 433-439.



*

Public Key Encryption Explained

Muhammad Asyraf Asbullah

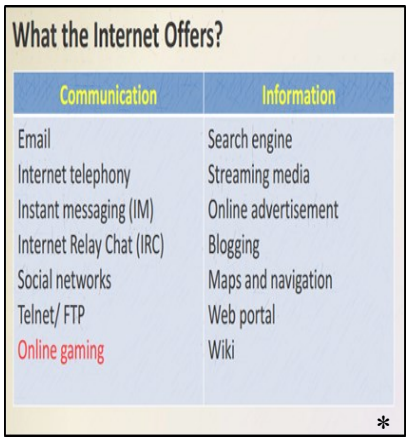
ABSTRACT

Post-1990's, the most common medium for transporting information is through electronic means that is the internet. Dependencies over the use of the internet led us to consider the issue of security and privacy of communication that occurs in the cyberspace, since it may easily be compromised by the unintended entities. Hence, the field of public key cryptography turns into a handy tool as a solution for that matter. This article will begin with the basic notion of cryptography that is known as the Kerckhoffs' principle, followed by a discussion of the public key encryption concept. Then, this article mentioned the concept of a one-way function and trapdoor one-way function, which are very important ingredients in order to design a functional public key cryptosystem. Finally, the terminology of the cryptographic hard problem is elaborated.

* *Image source:*
Optimal Design of a Rabin-like Cryptosystem, Poster PRPI2016, INSPEM

INTRODUCTION

Post-1990's, the exponentially growing common medium for transporting information is through electronic means. Currently, the internet assumes this role. The internet; is a worldwide network that is being shared amongst the people all around the globe. The internet contains many entities, indistinguishable from countries or nations, with users of varied interests and intentions, in every aspect imaginable. With just simple clicks, we could send emails or communicate with people, do monetary transactions through electronic commerce, and purchase items online.



*

Nowadays, our daily activities and conversation are dependent on the internet connectivity. Such internet dependencies led us to consider about the security and privacy of communication that occurs in the cyberspace, since it may easily be compromised by the authorities, hackers, or terrorists, of which some consider them as the adversary of the system. Hence, it is necessary and important for establishing a system or environment that guaranty the security of the internet users from any type of adversary.

Out of the wilderness and all the sophistication that we experience within the online world, the field of cryptography turns into a handy tool when security begins to matter. Cryptography provides a mean to ensure that our privacy and confidential information is secured, hence provides confidence for sharing and exchanging such information between other parties (the sender and the intended receiver). It is of a great interest, to be able to analyse the strengths and weaknesses of encryption and decryption processes.

In classical terminology, encryption is defined as a conversion procedure of information; which changes its readable state into another type of information, yet appearing to be nonsense. When we enter the age of the computer, the technologies evolve at a rapid state; therefore the definition of encryption is also amended.

In modern terminology, we may say that encryption is a process of converting ordinary information (i.e. known as a plaintext) into an unintelligible form (i.e. called as a ciphertext). On the opposite, the decryption is the reverse process of encryption, which functions to recover the intended or actual plaintext from its corresponding ciphertext.

Apparently, both of the encryptor (sender) and the decryptor (receiver) must have 'the key' in order to successfully perform their operation, respectively. The encryptor uses the key to scramble a plaintext (i.e. ordinary information such as a readable message or any meaningful data) and turns it into a ciphertext. This very same key is also being used by decryptor in order to recover back the original plaintext from its ciphertext. Consequently, no matter how obscure the algorithm for encryption and decryption is, it could be problematic if the key is not safe in the first place. This is the basic concept that is well known as the Kerckhoffs' principle, which states that the security level of encrypted information is as strong as the security of its key.

Definition 1. *(Kerckhoffs' Principle). Security of any cryptosystem should depend only on the secrecy of its key, and not the secrecy of the cryptosystem algorithm itself.*

The reason behind this is because it is much easier to maintain the secrecy of a key instead of an algorithm. If the key is exposed (independent to any reason on how it has happened), then it is easier to change the key instead of replacing the algorithm being used. Accordingly, it is good practice to replace a new key after a certain period. Furthermore, it is much more practical to share the same algorithm publicly between the communicating parties.

As suggested by Kerckhoffs's principle, the details of any cryptographic algorithm need to be known in public domain, except the secrecy for the key (Katz and Lindell, 2008), which is contrasting to the concept of the *'security by obscurity'. In modern cryptography philosophy, it is natural to assume that the adversary knows everything about the algorithm. Therefore, the only Information that needs to remain secret is the key.*

PUBLIC KEY ENCRYPTION

In the classical system, the secret key is supposedly being shared between the sender and the receiver in a symmetrical manner. In order to maintain the secrecy, the key must be shared or distributed securely to both parties beforehand. However, the process of exchanging such secret keys becomes problematic when the number of users gets larger since more keys are needed to be delivered to various parties. To tackle this problem, Diffie and

* *Image source:*
Nota Kuliah SSK1000 Pengenalan Kepada Teknologi Maklumat, Pusat Asasi Sains Pertanian, UPM

Hellman (1976) have come up with an indigenous idea that gives birth to the notion of *public key encryption.*

Definition 2. *(Diffie and Hellman, 1976). Let M denote the message space, C denote the ciphertext space, K denote the key space, m denote the plaintext and c denote the ciphertext. Public key encryption scheme is defined as follows.*

i. Key generation algorithm K is a probabilistic algorithm that will generate a public key denoted as e ϵ K and private key as d ϵ K respectively.
ii. Encryption algorithm E is a probabilistic algorithm that takes a message m ϵ M and the public key e, to produce a ciphertext c ϵ C as a function of c = $E_e(m)$.

iii. Decryption algorithm D is a deterministic algorithm which is given the ciphertext c and the private key d, will output m. That is m = $D_d(c)$.

Basically, if a cryptosystem that uses the same secret keys and shared by both; sender and receiver, then it is called as the symmetric cryptosystem. If a cryptosystem involves private(s) and public key(s), then the cryptosystem is commonly referred to as public key cryptosystem.

Definition 3. *(Proof of Correctness). For each pairs of key (e,d) ϵ K output by the algorithm K, and for every message m ϵ M and ciphertext c ϵ C then $D_d(c) = D_d(E_e(m)) = m$. c ϵ C then $D_d(c) = D_d(E_e(m)) = m$.*

The proof of correctness, as defined by Definition 3, suggest that the decryption is the reversal operation of encryption (i.e. to recover the plaintext from its ciphertext) and should be proven correct all the time.

CRYPTOGRAPHIC HARD PROBLEM

The design of the encryption and decryption function in a public key setting can be realised using the concept of a one-way function and trapdoor one-way function, respectively (Diffie and Hellman, 1976). It is a surprise to learn that despite years of research, it is still not known whether one-way functions exist (Katz and Lindell, 2008).

Definition 4. *(One-way Function). A one-way function is a function that is easily applied in one direction, but very difficult to calculate the inverse.*

Let $f: x \rightarrow Y$ be an invertible function. For $x \epsilon X$ and $y \epsilon Y$ then
i. it is easy to compute the value of y = f (x),
ii. it is hard to compute the value of $x = f^{-1}(y)$

The trapdoor information is a piece of auxiliary information that allows the inverse to be easily computed (Hoffstein et.al, 2008). For instance, the private key is said to be the trapdoor information to the encryption function. Without the correct private key, one will not be able to do decryption. On the contrary, decryption is an easy task with correct private key.

Definition 5. *(Trapdoor One-way Function). A trapdoor one-way function is a piece of information that allows the inverse for the one-way function to be easily computed (i.e. it is easy to compute the value of $x = f^{-1}(y)$ by using trapdoor information).*

Since we cannot prove the existence of the one-way function, we can always show that a problem is indeed hard corresponding to the concept of the one-way function.

Definition 6. *(Cryptographic Hard Problem). A cryptographic hard problem is defined as a concrete mathematical object which is easy to compute in one direction, but very hard to invert.*

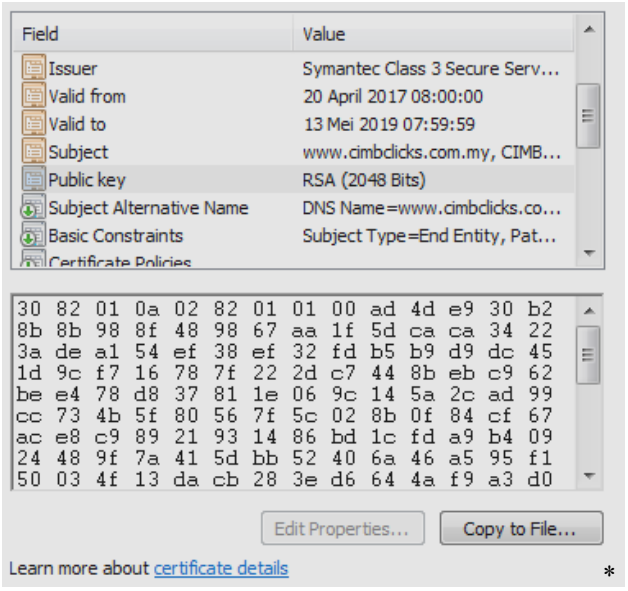
Basically, a cryptographic hard problem is widely believed or assumed to be very difficult to solve. Cryptographically speaking, the word *'hard'* from Definition 6 is referring to the difficulty level for solving a certain mathematical problem, including with the help from the state of the art technology. The terminology of the cryptographic hard problem provides confidence to the designing process of a cryptosystem, which the security measure is dependent on how difficult its related hard problem could be. If the correct steps are taken and the appropriate parameters are chosen, then to solve hard

* *Image source: https://www.cimbclicks.com.my/ibk/*

Image source: Buku Sainslah-2

problems might be infeasible, even via brute force or exhaustive search (i.e. tries all possible solutions). This is the main ingredient for designing and constructing a public key encryption algorithm.

The remark that from the Definition 6, does not necessarily mean that no one has figured out on how to do the inversion, but it is rather shown that there exists no efficient algorithm that runs in a reasonable time (i.e. in polynomial time) that can do such operation (Katz and Lindell, 2008). Thus, if the effort to solve a stated mathematical problem exceeds a certain amount of times (i.e. in exponential time) then we say that such mathematical problem is considered to be intractable, even using the most powerful tools available. On the other hand, suppose the stated mathematical problem can be solved below or within the range of a certain polynomial time, then the cryptosystem that relies upon such problems are considered insecure (Galbraith, 2012).



To date, one of the most celebrated problems in mathematics, particularly in number theory is known as the integer factorization problem and exhibits properties of a cryptographic hard problem.

The problem is to find the prime factors p and q from $N = p \ X \ q$. Until now, this problem is still being considered as a very difficult problem (i.e. infeasible to be solved in a reasonable time).

It is assumed to be very difficult to solve and is supported by decades of evidence for its hardness. In addition, it is widely believed that the integer factorization problem is a suitable candidate for a one-way function.

CONCLUSION

In the beginning, we have elaborated why it is necessary to ensure the security of the key, for both theoretical and practical point of views. We then further discussed the basic principle of public key encryption designs, which consist of three important algorithms; the key generation algorithm, the encryption algorithm and the decryption algorithm. In addition, it is customary for any cryptosystem to provide the proof of correctness for their algorithms. This is meant to show how the algorithms used for decryption could always decrypt the encrypted data of intended messages.

Finally, we conclude with an explanation of a mathematical object called the cryptographic hard problems, of which basically are used as parts of the designing process for public key encryptions in particular, and for any modern cryptosystems in general.

* *Image source: https://www.cimbclicks.com.my/ibk/*

AFFILIATION

Muhammad Asyraf Asbullah

Senior Lecturer,
Centre of Foundation Studies for Agricultural Science,
Universiti Putra Malaysia
43400 UPM Serdang,
Selangor,
Malaysia.

REFERENCES

[1] Diffie, W., and Hellman, M. E. (1976). New Directions in Cryptography. Information Theory, IEEE Transactions on, 22(6), 644-654.

[2] Galbraith, S. D. (2012). Mathematics of Public Key Cryptography. *Cambridge University Press.*

[3] Hoffstein, J., Pipher, J. C., Silverman, J. H., and Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. *New York: Springer.*

[4] Katz, J., and Lindell, Y. (2012). Introduction to Modern Cryptography. *CRC Press*.

Effects of Problem Posing on Mathematics Performance of Secondary School Students

Kanageshvary Sinnathamby,
Rosnaini Mahmud,
Rohani Ahmad Tarmizi

ABSTRACT

The challenge of globalisation today requires students to master the problem solving skills of mathematics. This study was conducted to explore the effects of Problem Posing (PP) as an alternative instructional strategy in the teaching and learning of mathematics effectively in Malaysian secondary schools. Previous research had discovered that PP enhances students' problem solving skills and mathematical behaviour. In addition, interest in the subject significantly improved. A quasi experimental study with non-equivalent control group post-test only design was conducted to investigate the effects of Problem Posing on form four Malaysian students' mathematics performance and instructional efficiency.

* *Picture of the author with students in her classroom during teaching period.*

The experiment was carried out for four weeks involving 74 Form Four students randomly selected from the district of Klang. The experimental (PP) group (n=38) were exposed to the PP instruction whereas the control (CT) group (n=36) were taught conventionally. The content of activities for two the groups was the same but differed in its structure of teaching. There were two instruments used in this study namely, mathematical learning worksheets, a post-test and Paas Mental Effort Rating Scale. The data were analysed using analysis of covariance (ANCOVA) and independent sample t-test. The findings of the study indicated that PP is more efficient than the conventional teaching strategy in enhancing Form Four students' mathematics performance.

INTRODUCTION

According to the National Curriculum Teaching Mathematics (NCTM), one of the central goals of Malaysia mathematics education is the development of the problem solving skills of the students. Competence based teaching, and the solution of practical problems call for teaching professionals who themselves are capable and knowledgeable in solving problems, and are able to rephrase real life situations in the language of mathematics. In order to train professionals who can adapt to the contemporary challenges, higher education needs to concentrate on the development of problem solving and problem posing skills. Future teachers need to attain problem solving skills and experiences to train the students in problem solving taking into account varying student skill sets and preparedness. Teachers need to provide multiple representations of problems including graphical approaches, as well as activities that fit the students' developmental stage and conceptual understanding. These different representations promote understanding and discovery of the underlying connections necessary for successful problem solving. It is especially important for future teachers to learn and practice the methods of problem posing, which are even more significant in the ever changing circumstances.

IMPORTANCE OF PROBLEM SOLVING

NCTM (2000) stated that problem-solving plays a crucial act in Mathematics especially through learning and understanding it. Problem-solving described as "engaging in a task for which the solution method is not known in advance," as well as proposed that "solving a problem is not only a goal of learning Mathematics, but also a major means of doing so" (p. 52). Problem-solving becomes a teaching tool for mathematical growth. The importance of a problem-solving task might have various opinions among learners. A problem-solving task can be a significant task for one student but could be a common task for another. When a question is encountered by students, which they have no immediate solution, problem-solving is the medium for which they can directly apply to come to an answer (Schoenfeld, 1985). In Malaysia, the understanding levels of problem-solving skills are the most important components of both primary and secondary Mathematics curriculum (Ministry of Education, 2013).

NCTM (2000) pointed out that to begin mathematical lessons and engage students' attention problem -solving based teaching should use interesting and well-selected problems. According to Kaur (2001), many teachers in countries such as Hong Kong and Singapore are more aware of problem-solving approaches to teach Mathematics. Kaur (2001) reported that the results of an early TIMSS study had led to several changes in the curriculum in Singapore where the teaching load was reduced by 30% and problem-solving had become the primary goal of learning Mathematics.

In any situation when the students were given chances and guided properly, they can become the effective problem-solvers and decision-makers, regarded that the environment must be right and suitable for them as discussed by Akinleye (2010). The students must get involved in the correct way of problem-solving processes with proper understanding and sense. Tchoshanov (2006) claimed that problem posing could support to develop students' problem-solving ability. In order to provide a quality problem, each student is encouraged to be engaged in a problem posing environment.

IMPORTANCE OF PROBLEM POSING

Mishra and Iyer (2013) defined problem posing as a production of new problems or a question by learners based on the given situation. Both the production of new problems and the re-generation of the given problems are what problem posing is all about. Therefore, problem posing can occur before, during or after a problem is solved. Problem formulation or re-formulation is one type of problem posing which can occur within the process of problem-solving. A problem-solver who engages in this form of problem posing would re-create a given problem in some ways to make it more accessible for a solution especially when solving a non-trivial problem. A problem formulation can represent one type of problem posing process. This is because the problem-solver

*

reconstructs a given statement of a problem into a new version that becomes the focus of solving. Since it may involve posing problems, problem formulation is somehow related to planning (Ilfi & Md. Nor, 2009).

In the newly-amended curriculum, priority will be given to classroom teaching and learning processes. To make learning more interesting, motivating and meaningful, instructional methods and pedagogies will be adapted towards more holistic approaches. The challenge in education nowadays is to effectively teach students of divergent abilities and differing rates of learning.

According to Zahara (2011), teachers should adopt various teaching methods to encourage active involvement among students in the teaching and learning process. Teachers should change their exam-oriented teaching strategies to strategies that are more appropriate to the needs of students. The effective teaching strategies were necessary in realizing the different abilities of students (Moore, 2014). The active teaching methods used by teachers could help them gauge the levels of skills that students have acquired before they can advance to a higher level of skills. Therefore, in learning a subject matter, students must first learn the terminologies, the basic concepts and the procedures before applying the basic knowledge to novel problems in everyday life.

HOW PROBLEM POSING RELATED TO PROBLEM SOLVING?

The objective of the curriculum of Malaysian secondary Mathematics is to develop students with deep mathematical knowledge in order for them to practise this knowledge in problem-solving and decision-making (Curriculum Development Centre, 2011). In the current curriculum of Malaysia, the course of coaching and acquiring knowledge such as problem-solving, interacting, thinking, making networks and the use of technology are affirmed. In fact, a crucial area in teaching and learning of Mathematics is the development of problem-solving skills. Polya (1945) reported that there are four stages of problem-solving heuristics which contain mastering the problem, scheming the strategy, carrying out the idea and reversing on the solutions. All these perhaps practiced by students while finding solutions for the problems in Mathematics and in their everyday routine.

In terms of problem posing, Kilpatrick (1987) argues that it should be the aims and means of instruction in Mathematics. It is possible to assimilate problem posing into the current Mathematics curriculum. Therefore, it should be given deliberation since how Mathematics is used in fixing real-world problems is exemplified. He suggested that the students can enhance problem-solving performances if students' concentration is drawn towards the reformulating process and giving practices in it. For example, students must understand that value of distance cannot exist in negative numbers in order to solve a word problem on the distance between two cities.

In order to boost students' achievement in problem-solving Mathematics, many researchers have concentrated on new instructional methods. The purpose is to help students understand the concepts of conceptualized abstract in Mathematics. Problem-solving is a complicated mental process that includes

***** *Picture of students while doing their assignments given during teaching period.*

processes such as making connections by correlating ideas, using background knowledge (concepts, facts, structures), perplexing, self-observing, thinking, inquiring, judging, and anticipating (Akay and Boz, 2010). The interpretation of this complex mental process into reality is by comprehending the challenges faced by students in Mathematics

According to Moore (2014), teachers could understand students learning through students' responses to the problem posing tasks. In his research, the problem posing activities engaged by students in producing problems are useful tools for assessing students' understanding. Akay and Boz (2010) in their research on the exploration of the use of meta cognitive skills by students during problem posing activities found that problem posing approach can be critical for positive attitudes of students towards Mathematics.

Problem posing activities are a proper channel to promote mathematical thinking amongst students. In problem posing circumstances, students are stimulated to make observations, experiments through differentiating some data and analyzing the results, and devise their own new problems that could be solved equally by using similar or different patterns.

The specific objectives of this study were:

i. To compare the overall mathematics performance between the PP group and the CT group.

ii. To compare instructional efficiency in mathematics based on a Paas Mental Effort Rating Scale between the PP group and the CT group.

METHODOLOGY

In this study, a quasi-experimental *post-test only control group* design (Creswell, 6446) was employed. Two Form Four social science elective classes were selected as intact groups in this study. The PP group involved 38 students whereas the CT group consisted of 36 students. A total of eight 70 minute lessons and four 35 minute lessons of mathematics were conducted by the researcher herself throughout the study. Table 1 shows the diagrammatic represen tation of the non-equivalent control-group post-test only design. An X indicates an experimental treatment, and a "dash" indicates no experimental treatment. The O indicate the measurements made during the post-test with Paas Mental Effort Rating Scale (PMERS).

Table 1. Non-equivalent Control-Group Post-test Only Design

Group	Treatment	Post-test Measures
Experimental	X	O + PMERS
Control	X	O + PMERS

During the acquisition phase of each lesson a worksheet was given to assess students' mental effort (load) expended to answer the given question. A well-designed activities integrating the use of the problem posing approach were prepared as modular lessons in this study. These modular lessons were used in helping the students to build mathematical understanding by the experimental group teacher. On the other hand the conventional instruction strategy was a whole-class instruction. Students were not allowed to use the problem posing approach modular. At the end of the treatment, a post-test were administered to both groups. Three instruments were used in this study.

The instruments applied were the learning assessments on mathematical concepts and skills learnt in the topic Algebraic (Quadratic Expression & Equation), the algebraic post-test and the Paas Mental Effort Rating Scale (PMERS). The one-way Analysis of Co-variance (ANCOVA) was used to test the statistical significance difference between the experimental group and the control group. All analyses were conducted using Statistical Package for the Social Sciences version 22 (SPSS 22.0). The statistical significance level was set at $p<0.05$.

VARIABLES STUDIED

The overall mathematics performance refers to students' overall achievement based on the Mathematics Achievement score which indicated the students' ability to demonstrate their understanding of mathematical concepts in Quadratic Expression & Equation topic learnt during the experimental period of time.

Mental effort can be considered to reflect the actual cognitive load which refers to the cognitive capacity that is actually allocated to accommodate the demands imposed by the task (Paas, Tuovinen and Tabbers, 2003). The nine point symmetrical rating-scale, ranging from very, very low mental effort (1) to very, very high mental effort (9), designed by Pass and van Merrienboer (1994) and Pass (1992) was used in this

study. Mental effort can be considered to reflect the actual cognitive load (Pass et al., 2003). Subjects were asked to report their invested mental effort on a nine-point symmetrical category scale by translating the perceived amount of mental effort into the numerical value, 1 to 9.

Instructional efficiency is a diagnostic instrument to identify and differentiate the efficiency of instructional conditions. It is measured by the 2-dimensional (2-D) instructional efficiency, which combines the measures the test and the mental load invested in the learning phase. The mean standardized test performance (P) and the mean standardized mental load during learning process (E) scores will be attained by learners in a certain condition are substituted into the following formula:-

$$\text{Instructional Efficiency} = \frac{zP_{test} - zE_{learning}}{\sqrt{2}}$$

In this study, instructional efficiency of each approach (problem posing & conventional teaching) will be computed by obtaining the mean overall test performance scores for each instructional approach and the mean mental load incurred during the solving of the assessment problems (students rating of each problem solving task using the PMER scale). The two scores are entered in the above formula to obtain the instructional efficiency score or index.

RESULT AND DISCUSSION

Performance measures

In this study, a one-way Analysis of Co-variance (ANCOVA) was used in order to find the effects of instructional methods, in the control group and the experimental group, on post-test scores. The dependent variable was the student's scores and the covariate was the student's pre-test scores. After adjusting for prior mathematics knowledge scores, there was a statistically significant effects between the two treatments on mathematics performances in Algebra, F (1, 66) = 19.19, p = .0001. The effect size, with partial eta squared value = .23 (which is a large effect size according to Cohen's (1988) guidelines, indicated that 23% of the variance in the mathematics performances in Algebra scores was explained by the treatments. An independent-samples t-test was conducted to compare the mean instructional efficiency index in Algebra for problem posing group and conventional teaching group. There was a significant difference in mean scores for problem posing group (M = .7391, SD = 1.052) and conventional strategy group (M = -.757, SD = 0.855); t (67) = 6.491, p =0.0001 (two tailed). Descriptive results in experiment, showed that students in problem posing group performed better on overall mathematics performance.

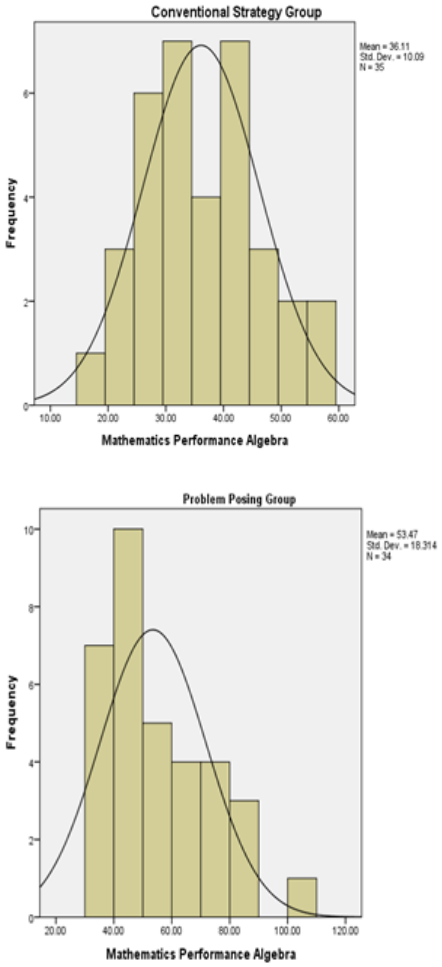


Figure 1 : Histogram with Frequency Curve of Mathematics Performance in Algebra.

CONCLUSION

From the perspective of teaching and learning mathematics, problem-posing have become imperative instructional approaches in classroom. These activities can be used to uncover how individuals learn mathematics based on the constructivist learning theory. However, adaptive, meaningful, and unique assessments are still underdeveloped for assessing students' learning, particularly for

problem-posing. The community of practice should take a step ahead to improve the assessment tools and should move from using traditional to more authentic assessment to measure students' learning holistically. In the context of research, large number of significant works has been published in the interim on problem-solving, but still very little on problem-posing has been written. Future studies should be exploring the complex link between problem-solving and problem-posing and should find authentic ways to assess students' learning based on these activities as a whole. Finally, as these activities have emerged as a significant component in mathematics education community, a more scholarly piece of work remains to be undertaken in the near future to improve the quality of education, particularly the teaching and learning of mathematics.

Picture with students in one of author's classroom.

AFFILIATION

Kanagesh Sinnathamby

Mathematics Teacher,
SMK(P) Raja Zarina,
Persiaran Raja Muda Musa,
42000 Pelabuhan Klang,
Selangor,
Malaysia.

Rosnaini Mahmud

Associate Professor,
Head of Laboratory of
Ethnomatematics and Didactics,
Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang,
Selangor,
Malaysia.

Rohani Ahmad Tarmizi

REFERENCES

[1] Akay, H., and Boz, N. (2010). The Effect of Problem Posing Oriented Analyses-II Course on the Attitudes toward Mathematics and Mathematics Self-efficacy of Elementary Prospective Mathematics Teachers. *Australian Journal of Teacher Education*, 35(1), 57-75.

[2] Akinleye, G.A. (2010). *Enhancing the quality of life in this complicated but dynamic world*. 69th Inaugural lecture, University of Ado-Ekiti, April 6.

[3] Aziz, Z., Nor, S. H. M., and Rahmat, R. (2011). Teaching strategies to increase science subject achievement: using videos for year five pupils in primary school. *World Applied Sciences Journal*, *14* (SPL ISS 4), 8-14.

[4] Creswell, John W., Plano Clark, Vicki, L., Gutmann, Michelle L., and Hanson, William E. "Advanced mixed methods research designs." *Handbook of mixed methods in social and behavioral research* 209 (2003): 240.

[5] Curriculum Development Centre (2011). *KBSM Mathematics Form Four*. Kuala Lumpur: Malaysian Education Ministry.

[6] Kaur, B. (2001). TIMSS & TIMSS-R – Performance of grade eight Singaporean students. In C. Vale, J. Horwood, & J. Roumeliotis (Eds), 2001 a mathematical odyssey (pp. 132-144). Proceedings of the 38th annual conference of the Mathematical Association of Victoria, Brunswick, Vic: MAV.

[7] Kilpatrick, J. (1987). *Soviet Studies in the Psychology of Learning and Teaching Mathematics.* Chicago: University of Chicago Press.

[8] Ministry of Education, Malaysia. (2013). *Malaysia Education Blue-print 2013: Preliminary Report 2013-2025.* Retrieved December 2015, 10, from http://www.moe.gov.my/en/pelan-pembangunan-pendidikan-malaysia- 2013-2025.

[9] Mishra, S., and Iyer, S. (2013, December).Problem Posing Exercises (PPE): An instructional strategy for learning of complex material in introductory programming courses. In *Technology for education (T4E), 2013 IEEE fifth international conference on* (pp. 151-158). IEEE.

[10] Moore, K. D. (2014). *Effective instructional strategies: From theory to practice*. Sage Publications.

[11] National Council of Teachers of Mathematics (NCTM) (2000). *Principles and Standards for School Mathematics*. Reston, VA: NCTM.

[12] Norman, I., Zaid Zainal, A., and Bakar, M. N. (July 21-23 2011). Secondary School Students' Abilities Through Problem Posing Activities. *Proceedings International Seminar and the Fourth National Conference on Mathematics Education* (pp. 1-12). Yogyakarta: Department of Mathematics Education, Yogyakarta State University. Retrieved December 12, 2015, from http://eprints.uny.ac.id/964/

[13] Polya, G. (1945). How to solve it: A new aspect of mathematical model.

[14] Paas, F.; Tuovinen, J. E., Tabbers, H. and Van Gerven, P. W. M. (2003). Cognitive load measurement as a means to advance cognitive load theory. *Educational Psychologist*. 38(1): 63-71.

[15] Schoenfeld, A. H. (1985). Mathematical problem solving. Orlando, FL. Academic press.

[16] Tchoshanov, M., Lesser, L., and Salazar, J. (2008). Teacher Knowledge and Student Achievement: Revealing Patterns. *Journal of Mathematics Education Leadership*, *10*(6), 38-48.

Abstract of Theses

Variational-Fixed Point Iteration Method for Boundary Value Problems of Ordinary Differential Equation

Mutah Wadai. 2017. Ph.D.
Supervisor: Prof. Dr. Adem Kilicman

Numerical methods are basically methods of approximation techniques, procedure or algorithm of various types used for solving mathematical problems, where the extent of possible errors are taken into account. Variational iteration method, fixed point iteration methods and finite element method have been shown to be among the most powerful tools for solving boundary value problems of ordinary differential equation over the years. These iterative methods are good for obtaining the approximate solution of ordinary differential equations. However, despite their good performances, variational iteration method and fixed point iteration method have some limitations in the choice of initial approximation which is done by guess work or chosen arbitrarily where the success of these methods largely depends on it. An inappropriate or unsuitable choice of initial approximation affects the result in a negative manner. While an increased inter element smoothness requirements placed on the base functions which always provide weak results are the major short comings of the finite element method.

In this study, we developed new alternative method of approximation which is the combination of variational iteration, fixed point iteration and the finite element method known as variational fixed point iteration method which harmonizes their full advantages and in many instances avoid their drawbacks for solving boundary value problem of ordinary differential equation. A simple strategy to determine the initial approximation to overcome the traditional way of determining the starting function through assumption or guessing is suggested. The finite element method is used as the starting function to variational iteration method while the first order approximation of variational iteration method is use as the initial approximation for fixed point iteration which will be used continuously until the result is obtained. We applied the variational fixed point iteration method for solving two-point and three-point boundary value problems of ordinary differential equation to demonstrate the efficiency and reliability of the method and comparisons were made with exact solution and other existing methods. The numerical results demonstrate that variational fixed point iteration method is promising and performs better than most of the existing methods because of its unique identification of the starting function which makes it an efficient tool for solving boundary value problems.

Successful Factoring Directions upon the Modulus $N = p^2 q$

Normahirah Binti Nek Abd Rahman. 2017. Ph.D.
Supervisor: Prof. Madya Dr. Muhammad Rezal Kamel Ariffin

The RSA public key cryptosystem widely used in practical cryptographic systems due to its security and effective encryption and decryption implementation. To obtain higher implementation efficiency, RSA with specific parameters were adopted in practical applications including RSA with small encryption exponents aiming to achieve a very fast encryption operation and those with small decryption exponents to speed up decryption process. Meanwhile, many variants of RSA have also been proposed for instance to achieve a fast decryption implementation. This is the reason most research focused on reducing encryption or decryption execution time and further analysis in term of mathematical proof are needed.

The thesis focuses on the development of new approach to deal with the existing problems of the previous work for solving factorization problem. The effort to attain this is through the implementation of the modulus

$N = p^2q$. The first part of this thesis describes the security and the difficulty level of factoring the modulus $N = p^2q$. As a result, a four new cryptanalysis has been developed under certain conditions using continued fractions expansion to show that $N = p^2q$ can be factored in polynomial time consecutively together with the estimation number of weak exponents satisfying the generalized key equation.

The second part of this thesis concentrates on generating *k* moduli of the form $N_i = p_i^2 q_i$ for some of the generalized key equations with the goal to factor the modulus $N = p^2q$. The existing method showed the way that the attack works for *k* instances of RSA moduli of the form $N_i = p_i^2 q_i$. Thus, the some attacks has been developed to compute the prime factors p_i and q_i of the moduli of the $N_i = p_i^2 q_i$ form in the polynomial time with some restriction on some parameter. All the proposed attacks prove that after transforming the generalized key equations into simultaneous diophantine approximation and the applying LLL algorithm to find suitably small parameters lead to factor moduli of the form $N_i = p_i^2 q_i$ simultaneously.

Additionally, by using certain term as an approximation of $\phi(N)$ satisfying the key equation leads to the factorization of moduli $N = p^2q$ in polynomial time using continued fractionexpansion. Then, two differences approaches system of equation for the key equation are also presented in order to factor *k* moduli of the form $N_i = p_i^2 q_i$ for the case $p \approx q$ and $p \approx 2q$.

Diagonal Quasi-Newton Updates Using Variational Principle Under Eneralized Norm

Sharareh Enshaei. 2017. Ph.D.
Supervisor: Assoc Prof. Dr. Leong Wah June.

This thesis concentrates on the development of some diagonal quasi-Newton (DQN) updating formula based on variational principle under various measures (norms) for matrices. The basic idea underline this type of methods is to approximate the solution of Newton's equation by means of approximating the Hessian matrix via quasi-Newton update. So, diagonal quasi-Newton methods, which are a class of quasi-Newton methods, alter the standard quasi-Newton updates of approximating the Hessian matrix to diagonal updating matrices. Under weak secant equation, updating formulas are derived as the solution of the variational problems which is typically used in deriving standard quasi-Newton method. One of the most significant factors to find the metric is by choosing an appropriate norm which measures the deviation between Hessian (also inverse of Hessian) and the approximation. Hence, the aim of this thesis is to exploit associated techniques in deriving diagonal updates with weak secant equation in order to construct a new diagonal updating for DQN methods under some generalized Frobenius norm. It leads to recommendation of the best matrix norms for solving proposed variational problems. Lastly, the convergence of the methods under the standard line search methods are shown using some mild assumptions. To preserve the positive definiteness of the new DQN updating scheme, it is essential to incorporate some strategies into the methods. Thus, another purpose of this thesis is to formulate a technique for diagonal updating subject to secant equation for non-positive definite cases. An approach to preserve positive definiteness through updating the square root or Cholesky factor of the approximating matrices is proposed. In addition, we suggest a modified diagonal update for DQN method which uses more accurate curvature information in deriving the diagonal updating formula. Higher order Taylor expansion is applied and leads to approximate the second-order curvature by modified DQN curvature condition with a higher precision than the unmodified ones. The slight improvement of modified methods which use both available gradient and function value information is reasonable. Finally, the conclusion of this thesis is given and a few future studies have been suggested.

Robust Estimation For Single Index Quantile Regression. And Bayesian Variable Selection

Taha Hussein Ali Alshaybawee. 2017. Ph.D.
Supervisor: Prof. Dr. Habshah Midi

Quantile regression (QReg) can be considered as one of the important statistical breakthroughs in recent decades and has become a popular technique. The attractive feature of QReg is that it is capable of giving a more complete picture of the underlying interrelations than the ordinary least square regression analysis. Moreover it is robust to outliers in the y direction. Nonetheless, it is easily affected by High Leverage Points (HLPs). The least trimmed quantile regression (LTQReg) methods is put forward to overcome the effect of high leverage points. However, it is not very successful in reducing the effects of HLPs. Hence, we proposed two modified least trimmed quantile regression (MLTQReg). The first MLTQReg is developed by incorporating the Reweighted Least Trimmed of Squares (RWLTS) in the LTQReg algorithm and we call it the Reweighted Least Trimmed Quantile Regression (RWLTQReg). The second MLTQR method is called the Modified Least Trimmed Quantile Regression based on Robust Mahalanobis Distance (RMD) denoted as RMD-LTQReg. The weight based on RMD and the RWLTS are integrated in the LTSReg algorithm in order to establish the RMD-LTQReg. The results of the study indicate that the RMD-LTQReg is the most efficient method followed by the RWLTQReg and other existing methods in this study.

In this study, an alternative method of reducing the effect of HLPs in QReg is proposed. The proposed method is based on weighting steps that aim to improve the efficiency of the estimates. Not much research has been done to develop such method in QReg. Therefore, Weighted Quantile Regression (WQR) is developed to reduce the effect of HLPs in QReg. The proposed method is formulated based on the weight derived from the Diagnostic Robust Generalized Potential (DRGP). The findings indicate a significant superiority of the proposed WQR method compared to RMD-LTQReg, RWLTQReg and other existing methods in this study.

The single index quantile regression model (SIQReg) is proposed by Wu et al. (2010) to overcome the dimensionality problem in nonparametric quantile regression. It has an attractive features where it combines the strength of parametric and the flexibility of nonparametric modelling. Nevertheless, SIQReg is easily affected by HLPs. Thus far, no research has been done on the development of estimation method to reduce the effect of HLPs in SIQReg. Hence, Robust Single Index Quantile Regression (RSIQReg) Estimation Algorithm is proposed to close the gap in the literature. The results of the study signify that our proposed RSIQReg method has done a credible job compared to other methods in this study.

Due to the attractive feature of the SIQReg, we propose a Bayesian Single Index Quantile Regression (BBSIQReg) approach for modelling a binary data. Bayesian hierarchical model constructs are formulated, with an adaptive lasso penalty as a variable selection to model a binary data. To the best of our knowledge, no such algorithm has been developed. The results of the study show that out proposed BBSIQReg is more efficient than other methods. It is now evident that the elastic net approach has attracted much interest in the variable selection methodology especially when the number of variables is greater than sample size, n. Thus far, no specific algorithm has been proposed to formulate Bayesian elastic net for single index quantile regression (BENSIQReg) for estimation and variable selection. Hence, we develop BENSIQReg algorithm, in this regard. The Gaussian process prior is considered for an unknown link function and a Gibbs sampler algorithm is adopted for posterior inference. From this study, we concluded that our proposed BENSIQReg performs better than other existing methods.

Simulation studies and real data examples are used to evaluate the performance of our proposed methods. We conclude that all the proposed methods are very efficient compared to other existing methods.

Numerical Solutions of Linear Fredholm Integro-Differential Equations of the Second Kind Using Quadrature-Difference Methods

Chriscella Binti Jalius. 2017. M.Sc.
Supervisor: Prof. Dr. Zanariah Abdul Majid

Fredholm integro-differential equation (FIDE) is an equation which is the unknown functions appears under the sign of derivative and also integral sign. Therefore, the formulation of numerical quadrature rules and finite difference method are applied for solving first-order and second-order linear FIDE of the second kind. The finite difference method is used for ordinary differential equations part, while composite quadrature rules are applied for the integral part of FIDE. Numerical solutions of linear FIDE by using quadrature-difference methods are proposed in this thesis.

There are four types of formulation proposed in this thesis which composite Simpsons 3/8 rule with first derivative of 5-point finite difference, composite Simpsons 3/8 with second derivative of 5-point finite difference, composite Booles rule with first derivative of 7-point finite difference and composite Booles rule with second derivative of 7-point finite difference. These formulations will be used to produce an approximation equation in order to discretize the FIDE into a system of linear algebraic equation. The system of linear algebraic equation will be solved by using Gauss elimination method. An algorithm and a coding of the proposed methods developed in this thesis. The source of the coding for solving linear FIDE is developed by using C programming with constant step size.

The four types of formulation which based on quadrature rules and finite difference method are implemented for solving Type 1 and Type 2 of first-order and second-order linear FIDE. In this thesis, the boundary condition will be considered in solving the second-order linear FIDE. Moreover, the order of accuracy of the proposed method are studied in this thesis.
Finally, the numerical experiments were carried out in order to examine the accuracy of the method. The result indicated that the proposed methods are suitable for solving first-order and second-order linear FIDE of the second kind.

Effects of Using Geogebra Software on Students' Achievement with Different Spatial Visualization Ability In Learning Coordinate Geometry Among Form Four Students

Royati Binti Abdul Saha. 2017. M.Sc.
Supervisor: Assoc. Prof. Dr. Ahmad Fauzi Mohd Ayub

The purpose of this study is to identify the effectiveness of the use of open source software, Geogebra towards mathematics performance for the topic of Coordinates Geometry. Besides that, this study will examine the use of Geogebra towards student with different spatial visualization ability and motivation towards mathematics. The study was conducted using quasi-experimental design with a post-test control group of 53 students of form 4 in one school in Wilayah Persekutuan Kuala Lumpur. Students are divided into two groups, a control group (N = 26 students) and treatment group (N = 27 students). The study was conducted for eight weeks involving four instruments namely Coordinate Geometry Achievement Instructional Materials Motivation (IMMS), Geogebra Usage Survey and Van Hiele test. The findings show that the use of the Geogebra significantly help students get a better score rather than the control group. Furthermore, students with low visual abilities in Geogebra group scored significantly better than low visual abilities in control group. In terms of motivation toward mathematics, students from the Geogebra group had a mean score significantly higher than the control group. Geogebra also help students improved their Van Hiele level of geometric thinking. Overall, this study showed that the use of Geogebra can help students gain a good score and motivate them to learn mathematics. Geogebra also can help low visual students to acquire a better score. Therefore, using the Dynamic Geometry Software, Geogebra is an effective strategy in teaching and learning mathematics.

Numerical Solutions Of Boundary Value Problems Using Direct Two Point Block Methods.

Nurul Nadirah Binti Zakaria. 2017. M.Sc.
Supervisor: Prof. Dr. Zanariah Abdul Majid

In this study, a new direct two point block method is proposed for solving boundary value problems. The direct two point block method is used together with the non-linear shooting technique in solving boundary value problems using constant step size. Moreover, this block method is also implemented with one-off step point and two-off step point for solving second order boundary value problems of Dirichlet and Neumann types. The algorithms for solving second order boundary value problems with Dirichlet and Neumann types are then executed in programming code which is written in C language.

Some researchers have developed the block method for solving boundary value problem numerically. The advantage of the new direct two point block method proposed in this research is that it is able to solve second order boundary value problems directly without reducing it to a system of first order differential equation with boundary conditions. Besides, this method is able to apply together the Newton and the Newton-like method to improve convergent rate of the problems.

The outcome showed that the performance of these methods can obtain better results in term of total step, maximum and average error, and execution time when compared to existing methods. In conclusion, the proposed method in this study is suitable for solving equation of second order two point boundary value problems with Dirichlet and Neumann types.

INSTITUTE FOR MATHEMATICAL RESEARCH
Universiti Putra Malaysia
43400 UPM Serdang
Selangor
Malaysia

+603-8946 6878 **+603-8946 6973**