Embracing Mathematical Diversity

Selected papers from

SEMINAR ON MATHEMATICAL SCIENCES 2019 (SOMS2019)

UNIVERSITI PUTRA MALAYSIA

BERILMU BERBAKTI

Editors

Muhammad Asyraf Asbulah

Mohd Ezad Hafidz Hafidzuddin

Muhammad Asyraf Asbulah
Mohd Ezad Hafidz Hafidzuddin
Editors

Embracing Mathematical Diversity

Selected papers from Seminar on Mathematical Sciences 2019 (SOMS2019)

Published by
UPM Press
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

First Print 2019

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Embracing Mathematical Diversity: Selected papers from Seminar on Mathematical Sciences 2019 (SOMS2019) / Editors Muhammad Asyraf Asbullah, Mohd. Ezad Hafidz Hafizuddin.

ISBN 978-967-2395-08-9
1. Mathematics--Research--Malaysia--Congresses.
2. Education, Higher--Research--Malaysia-- Congresses.
3. Government publications--Malaysia.
I. Muhammad Asyraf Asbullah.
II. Mohd. Ezad Hafidz Hafizuddin.
III. Seminar on Mathematical Sciences (2019: Serdang, Selangor).
510.720595

Preface

The first Seminar on Mathematical Sciences (SOMS2019) took place at the Seminar Room, Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia on twenty-fifth September 2019. Researchers and postgraduates from various universities over Malaysia gave an attention-grabbing presentation concerning the present literature reviews on their field.

At the end of the seminar, the presenters and the audience concurred that mathematical variety may be an intriguing research challenge. In the era of multidisciplinary research, such a challenge can be crucial for the long term to the mathematical community in Malaysia. Hence, we determined to edit a book to fit with the word of wisdom; *Embracing Mathematical Diversity* which also was chosen as the theme of SOMS2019.

UPM Press, Universiti Putra Malaysia promptly agreed to publish such a volume. We approached leading scientists within the several fields and received favorable answers from all of them. There have been sixteen papers chosen for publication. It covers selected areas in mathematical studies like fluid dynamics, mathematical cryptography, and numerical analysis.

We are now very happy to present this book. We hope that it serves as an introduction to the respective mathematical field, as an overview of the state of the art, and as an encouragement for many more researchers and graduated students to join us in embracing mathematical diversity.

UPM Serdang, Malaysia
November 2019

Muhammad Asyraf Asbullah
Mohd Ezad Hafidz Hafidzuddin

List of Corresponding Authors

Nor Fadzillah Mohd Mokhtar
Universiti Putra Malaysia
nor_fadzillah@upm.edu.my

Muhammad Rezal Kamel Ariffin
Universiti Putra Malaysia
rezal@upm.edu.my

Mohd Ezad Hafidz Hafidzuddin
Universiti Putra Malaysia
ezadhafidz@upm.edu.my

Siti Suzilliana Putri Mohamed Isa
Universiti Putra Malaysia
ctsuzilliana@upm.edu.my

Kartini Ahmad
International Islamic University Malaysia
kartini@iium.edu.my

Muhammad Asyraf Asbullah
Universiti Putra Malaysia
ma_asyraf@upm.edu.my

Ahmad Nazri Mat Som
Universiti Putra Malaysia
nazrims@upm.edu.my

Yong Faezah Rahim
Universiti Putra Malaysia
yfaezah@upm.edu.my

Mohammad Hasan Abdul Sathar
Universiti Putra Malaysia
mohdhasan@upm.edu.my

Ahmad Fadly Nurullah Rasedee
Universiti Sains Islam Malaysia
fadlynurullah@usim.edu.my

Norfifah Bachok
Universiti Putra Malaysia
norfifah@upm.edu.my

Contents

Chapter 1

Introduction

Muhammad Asyraf Asbullah*

* Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: ma_asyraf@upm.edu.my

On September 25, 2019, Wednesday, Mathematics Unit of the Center for Agricultural Science, Universiti Putra Malaysia held a mathematics seminar entitled "Seminar on Mathematical Sciences" (SOMS2019). The seminar aims to bring together to share ideas and research works among academics, researchers and postgraduates involved in mathematical science research. A total of 35 participants attended the seminar and 16 of them have presented their findings. Participants included researchers from various research backgrounds and universities in Malaysia. It is hoped that these seminars will play a role in leading the sustainability industry which requires mastery of science especially in the field of Mathematics. The rest of this book is organized as follows.

A theoretical investigation of Marangoni-Bénard convection in the existence of internal heating of an anisotropic porous medium of a ferrofluid layer system had been presented in Chapter 2 by using regular perturbation method. The goal is to initiate Marangoni-Bénard convection in an anisotropic porous medium of a ferrofluid layer system with additional internal heating impact. The lower and upper limits are regarded to be rigid-free borders and both limits are regarded to be insulated to any disturbance of temperature. Using a regular perturbation technique, the eigenvalue problems are solved. Hence the critical equation of Marangoni and thermal Rayleigh acquired.

A discussion on linear stability analysis as a tool to study the effect of internal heating and Coriolis force on couple stress fluid in an anisotropic porous medium, which is heated from below is presented in Chapter 3. The Boussinesq approximation and momentum equation also used for the density variation in the porous medium. The eigenvalue problems of the perturbed state are obtained by using the Galerkin method from a normal mode analysis. The results in this chapter show the effect of internal heating and mechanical anisotropic parameter destabilizes the system while increasing the thermal anisotropic parameter, the effect of Coriolis force and couple stress fluid helps to stabilize the system.

A survey on the partial key exposure attacks which are categorized for the type of exposure on the RSA cryptosystem parameters is discussed in Chapter 4. The first category compiles the attacks where the adversary has Most Significant Bits (MSB) or Least Significant Bits (LSB) of the RSA primes. The second category focuses on the attacks where MSBs of the RSA private exponent are exposed and the last category considers attacks where LSBs of the RSA private exponent are exposed. In a nutshell, both attacks assume that an adversary employs an incomplete arrangement of bits of the RSA private keys. The methods used in the attacks manipulate mathematical structures of the keys.

Next, Chapter 5 aims to solve a problem of magnetohydrodynamics rotating boundary layer flow over a permeable shrinking sheet numerically via the Keller-box Method. The similarity transformations are used to reduce the system of partial differential equations (PDE) into a system of ordinary differential equations (ODE). The transformed equations are then solved using the Keller-box Method. The effects of the governing parameters involved, namely magnetic parameter, suction parameter and rotating parameter on both the velocity and lateral velocity fields are presented and discussed.

A study about magnetohydrodynamics (MHD) Newtonian fluid flow caused by an exponentially stretching sheet is presented in Chapter 6, subjected to the parameters such as assisting flow and buoyancy ratio. The governing basic equations such as flow, momentum, energy and concentration equations are converted to nonlinear ordinary differential equations (ODEs) by using the non-similarity method. Subsequently, the ODE is solved numerically, hence the numerical results for the skin friction coefficient, the local Nusselt number, and the local Sherwood number are obtained. Moreover, the variations of the velocity, temperature, and concentration profiles are presented, along with the characteristics of the flow, heat and mass transfer.

The mathematical model of the magnetohydrodynamics (MHD) of Casson fluid flow with heated at the surface due to Newtonian heating is described in detail in Chapter 7. The study takes into account in a concentrated Casson fluid flow with the existence of thermal radiation. Similarity transformation is used, to convert the governing equations, for instance; continuity, momentum, energy, and mass diffusion equations into ordinary differential equations (ODE). Later on, these ODE is determined by applying the finite-difference method. The profiles of velocity, temperature, concentration and concentration gradient are depicted for certain values of controlling parameters.

Chapter 8 reviews several variants of RSA cryptosystem constructed based on various algebraic structures such as the instances of RSA extended with elliptic curves, Gaussian integers, and Lucas sequences. Remark that this chapter specifically focuses on the variants of RSA having its public and corresponding private keys e and d respectively and satisfying a very particular key equation. All cryptanalytic works presented in this chapter were scrutinized especially via the continued fractions method and Coppersmith's method.

The qualitative effect of a cubic temperature gradient on the linear stability

analysis on the onset of Rayleigh-Benard convection in an Eringen's micropolar fluid is studied throughout Chapter 9 via a single term Galerkin technique. In the case of Rayleigh-Benard convection, the eigenvalues are obtained for free-free, rigid-free, rigid-rigid velocity boundary combinations with isothermal and adiabatic temperature conditions on the spin-vanishing boundaries. The influence of various parameters has been analyzed. This chapter deals with two cubic temperature gradient and a linear temperature profile and their comparative influence on the onset of convection are discussed.

Chapter 10 investigates the influence of non-uniform basic temperature gradients in the presence of internal heat generation, electric field and feedback control on the onset of Marangoni convection in a micropolar fluid via the linear stability analysis. As a result, the eigenvalue for an upper free adiabatic and lower rigid isothermal boundaries are obtained and solved using the Galerkin method. The effect of internal heat generation, electric number, and feedback control on the onset of Marangoni convection have been figured out. Three non-uniform basic profiles of the temperature are studied and several general conclusions about their destabilizing effects are revealed.

The characteristics of the fluid flow and heat transfer of magnetohydrodynamic (MHD) thermosolutal Marangoni convection in the presence of heat and mass generation or consumption with radiation through the permeable surface is studied Chapter 11. The basic governing partial differential equations transformed into a nonlinear ordinary differential equation using the similarity transformation and solved numerically. The analysis is done to analyze the effect of radiation and suction/injection on the flow of the fluid and the features of the problem are generalized in the form of tables and figures. The result obtained is then compared with the previous work on which dual solutions exist, thus a stability analysis is performed.

The solution for single, double and triple integrals with variable limits based on linear Legendre multi-wavelets are proposed in Chapter 12. An algorithm with the properties of linear Legendre multi-wavelets is constructed to find the numerical approximation for the integrals. The generalized algorithms for solving the integrals are simple and easily applicable. Some numerical examples for single, double and triple integrals are given to show the efficiency of the method. The approximation of the integrals by using linear Legendre multi-wavelets is compared with the existing methods in order to validate the error estimation.

Chapter 13 revisit the construction of the first lattice-based encryption scheme that was considered practical known as the Goldreich-Goldwasser-Halevi (GGH) cryptosystem. Despite offering better efficiency and practicality compared to number-theoretical schemes, the GGH cryptosystem is considered broken due to the Nguyen's and Lee-Hahn's attacks. Moreover, these attacks are described in detail in order to facilitate the investigation of the weak points of the GGH cryptosystem that being exploited by the said attacks. As a result, several potential strategies to strengthen the GGH cryptosystem are presented.

Chapter 14 presents a multi-step method in backward difference form. The backward difference formulation offers a solution to the tedious calculation of integration

coefficients. Remark that the previous multi-step method using a divided difference formulation for solving higher order ordinary differential equations (ODEs) requires calculating the integration coefficients at every step. Rather than calculating integration coefficients at every step change, a backward difference formulation in this chapter requires calculating integration coefficients only once in the beginning and if required, once more at the end.

Chapter 15 investigates a study of boundary layer flow of water-based nanofluids containing single (SWCNTs) and multi-walled (MWCNTs) carbon nanotubes past a moving plate with the effect of second-order slip flow. After initiating the appropriate similarity variables, the resulting nonlinear ordinary differential equations are obtained. Influences of the selected values of parameters involved in the governing equations such as first and second-order slip parameters, velocity ratio parameter and nanoparticle volume fraction parameter on the velocity, temperature, skin friction coefficient and local Nusselt number are explained graphically. It is revealed that for a certain range of the velocity ratio parameter i.e., the plate moves in the opposite direction, dual solutions exist. The existence of the slip parameter also increases the range of solution and heat transfer rate, whereas the skin friction decreased.

An analysis has been done to examine the boundary layer flow of an electrically conducting nanofluid passing through a horizontal thin needle in Chapter 16. The resulting system of ODE is obtained via similarity transformations. The results for the local Nusselt number, skin friction coefficient, and profiles are graphically portrayed concerning the parameters of interest. The results obtained have shown that the multiple solutions are available in a certain region of the velocity ratio parameter. Stability analysis is applied to verify which of the solutions obtained are stable. It is noticed that the stable solution is represented by the upper branch solution.

The final chapter which is Chapter 17 focuses on the mathematical formulation for the stability analysis of an unsteady three-dimensional boundary layer flow past a permeable stretching/shrinking sheet. Similarity transformation is used to reduce the governing system of nonlinear PDEs into a system of ODEs. Multiple solutions are found for a certain range of the governing parameters. The stability of the solutions obtained is analyzed to determine which solution branch is stable and physically realizable.

Chapter 2

Marangoni-Bénard Convection in an Anisotropic Porous Medium with the Effect of Internal Heating

Nor Halawati Senin[1], Nadia Diana Mohd Rusdi[1], **Nor Fadzillah Mohd Mokhtar**[1,2,*], Mohamad Hasan Abdul Sathar[1,2]

[1] Laboratory of Computational Sciences and Mathematical Physics, Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: nor_fadzillah@upm.edu.my

Abstract

In an anisotropic ferrofluid layer system, a linear stability assessment was performed to study the impact of internal heating on the onset of Marangoni-Bénard convection. The system is heated from below with both the lower and upper limits being deemed completely insulated to the disturbance of temperature. The eigenvalue problem is solved by using regular perturbation technique to obtain the critical Marangoni number and also the critical thermal Rayleigh number. It is noted that the increase of value internal heating, anisotropic permeability and also magnetic number will destabilize the system while the increasing values of Darcy number and also anisotropic thermal diffusivity will help to delay the convection.

Keywords: Anisotropic, Ferrofluid, Marangoni-Bénard, Internal Heating.

2.1 Introduction

Ferrofluid or also known as a fluid that contains a magnetic particle and Kaiser and Miskolczy [1] list and discussed the application of this fluid in their researched. Hennenberg et al. [2] are then discussed the ferrofluid layer system with a deformable surface in the combination between Marangoni and Cowley-Rosensweig. A lot of studied related to the convection ferrofluid with a various effect had been done one of it are from Sheikholeslami and Ganji [3] that studied external magnetic source in ferrofluid.

Yang [4] researched the impact of thickness boundary on the convection of Marangoni-Bénard. Hennenberg et al. [5] had proved the implementation of the Brinkman model in the convection of Marangoni-Bénard. In a recent studied, Mokhtar et al. [6] the impact of the internal heating with the upper boundary are considered to be deformable in a two layer system while Abdullah and Bakhsh [7] added the effect of rotation in a Marangoni-Bénard convection.

In most of a previous research only a considering an isotropic porous medium but recently anisotropic porous medium had been examined. Degan and Vasseurt [8] examined the vertical anisotropic porous medium on the onset of convection. Convection of a ferrofluid layer system in an anisotropic porous medium had been done by Sekar, Vaidyanathan, and Ramanathan [9]. Shivakumara et al. [10] examined the impact of internal heating in two layer system on the onset of Marangoni convection. Recently, Hamid et al. [11] considered on nonlinear temperature profile in an anisotropic porous medium of a binary fluid.

The reaction of internal heating in convection of a deformable surface had been demonstrated by Char and Chiang [12]. Wilson [13] investigated the impact of internal heating in a Marangoni convection while Nanjundappa, Shivakumara, and Arunkumar [14] researched the impact of internal heating in a ferrofluid layer system. The combination of feedback control and internal heating on the onset of double diffusive convection had been done by Khalid et al. [15].

The objective of this research is to initiate Marangoni-Bénard convection in anisotropic porous medium of a ferrofluid layer system with additional internal heating impact. The lower and upper limits are regarded to be rigid-free borders and both limits are regarded to be totally insulated to any disturbance of temperature. Using regular perturbation technique, the eigenvalue problems are solved and we acquired the critical equation of Marangoni and thermal Rayleigh.

2.2 Methodology

We considered a horizontal ferrofluid layer system is heated from below as shown in the Figure 2.1. The lower boundary is set to be rigid while the upper boundary is set to be free. Both of the boundaries are fixed to be constant but the temperature of the lower bound are higher compared to the upper bound.

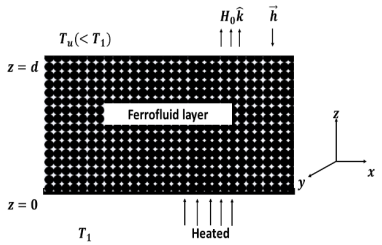

Figure 2.1: Physical configuration of the system.

By referring to Nanjundappa and Vijay Kumar [16], the problem can be written as in the following form after going through the process of non-dimensionalizing and

normal mode

$$\left[\Lambda\left(D^2-a^2\right)^2 - Da^{-1}\left(\frac{1}{\xi}D^2-a^2\right)\right]W+ \tag{2.1}$$
$$a^2 Rm\, F\left(D\phi-\theta\right) - a^2 Rt\,\theta = 0,$$
$$D^2\theta - \eta a^2\theta - F(1-M_2)W = 0, \tag{2.2}$$
$$D^2\phi - a^2 M_3\phi - D\theta = 0, \tag{2.3}$$

with the boundary condition

$$W = D\theta = DW = \phi = 0 \qquad \text{at } z=0, \tag{2.4}$$
$$W = D\theta = D\phi = D^2W + Ma\, a^2\theta = 0 \quad \text{at } z=1, \tag{2.5}$$

where:
$\xi = \frac{k_h}{k_v}$ is an anisotropic permeability,
$D = \frac{d}{dz}$,
$Rm = RtM_1 = \frac{\mu_0 K_1^2 \beta}{(1+\chi)\alpha_t \rho_0 g}$ is the magnetic Rayleigh number,
$F = Ns(1-2z) - 1$ internal heating,
$a^2 = l^2 + m^2$ is the wave number,
$\Lambda = \frac{\widetilde{\mu}_f}{\mu_f}$ is the ratio viscosity,
$Rt = \frac{\alpha_t g \beta d^4}{\nu\kappa A}$ is the thermal Rayleigh number,
$\eta = \frac{\kappa_h}{\kappa_v}$ is an anisotropic effective thermal diffusivity,
$Da^{-1} = \frac{k_h}{d^2}$ is the Darcy number,
$M_2 = \frac{\mu_0 T_0 K_1^2}{1+\chi}$ is the magnetic parameter,
$M_3 = \frac{1+\frac{M_0}{H_0}}{1+\chi}$ is the nonlinearity of the ferrofluid,
$Ma = \frac{\sigma_T \triangle T d}{\mu\kappa}$ is the Marangoni number.

By referring to Finlayson [17], M_2 will not affect the Marangoni-Bénard convection since the value of it will be approximated to zero because the value too small which is 10^{-6}. In order to solve (2.1) till (2.3) with the boundary conditions (2.4) and (2.5), regular perturbation method will be used. The variables are in following the form

$$(W,\theta,\phi) = (W_0,\theta_0,\phi_0) + a^2(W_1,\theta_1,\phi_1) + \cdots, \tag{2.6}$$

By substituting equation (2.6) into (2.1) till (2.5) we will get the zeroth equation as follows

$$\Lambda D^4 W_0 - Da^{-1}\left(\frac{1}{\xi}D^2W_0\right) = 0, \tag{2.7}$$
$$D^2\theta_0 - FW_0 = 0, \tag{2.8}$$
$$D^2\phi_0 - D\theta_0 = 0, \tag{2.9}$$

with the boundary conditions

$$W_0 = DW_0 = \theta_0 = \phi_0 = 0 \text{ at } z=0, \tag{2.10}$$
$$W_0 = D^2W_0 = D\phi_0 = D\theta_0 = 0 \text{ at } z=1. \tag{2.11}$$

The solution to the zeroth order equation (2.7) till (2.9) by using boundary conditions (2.10) and (2.11) are as follow

$$W_0 = 0,$$

$$\theta_0 = 1, \tag{2.12}$$
$$\phi_0 = 0.$$

By substituting (2.12) we will get the first order equations as follow

$$\Lambda D^4 W_1 - Da^{-1}\left(\frac{1}{\xi} D^2 W_1\right) - RmF - Rt = 0, \tag{2.13}$$
$$D^2\theta_1 - \eta - F\ W_1 = 0, \tag{2.14}$$
$$D^2\phi_1 - D\theta_1 = 0, \tag{2.15}$$

with the boundary conditions

$$W_1 = DW_1 = D\theta_1 = \phi_1 = 0 \quad \text{at } z = 0, \tag{2.16}$$
$$W_1 = \phi_1 = D\theta_1 = D^2 W_1 + Ma = 0 \quad \text{at } z = 1. \tag{2.17}$$

The equation (2.13) to (2.17) will be solved by using MAPLE. The equation of Ma_c will be generate in term of $Ns, M_1, Rt, Rm, \eta, \lambda, \xi$ and Da^{-1}.

2.3 Results and Discussion

Internal heating is assessed in an anisotropic porous medium at the onset of the convection of Marangoni-Bénard. The findings are shown graphically in Figure 13.24-2.6 showing the variables relationship with Mac and Rtc. The study shows that M_3 did not have any contribution towards the convection of the system and this result coincide with a previous study from Nanjundappa, Shivakumara, and Arunkumar [14].

Figure 13.24 represent the relation of Ns with different values of η. The Ma_c values drop as the value of Ns increase meanwhile the increment of η lead to the escalation of Ma_c. It shows that the increasing of Ns cause a destabilization to the system which is contradict to the effect of η that help to stabilize the system. It is because heat energy can be supplied efficiently through the porous medium due to the increase of η that cause the increasing of thermal diffusivity. As a consequence, the lower value of Ma_c are required since no need of horizontal temperature difference to support the convection (Shivakumara et al. [10]). While the reason behind the behavior of Ns is that the increasing of the energy supply lead to a destabilization of the system (Khalid et al. [15]).

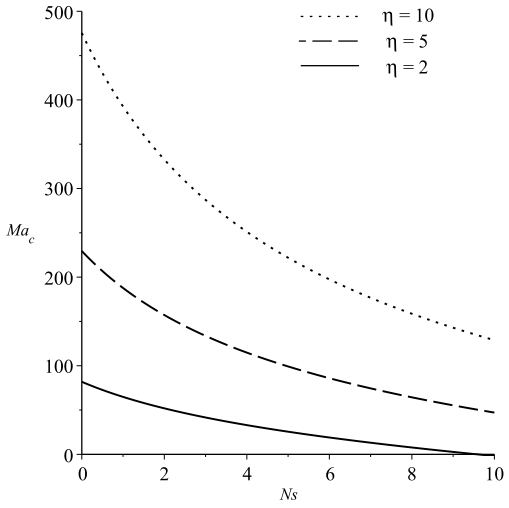

Figure 2.2: Impact of η on Ma_c against Ns.

The effect of Da^{-1} with different value of Ns are demonstrate in Figure 13.25. The graph shows that the increment of the value Da^{-1} lead to the increasing of the Ma_c thus delay the Marangoni-Bénard convection towards the system. The increasing of Ns and decreasing of Da^{-1} are found to help promotes the convection.

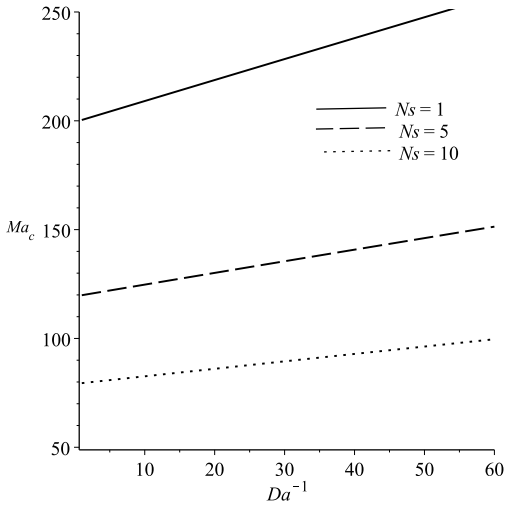

Figure 2.3: Impact of Ns on Ma_c against Da^{-1}.

Figure 13.26 shows the response of ξ on Ma_c. This figure clearly shows that the boost of the ξ values will lessen the value of Ma_c and this indicates that the effect of ξ will destabilize the system. It is observed that this is due to the encouragement of the fluid flow because of the increasing of permeability when ξ increase thus it makes the system destabilize (Shivakumara et al. [10]). From this figure also, the increasing of both ξ and Ns values will hasten the convection.

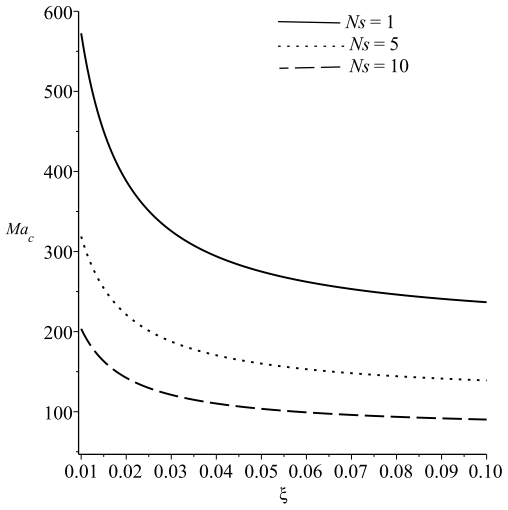

Figure 2.4: Impact of Ns on Ma_c against ξ.

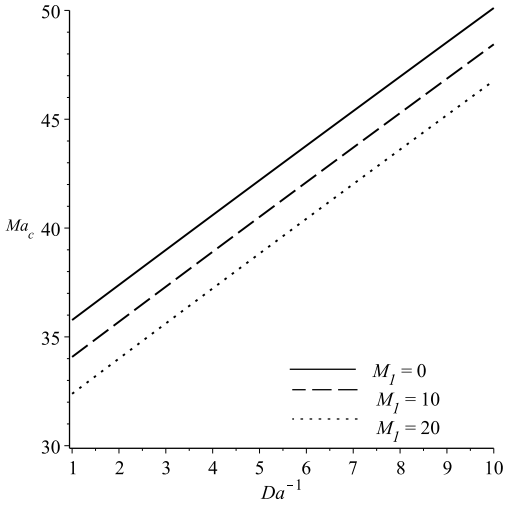

Figure 2.5: Impact of M_1 on Ma_c against Da^{-1}.

Figure 2.5 illustrated the combination effect of Da^{-1} and M_1. The increasing of M_1 values will reduce the values of Ma_c. It happens because the rise of M_1 values will hike the destabilize magnetic force that lead to the destabilization of the system (Nanjundappa, Shivakumara, and Arunkumar [14]).The simultaneous effect of increasing M_1 and decreasing the values of Da^{-1} will destabilize the system.

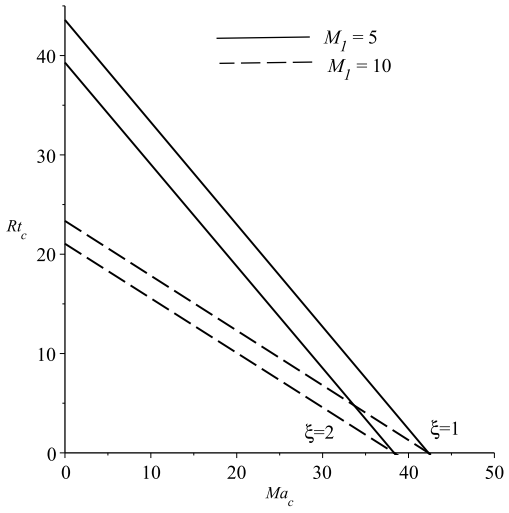

Figure 2.6: Impact of M_1 on Rt_c against Ma_c.

Figure 2.6 display the response of M_1 on Rt_c against Ma_c for different value of ξ. From the figure it can be seen clearly that the increasing of M_1 and Ma_c will compress the values of Rt_c. The values of M_1 will compress to a fixed value of Ma_c which is in this case for value $\xi = 1$ the $Ma_c = 42.3$ while for $\xi = 2$ the $Ma_c = 38.3$. This finding is coinciding with the previous graph which is ξ will enhance the convection.

2.4 Conclusion

A theoretical investigation of Marangoni-Bénard convection in the existence of internal heating of an anisotropic porous medium of a ferrofluid layer system had been done by using regular perturbation method. We can conclude that the increasing of Ns, M_1 and ξ will promotes the Marangoni-Bénard convection while Da^{-1} and η will help to stabilize the system. The combination of decreasing Da^{-1} and increasing of Ns or M_1 will enhance the convection. Besides the increasing of both Ns and ξ also will destabilize the convection.

Acknowledgement

We would like to thank Universiti Putra Malaysia for all the equipment and financial support. The present research was partially supported by the Putra Grant - Putra Graduate Initiative (IPS)-GP-IPS/2018/9642900.

Bibliography

[1] Kaiser, Robert, and Gabor Miskolczy. (1970), *Some Applications of Ferrofluid Magnetic Colloids*, IEEE Transactions on Magnetics 6(3): 694–98.

[2] Hennenberg, M., B. Weyssow, S. Slavtchev, and B. Scheid. (2007), *Coupling between Stationary Marangoni and Cowley-Rosensweig Instabilities in a Deformable Ferrofluid Layer*, Fluid Dynamics and Materials Processing 3(4): 295–302.

[3] Sheikholeslami, M, and D D Ganji. (2018), *Ferrofluid Convective Heat Transfer under the Influence of External Magnetic Source*, Alexandria Engineering Journal 57(1): 49–60.

[4] Yang, H. Q. (1992), *Boundary Effect on the Bénard-Marangoni Instability*, International Journal of Heat and Mass Transfer 35(10): 2413–20.

[5] Hennenberg, M., M. Ziad Saghir, A. Rednikov, and J. C. Legros. (1997), *Porous Media and the Bénard-Marangoni Problem*, Transport in Porous Media 27(3): 327–55.

[6] Mokhtar, N. M., Arifin, N. M., Nazar, R., Ismail, F.,and Suleiman, M. (2011), *Effect of Internal Heat Generation on Marangoni Convection in a Superposed Fluid-Porous Layer with Deformable Free Surface*, International Journal of the Physiacal Sciences 6(23): 5550–63.

[7] Abdullah, Abdullah Ahmad, and Abeer Habeebullah Bakhsh. (2015) *Rayleigh-Benard Instability in a Horizontal Porous Layer Affected by Rotation*, Applied Mathematics 06(14): 2300–2310.

[8] Degan, G, and P Vasseurt. (1995), *Convective Heat Transfer in a Vertical Anisotropic Porous Layer*, International Journal Heat Mass transfer 38(11): 1975–87.

[9] Sekar, R., G. Vaidyanathan, and A. Ramanathan. (1996), *Ferroconvection in an Anisotropic Porous Medium*, International Journal of Engineering Science 34(4): 399–405.

[10] Shivakumara, I. S., S. P. Suma, R. Indira, and Y. H. Gangadharaiah. (2012), *Effect of Internal Heat Generation on the Onset of Marangoni Convection in a Fluid Layer Overlying a Layer of an Anisotropic Porous Medium*, Transport in Porous Media 92(3): 727–43.

[11] Hamid, N. Z. A. H., Mokhtar, N. F. M., Arifin, N. M. and Sathar, M. H. A. (2019), *Effect of Nonlinear Temperature Profile on Thermal Convection in a Binary Fluid Saturated an Anisotropic Porous Medium*, Journal of Advanced Research in Fluid Mechanics and Thermal Sciences 1: 43–58.

[12] Char, M. I., and Ko Ta Chiang. (1994), *Stability Analysis of Benard-Marangoni Convection in Fluids with Internal Heat Generation*, Journal of Physics D: Applied Physics 27(4): 748–55.

[13] Wilson, S. K. (1997), *Effect of Uniform Internal Heat Generation on the Onset of Steady Marangoni Convection in a Horizontal Layer of Fluid*, Acta Mechanica 124(1–4): 63–78.

[14] Nanjundappa, C. E., I. S. Shivakumara, and R. Arunkumar. 2011. "Onset of Benard-Marangoni Ferroconvection with Internal Heat Generation." Microgravity Science and Technology 23(1): 29–39.

[15] Khalid, I. K., Mokhtar, N. F. M., Hashim, I., Ibrahim, Z. B., and Gani,S.S.A. (2017), *Effect of Internal Heat Source on the Onset of Convection in a Nanofluid Layer with Feedback Control Strategy*, 116(January): 1827–32.

[16] Nanjundappa, C.E., and B. Vijay Kumar. (2013), *Penetrative Ferroconvection Via Internal Heating In A Ferrofluid Anisotropic Porous Medium*, 49(3): 441–47.

[17] Finlayson, B. A. (1970), *Convective Instability of Ferromagnetic Fluids*, Journal of Fluid Mechanics 40(4): 753–67.

Chapter 3

Effect of Internal Heating and Coriolis Force on Couple Stress Fluid in an Anisotropic Porous Medium

Nadia Diana Mohd Rusdi[1], **Nor Fadzillah Mohd Mokhtar**[1,2,*], Norazak Senu[1,2], Siti Suzilliana Putri Mohamed Isa[1,2]

[1] Laboratory of Computational Sciences and Mathematical Physics, Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: nor_fadzillah@upm.edu.my

Abstract

Linear stability analysis is used to study the effect of internal heating and Coriolis force on couple stress fluid in an anisotropic porous medium, which is heated from below. The Boussinesq approximation and momentum equation also used for the density variation in the porous medium. The eigenvalue problems of the perturbed state are obtained by using Galerkin method from a normal mode analysis. The results show the effect of internal heating and mechanical anisotropic parameter destablizes the system while increasing the thermal anisotropic parameter, effect of coriolis force and couple stress fluid helps to stabilize the system.

Keywords: Anisotropic Porous Medium, Internal Heating, Couple Stress Fluid, Coriolis Force.

3.1 Introduction

Internal heating is one of important effects which has been studied by many researchers in porous medium problem. It also has attracted many researchers widely in the field of engineering and its application. For example, decay of the radioactive, combustion of the fossil fuels studies, gas and nuclear fuel. Couple stress fluid has been considered as an isolation of the fluid in the kinematic level that leads to fully determined by the velocity field by Stokes [1] . An extensively written review of the literature about the phenomenon and the convection of porous medium can be discovered which are from Ingham and Pop [2] , Nield and Bejan [3] and Vadász [4].

From the previous studies, a few researchers considered double diffusive to be investigated with internal heating. The internal heating is studied by Hill [5] with the linear stability and nonlinear stability together with the diffusive concentration in the porous medium while Srivastava et al, [6] added anisotropic in the porous medium and couple stress fluid in their research. Bhadauria [7] has considered internal heating which has been salted and heated from below in porous medium related to anisotropy with double diffusive convection. He used linear analysis and nonlinear analysis based on truncation Fourier series method and also been studied by Hill [5] .

Vadász [8] studied the linear theory and for nonlinear theory with the effect Coriolis related to gravity-driven convection. Malashetty and Swamy [9] also has considered rotation effect by using a linear and nonlinear theories on the layer with porous and also anisotropy effect. Vanishree and Siddheshwar [10] studied on temperature-dependent viscosity including mono-diffusive convection with anisotropic rotating porous layer with linear stability analysis. From Shivakumara et al, [11], they studied the couple stress rotating fluid with rigid saturared with layer of the porous and been performed by stability analysis has been studied.

Saturated couple stress fluid with porous medium(anisotropy) on onset with convection in different types and values of temperature gradient has been analyzed by Shivakumara [12]. Next, Malashetty and Kollur [13] considered double diffusive convection with the influence of in a anisotropic porous and couple stress in the fluid is studied analytically. Kulkarni [14] has investigated the solid surface and fluid surface with stability of couple stress fluid that being saturated with rotation of porous governed by Darcy-Brinkman model.

In addition, anisotopic porous medium has recently been concerned by the researchers. Govender [15] has investigated the used of Darcy model in natural convection of the stability convection in the anisotropy effect with rotating porous media. By using Galerkin method, Parthiban and Patil [16] concerned about the internal of heat source with convection in saturated horizontal anisotropy of the porous medium. While, Raghunatha et al, [17] considered perturbation method in investigating Oldroyd-B layer with fluid saturated with anisotropy Darcy porous medium in nonlinear stability thermal convection.

The purpose of our research is to carry out an investigation on the rotation and the internal heating effects on couple stress fluid horizontal anisotropic porous medium with respect to upper free conducting boundary conditions. Galerkin method has been programmed and eigenvalue problem will be solved.

3.2 Mathematical Formulation

The couple stress in the fluid with an infinite horizontal porous medium with the gravity is vertically downward, $\vec{g} = (0, 0, -g)$ has been considered. The depth, d is vertically bounded by the planes in between $z = 0$ until $z = d$, been heated from the bottom subject to constantly adverse temperature difference, $\triangle T = T_s - T_v$, where T_s is the fixed value of lower temperature and T_v is fixed value for upper temperature respectively. In addition, the system is rotated along the vertical axis roundly with a consistent $\mathbf{\Omega} = (0, 0, \Omega)$ which is angular velocity with heat source. The porous medium in the horizontal direction is assumed to be anisotropic on both thermal property and mechanical property. Moreover, the effect of density

variation is considered to go along with the Boussinesq approximation. With all these assumptions,

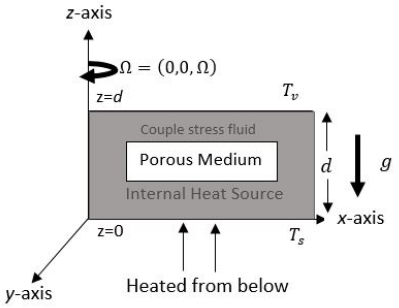

Figure 3.1: Schematic Diagram of the Problem.

the governing of the equations are

$$\nabla \cdot \vec{w} = 0, \tag{3.1}$$

$$\frac{\rho_o}{\phi}\frac{\partial \vec{w}}{\partial t} + \frac{\mu}{\vec{K}*} \cdot \vec{w} + 2\left(\vec{w} \times \Omega\right) + \bigtriangledown p^* - \rho^* g + \left(\mu - \mu_c \bigtriangledown^2\right)\vec{w} = 0, \tag{3.2}$$

$$\gamma\frac{\partial T}{\partial t} - \kappa_{Tz}\left(\nabla^2 T\right) + \left(\vec{w} \cdot \nabla\right)T - Q\left(T - T_o\right) = 0, \tag{3.3}$$

$$\rho^* = \rho_0 - \rho_0\left(T - T_0\right)\alpha. \tag{3.4}$$

The thermal boundary conditions is given as

$$T_0 = T - \triangle T,\ z = 0, \tag{3.5}$$

$$T_0 = T,\ z = d, \tag{3.6}$$

where $\vec{w} = (u^*, v^*, w^*)$ is the velocity vector while p^* and ϕ are the pressure and the porosity, $\vec{K}* = K_x\left(\vec{i}\vec{i} + \vec{j}\vec{j}\right) + K_z\left(\vec{k}\vec{k}\right)$ is recognized as permeability tensor, μ is the dynamic viscosity, μ_c is known as the viscosity couple stress of the fluid, Q is the heat source, γ is the ratio of heat capacity, ρ^* is the density of the porous which is depend linearly on the temperature, T_0 are the temperature, κ_{Tz} is the vertical thermal diffusivity, ρ_0 and α are called reference density and also thermal expansion coefficient respectively.

3.2.1 Basic State

Defined

$$p^* = p_b\left(z\right), \quad \vec{w}_b = (0,0,0), \quad T = T_b\left(z\right), \quad \rho^* = \rho_b\left(z\right). \tag{3.7}$$

Eq. (7) is the basic state where b stand for the basic.

Substitute Equations. (7) into Eqs (1)–(4) which also can be satisfied by the equations given

$$\frac{\mathrm{d}p_b}{\mathrm{d}z} = -\rho^* g,\ \frac{\mathrm{d}^2 T_b}{\mathrm{d}z^2} = 0,\ \rho_b = \rho^*\left[1 - \alpha\left(T_b - T_0\right)\right], \tag{3.8}$$

$$\kappa_T\frac{d^2(T_b - T_0)}{dz^2} + Q\left(T_b - T_0\right) = 0. \tag{3.9}$$

The conduction state temperature Eqs (9) subject to the thermal boundary conditions Eq. (5) and (6) are given by

$$T_b = T_0 + \Delta T \frac{sin\sqrt{\frac{Qd^2}{\kappa_{Tz}}}\left(1-\frac{z}{d}\right)}{sin\sqrt{\frac{Qd^2}{\kappa_{Tz}}}}. \tag{3.10}$$

3.2.2 Perturbed State

The infinitesimal perturbation for the basic state applied given as

$$\begin{aligned} w' = \vec{w}_b - \vec{w}, \;\; p' = \vec{p}_b - \vec{p^*}, \\ T' = \vec{T}_b - \vec{T}, \quad \rho' = \vec{\rho}_b - \vec{\rho^*}, \end{aligned} \tag{3.11}$$

where the primes representing the perturbation quantities. By using the infinitesimal perturbation equation in Eq. (11) to Eqs. (1)-(6), the pressure term will be eliminated by taking curl formula twice on the momentum equation of the porous medium. The resulting equations will be nondimensionalized by transforming the following transformation

$$\begin{aligned} (x', y', z') = (x^* d^*, y^* d^*, z^* d^*), \;\; t = \frac{\gamma \mathrm{d}^2 t^*}{\kappa_{Tz}}, \;\; T' = (\Delta T)\, T^*, \\ (u', v', w') = \left(\frac{\kappa_{Tz} u^*}{\mathrm{d}^*}, \frac{\kappa_{Tz} v^*}{\mathrm{d}^*}, \frac{\kappa_{Tz} w^*}{\mathrm{d}^*}\right), \end{aligned} \tag{3.12}$$

then the equation obtained are

$$\left[\frac{\sigma Da}{\gamma Pr}\frac{\partial}{\partial t}\bigtriangledown_h^2 + \left(\bigtriangledown_h^2 + \frac{1}{\xi}\frac{\partial^2}{\partial z^{*2}}\right)\left(1 - C\bigtriangledown_h^2\right)\right] w^* - Ra_T \bigtriangledown_h^2 T + \sqrt{Ta}\frac{\partial \zeta}{\partial z^*} = 0, \tag{3.13}$$

$$\left[\gamma\frac{\partial}{\partial t^*} - \eta\nabla_h^2 - \frac{\partial^2}{\partial z^{*2}} + \vec{u}^* \cdot \nabla\right] T^* - \left[Q\left((1-2z)-1\right)\right] w^* = 0, \tag{3.14}$$

$$\frac{\zeta^*}{\xi} + \zeta^* \varepsilon_n \frac{\partial}{\partial t^*} - \sqrt{Ta}\frac{\partial w^*}{\partial z^*} = 0, \tag{3.15}$$

where $Da = \frac{\mathrm{K}_z}{\mathrm{d}^2}$ known as the Darcy number, $Pr = \frac{\mu}{\rho_0 \kappa_{Tz}}$ known as the Prandtl number, $\nu = \frac{\mu}{p_0}$ is the kinematic viscosity, $Ra = \frac{\alpha g \Delta T d K_z}{\nu \kappa_{Tz}}$ is the thermal Rayleigh number, $Ta = \frac{2\Omega K_z}{\nu}$ is the Taylor number, ζ is the vorticity, $C = \frac{\mu_c}{\mu d^2}$ is couple stress parameter, Q is the heat source which defined as $Q = \frac{qd^2}{2\kappa\Delta T}$, $\xi = \frac{K_x}{K_z}$ and $\eta = \frac{\kappa_{Tx}}{\kappa_{Tz}}$ are the mechanical and thermal anisotropy parameter respectively and $\epsilon_n = \frac{\phi}{\gamma}$ is the normalized porosity. The wave number defined as a_x, a_y in $x-$direction and $y-$direction while σ represents the growth rate.

3.2.3 Linear Stability Analysis

Applied the nonlinear stability analysis on Eqs. (13)-(15) when nonlinear term is eliminated as shown and by using normal mode expansion given below

$$(w, T, \zeta) = (W(z), \Theta(z), \zeta(z))\, exp\left[i\left(a_k + a_l\right) + \sigma t\right], \tag{3.16}$$

the equations become

$$\left[\left(D^2 - a^2\right)\frac{\sigma Da}{Pr} + \left(1 - CD^2 - Ca^2\right)\left(\frac{D^2}{\xi} - a^2\right)\right]$$

$$W + \sqrt{Ta}D\zeta + a^2 Ra\Theta = 0, \tag{3.17}$$

$$\left(D^2 - \sigma - \eta a^2\right)\Theta + \left(1 - Q\left(1 - 2z\right)\right)W = 0, \tag{3.18}$$

$$\tfrac{\sigma}{Pr}\zeta - \left(\tfrac{1}{\xi} + D^2 - a^2\right)\zeta - \sqrt{Ta}DW = 0, \tag{3.19}$$

where $D = \frac{d}{dz}$ and $a^2 = a_k^2 + a_l^2$.

The appropriate boundary conditions that are given by

$$\begin{aligned} W = \Theta = D^2 W = \zeta = 0 \text{ at } z = 0, \\ W = \Theta = DW = \zeta = 0 \text{ at } z = 1. \end{aligned} \tag{3.20}$$

3.2.4 Method of Solution

Equations (17)-(19) with the boundary conditions for upper free boundries along with lower rigid boundaries in Eq. (20) to form a linear eigenvalue problem from the system. By using Galerkin higher series weighted residuals method, the eigenvalue problem of convection in the porous medium is solved numerically. Furthermore, the variables of W, θ and ζ are the basis function series and written as follows

$$W = \sum_{i=1}^{l} A_i W_i(z),\ \theta = \sum_{i=1}^{l} B_i \theta_i(z),\ W = \sum_{i=1}^{l} P_i \zeta_i(z), \tag{3.21}$$

where A_i, C_i and P_i are constants and $W_j(z)$, $\theta_j(z)$ and $\zeta_j(z)$ are the trial functions which satisfies the boundary conditions. Next, the resulting equation is multiplied with $W_j(z)$, $\theta_j(z)$ and $\zeta_j(z)$ respectively. By using integration by parts with respect to l from 0 to 1, the boundary conditions in Eqs.(20) will lead to the linear homogenous algebraic equations as follows

$$\begin{aligned} C_{ji}A_i + G_{ji}B_i + H_{ji}P_i = 0, \\ E_{ji}A_i + F_{ji}B_i + 0 = 0, \\ M_{ji}A_i + 0 + N_{ji}P_i = 0. \end{aligned} \tag{3.22}$$

The coefficients $C_{ji} - N_{ji}$ will involve the inner product of the functions and given by $C_{ji} = \left\langle \frac{1}{\xi}\left(D^2 W_j D^2 W_i - a^2 W_j a^2 W_i\right)\left(1 - C\left(D^2 - a^2\right)\right)\right\rangle$, $G_{ji} = \left\langle a^2 Ra W_j \theta_i \right\rangle$, $H_{ji} = \left\langle \sqrt{Ta} D W_j \zeta_i \right\rangle$, $E_{ji} = \langle 1 - Q(1-2z)\theta_j W_i \rangle$, $F_{ji} = \left\langle D^2\theta_j\theta_i - \eta a^2 \theta_j \theta_i \right\rangle$, $M_{ji} = \left\langle -\sqrt{Ta} D W_j \zeta_i \right\rangle$ and
$N_{ji} = \left\langle D^2\zeta_j\zeta_i - a^2\zeta_j\zeta_i + \frac{1}{\xi}\zeta_j\zeta_i \right\rangle$.

For $\langle f_1 f_2 \rangle = \int_0^1 f_1 f_2 dz$ in inner product is defined. When non-trivial solution occur, the system will be

$$\begin{vmatrix} C_{ji} & G_{ji} & H_{ji} \\ E_{ji} & F_{ji} & 0 \\ M_{ji} & 0 & N_{ji} \end{vmatrix} = 0, \tag{3.23}$$

The eigenvalue will be extracted from the Eqs. (23). From this, the trial function has been chosen as

$$\begin{aligned} W_i &= (2z^4 - 5z^3 + 3z^2)T_{i-1}^{**}, \\ \theta_i &= (z - z^2)T_{i-1}^{**}, \\ \zeta_i &= (z - z^2)T_{i-1}^{**}. \end{aligned} \tag{3.24}$$

where T_{i-1}^{**} is known as the Chebyhev polynomial. The inner products will be expand by the determinant of the matrix in (23) to obtain Rayleigh number, Ra as an eigenvalue of the functions and wavenumber, a with the different values of parameters. The results of the covergence by using 4th term of the Galerkin expansion is achieved. The eigenvalue is solved by using MAPLE software.

3.3 Results and Discussion

The coriolis force effect together with the effect of internal heating on couple stress fluid in an anisotropic porous medium has been analysed to examine the upper and lower free conduction plates. Linear stability analysis has been used in this research. The eigenvalue results are obtained from numerical solutions of the ordinary differential equations (ODE) by using Galerkin method respect to boundary conditions. Various parameters included in the natural stabilize curve which are the Taylor number, thermal anisotropic, mechanical anisotropic, Rayleigh number, internal heat source parameter and couple stress parameter. Prandtl number are fixed to $Pr = 1$ for the system excluding the varying one. All the results are obtained to show the various parameters reacts that can be observed on the Rayleigh number, Ra together with the wave number, a in Figures 2 until 6, respectively.

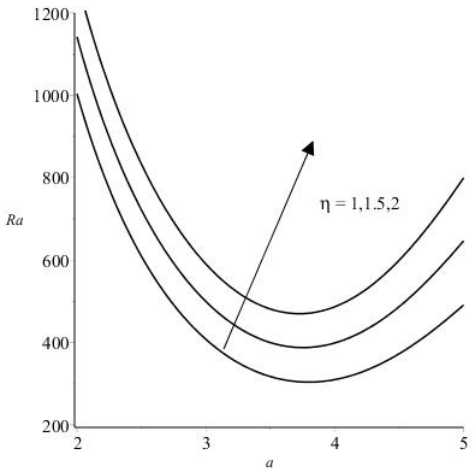

Figure 3.2: Ra against a, various values of η.

First, Figure 2 shows the various values of thermal anisotropic parameter, η from the graph of Rayleigh number, Ra versus wave number, a with fixed values $\xi = 1, C = 2, Q = 2, Ta = 100$. The value of thermal anisotropic parameter, η increases when the value of Ra increases, respectively. Hence, increasing the value of η will stabilize the system. Next, Figure 3 represents the graph of Ra with increasing effect of mechanical anisotropic parameter, ξ, the value of $\eta = 1, C = 2, Q = 2, Ta = 100$ are fixed. It has been shown that, with the increasing value of ξ,

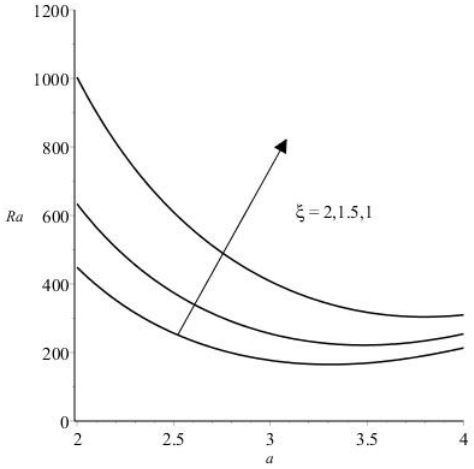

Figure 3.3: Ra against a, various values of ξ.

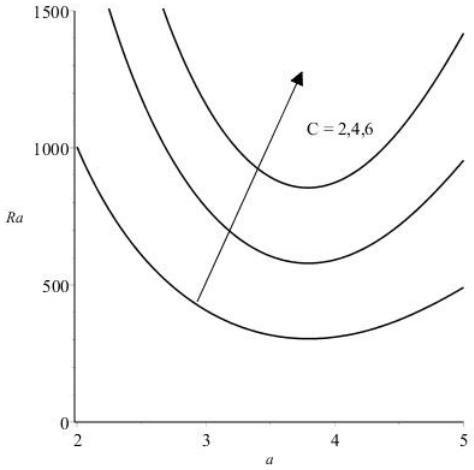

Figure 3.4: Ra against a, various values of C.

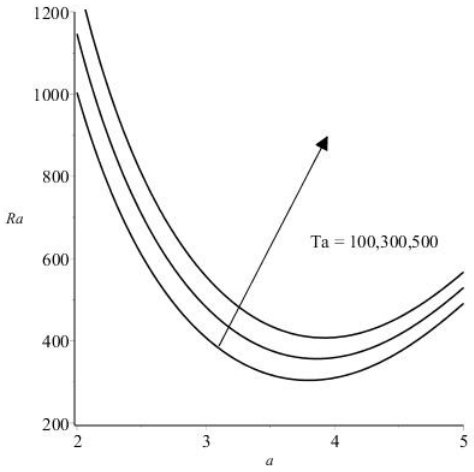

Figure 3.5: Ra against a, various values of Ta.

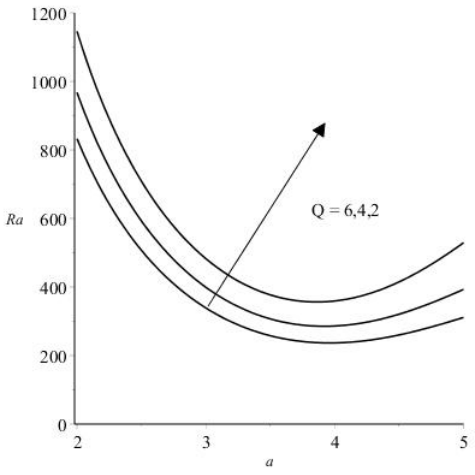

Figure 3.6: Ra versus a, various values of Q.

the Ra decreases. The increase in ξ will increase the porous medium and the steady free convection is occurred. Thus, the value of ξ will destablize the system.

Figure 4 displays the couple stress parameter, C towards Ra and the fixed values are $\xi = 1, \eta = 1, Q = 2, Ta = 100$. The variation of couple stress parameter increase when Ra increases. Based on the graph, the influence in increasing the couple stress parameter of the fluid will result in the delay of the onset of the convection. Besides, Figure 5 also deals with the various values of Taylor numbers, Ta which are $100, 300$ and 500 with respect to fix values of $\xi = 1, \eta = 1, Q = 2$ when $C = 1$ and $C = 1.5$. The effect of Coriolis force acting on the system will be higher than the Figures 2-4 because of the increase in the rotation of angular velocity, Ω. Hence, the influence of Coriolis force will also delay the system of the onset of steady of the convection. Next, the Rayleigh number, Ra versus wave number a is depicted in the Figure 6 with effect from internal heating, Q at fixed value of $\xi = 1, \eta = 1, C = 2, Ta = 100$. It is found that the increasing Q will decrease the value of Ra. The fact that increasing Q is to advance the onset of convection in the system according to Bhadauria et al, [18]. As a result, internal heating will destablize the system.

3.4 Conclusion

Numerically study has been carried on the couple stress fluid with the stationary thermal convection in horizontal state of anisotropic porous medium been heated along with the effect of Coriolis force and internal heating from below. In addition, the eigenvalue problem has been solved by linear stability analysis using Galerkin method which been programmed using MAPLE software. The values of Ta discovered to increase the number of Ra while Ra decreases when increasing heat source. Thus, effect of internal heating are found to advance the onset of the convection. Therefore, C will delay the onset of the convective. From the result obtained, the mechanical anisotropic parameter, ξ found destabilizing the system while the thermal anisotropic parameter, η stabilizing the system.

Acknowledgement

Thank you Putra Grant - Putra Graduate Initiative (IPS) -GP-IPS/2018/9642900 from Universiti Putra Malaysia for the support.

Bibliography

[1] Stokes, V. K. (1984) 'Couple Stresses in Fluids', in Theories of Fluids with Microstructure. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 34–80.

[2] Ingham, D. B., Pop, I.(1998). Transport phenomena in porous media. Elsevier.

[3] Nield, D.A. and Bejan, A., 2006. Convection in porous media (Vol. 3). New York: springer.

[4] Vadász, P. ed., 2008. Emerging topics in heat and mass transfer in porous media: from bioengineering and microelectronics to nanotechnology (Vol. 22). Springer Science and Business Media.

[5] Hill, A. (2005) 'Double-diffusive convection in a porous medium with a concentration based internal heat source', Proc. R. Soc. A, 461, pp. 561–574.

[6] Srivastava, A., Bhadauria, B. S. and Hashim, I. (2014) 'Effect of Internal Heating on Double Diffusive Convection in a Couple Stress Fluid Saturated Anisotropic Porous Medium', Advances in Materials Science and Applications, 3(1), pp. 24–45.

[7] Bhadauria, B. S. (2012) 'Double-Diffusive Convection in a Saturated Anisotropic Porous Layer with Internal Heat Source', Transp Porous Med, 92, pp. 299– 320.

[8] VADASZ, P. (1998) 'Coriolis effect on gravity-driven convection in a rotating porous layer heated from below', Journal of Fluid Mechanics, 376, pp. 351–375.

[9] Malashetty, M. S. and Swamy, M. (2007) 'The effect of rotation on the onset of convection in a horizontal anisotropic porous layer', International Journal of Thermal Sciences. Elsevier Masson, 46(10).

[10] Vanishree, R. K. and Siddheshwar, P. G. (2010) 'Effect of Rotation on Thermal Convection in an Anisotropic Porous Medium with Temperature-dependent Viscosity', Transport in Porous Media. Springer Netherlands, 81(1), pp. 73–87.

[11] Shivakumara, I.S., Sureshkumar, S. and Devaraju, N. (2011) 'Coriolis effect on thermal convection in a couple-stress fluid-saturated rotating rigid porous layer', Archive of Applied Mechanics, (81), pp. 513–530.

[12] Shivakumara, I. S. (2010) 'Onset of convection in a couple-stress fluid-saturated porous medium: effects of non-uniform temperature gradients', Archive of Applied Mechanics. Springer-Verlag, 80(8), pp. 949–957.

[13] Malashetty, M. S. and Kollur, P. (2011) 'The Onset of Double Diffusive Convection in a Couple Stress Fluid Saturated Anisotropic Porous Layer', Transport in Porous Media. Springer Netherlands, 86(2), pp. 435–459.

[14] Kulkarni, S. (2013) 'Darcy-Brinkman Convection In A Couple-Stress Fluid Saturated Rotating Porous Layer Using Thermal Non-Equilibrium Model', Journal of Global Research in Mathematical Archives(JGRMA), 1(8), pp. 16–33.

[15] Govender, S. (2006) 'On the Effect of Anisotropy on the Stability of Convection in Rotating Porous Media'.

[16] Parthiban, C. and Patil, P. R. (1997) 'Thermal instability in an anisotropic porous medium with internal heat source and inclined temperature gradient', International Communications in Heat and Mass Transfer. Pergamon, 24(7), pp. 1049–1058.

[17] Raghunatha, K. R., Shivakumara, I. S. and Sowbhagya (2018) 'Stability of buoyancy-driven convection in an Oldroyd-B fluid-saturated anisotropic porous layer', Applied Mathematics and Mechanics. Shanghai University, 39(5), pp. 653–666.

[18] Bhadauria, B. S. et al. (2011) 'Natural convection in a rotating anisotropic porous layer with internal heat generation', Transp Porous Med, 90, pp. 687–705.

Chapter 4

A Survey of Partial Key Exposure Attacks on RSA Cryptosystem

Amir Hamzah Abd Ghafar[1], **Muhammad Rezal Kamel Ariffin**[2,*], Mohamat Aidil Mohamat Johari[2], Muhammad Asyraf Asbullah[3]

[1] Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: rezal@upm.edu.my

Abstract

In today's digital world, RSA cryptosystem is regarded as the most widely deployed public-key cryptosystem on digital machines that compute cryptographic processes. It secures the sensitive data that are either transmitted via internet or at rest in the computing machines. It utilizes integer factoring problem which is essentially one of the unsolved number theoretic problem. Due to its vital functionality, RSA is confronted by cryptanalysis or 'attacks' to which define a higher benchmark of its security level. In this paper, we survey the established partial key exposure attacks on RSA. The attacks assume that an adversary employs an incomplete arrangements of bits of the RSA private keys. The methods used in the attacks manipulate mathematical structures of the keys.

Keywords: RSA cryptosystem, partial key attack, Coppersmith's method.

4.1 Introduction

Public-key cryptography gives a concept of a padlock which can be opened and locked by two different keys. It is an important solution of the key distribution problem that surrounds a digital communication system. It also ensures the privacy of the data in the system remains confidential. One of the earliest public-key encryption scheme is RSA cryptosystem which was introduced by Rivest, Shamir and Adleman in 1977 15. RSA utilizes a hard mathematical problem called integer factorization problem (IFP). It provides a notion that the processes of finding the prime factors of a very large integer as used in the RSA is an infeasible task for

a current computing machine. This notion is used as one of the security elements that safeguard the private keys of RSA. However many attacks have been introduced over the years to reduce the factorization computation in the RSA cryptosystem to a polynomial time computation which is a feasible task to be executed by a computing machine. One of the established attacks is known as the partial key exposure attacks. The attacks assume that an adversary have the partial information regarding some of the RSA parameters. This partial information includes some arrangements of the most significant bits (MSBs) or the least significant bits (LSBs) of the RSA private keys. The assumption is not misguided as there are real-world methods to collect this information of the RSA private keys. One of the practical method to do this is via a side-channel attack that can collect physical information leaked out of electronic devices. This includes the computational power and time of certain RSA computations, especially the RSA decryption processes in a digital device 13. However, the mathematical impetus of the partial key exposure attacks is mainly due to a method which is known as Coppersmith's method. The method is basically tries to find the small solutions of the polynomials modulo certain RSA parameter 4.

This paper presents a survey on the partial key exposure attacks which are categorized with respect to the type of exposure on the RSA parameters. The first category compiles the attacks where the adversary has MSBs or LSBs of the RSA primes. The second category focuses on the attacks where MSBs of the RSA private exponent are exposed and the last category considers attacks where LSBs of the RSA private exponent are exposed.

4.1.1 Overview of This Paper

In Section 4.2, we show the working algorithms of the RSA cryptosystem. To execute the partial key exposure attacks on the RSA cryptosystem, we must be familiar with the concept of lattice and the overview of a helpful method known as Coppersmith's method. All these are explained in Section 4.3. The partial key exposure attacks are categorized into the types of exposure on the RSA parameters. The first category is detailed in Section 4.4. The attacks of the second category are presented in Section 4.5. The third category of the partial key exposure attacks is shown in Section 4.6. Then, the paper is concluded in Section 4.7.

4.2 RSA and Cryptosystem

To begin using RSA cryptosystem, a security parameter, $\mathfrak{n}$ has to be chosen first. The parameter indicates the level of security of RSA intended for its users. The current recommendation value for $\mathfrak{n}$ is 2048 7. Using the value of $\mathfrak{n}$ as its input, RSA key generation algorithm selects randomly two different primes of n-bits size named, p and q to compute RSA modulus, N where $N = pq$. Then, the Euler's phi function of N is computed. Particularly, $\phi(N) = (p-1)(q-1)$. A parameter, e then is chosen where $e < \phi(N)$ before its corresponding d is obtained such that

$$ed \equiv 1 \pmod{\phi(N)} \quad \text{or} \quad ed - k\phi(N) = 1 \tag{4.1}$$

for some integers k. Equation (4.1) is commonly called as RSA key equation. By establishing all of the values, the algorithm outputs (N, e) as RSA public keys and key tuple $(p, q, \phi(N), d)$ as RSA private keys. The hardness of IFP embedded in

RSA is shown in the structure of N which cannot be factored easily if p and q are very large primes. We present RSA key generation algorithm as follows.

Algorithm 4.2.1 RSA Key Generation Algorithm 15

Input: Security parameter, $\mathfrak{n}$
Output: RSA public keys (N, e), and RSA private keys $(p, q, \phi(N), d)$
1: Generate randomly two distinct of n-bits primes p and q where $p < q < 2p$.
2: Compute $N = pq$.
3: Compute $\phi(N) = (p-1)(q-1)$
4: Choose e such that $e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$
5: Compute d such that $ed \equiv 1 \pmod{\phi(N)}$
6: Output (N, e) as RSA public keys and $(p, q, \phi(N), d)$ as RSA private keys.

The public key pair (N, e) can be obtained by anyone who intends to communicate securely with the owner of the RSA private keys. To encrypt the message, RSA encryption algorithm uses the public keys to transform it into an unreadable text called ciphertext, c using the equation

$$m^e \equiv c \pmod{N} \tag{4.2}$$

and send c via any communication line whether it is secure or not. The exponentiation calculation in (4.2) makes e can also be called as **RSA public exponent**. The encryption is shown in the following algorithm:

Algorithm 4.2.2 RSA Encryption Algorithm

Input: The plaintext m and the public key (N, e)
Output: A ciphertext c
1: Choose integer $0 < m < N$ such that $\gcd(m, N) = 1$
2: Compute $c \equiv m^e \pmod{N}$.
3: Output the ciphertext c

The owner of the RSA private keys then decrypts the ciphertext using RSA decryption algorithm which utilizes RSA private keys in the equation

$$c^d \equiv m \pmod{N} \tag{4.3}$$

The exponentiation calculation in (4.3) makes d can also be called as **RSA private exponent**. The decryption is shown entirely in the following algorithm:

Algorithm 4.2.3 RSA Decryption Algorithm

Input: A ciphertext c and the private key (N, d)
Output: The plaintext m
1: Compute $m \equiv c^d \pmod{N}$
2: Output the plaintext m

RSA utilizes a theorem from Euler to ensure the plaintext, m that is encrypted in (4.2) can be transformed back to its original form. The theorem, which can be read in 9 states that suppose N and a are coprime positive integers, then $a^{\phi(N)} \equiv 1 \pmod{N}$ where $\phi(N)$ is the Euler's totient function of N. The result from this theorem helps to prove the correctness of (4.3) as shown below.

Theorem 4.2.1 (RSA's Proof of Correctness)**.** *Let $N = pq$ be an RSA modulus and $\phi(N) = (p-1)(q-1)$. Suppose $ed \equiv 1 \pmod{\phi(N)}$. For any $0 < m < N$ with $\gcd(m, N) = 1$, if $m^e \equiv c \pmod{N}$ then $c^d \equiv m \pmod{N}$.*

Proof. Since $ed = 1 + k\phi(N)$ for some integers k then

$$c^d \equiv (m^e)^d \equiv m^{1+k\phi(N)} \equiv m \cdot m^{k\phi(N)} \pmod{N} \tag{4.4}$$

From Euler's Theorem, since $\gcd(m, N) = 1$ we know that $m^{k\phi(N)} \equiv 1^k \equiv 1 \pmod{N}$. Hence (4.4) can become

$$m \cdot m^{k\phi(N)} \equiv m \cdot 1 \equiv m \pmod{N}.$$

This terminates the proof. □

4.3 Lattices and Coppersmith's Method

To understand the method used in most of partial key exposure attacks on RSA, we need to be familiar with the concept of lattice which are used in the significant portions of the attack. The method tries to find the small solutions to the polynomial equations of modulo N or divisor of N. The method was proposed by 4 and is known as Coppersmith's method. But first, we introduce the definition of lattice and some of its useful properties used in the method.

Definition 4.3.1. Let $\mathbb{R}^n$ be n-dimensional real vector space. Suppose $b_1, \ldots, b_d$ are r linearly independent vectors for $\mathbb{R}^n$ with $r \leq n$. Then lattice that spans $b_1, \ldots, b_r$ is defined as the set all integer linear combinations of the vectors $b_1, \ldots, b_r$. Particularly,

$$\mathcal{L} = \left\{ \sum_{i=1}^{r} x_i b_i | x_i \in \mathbb{Z}. \right\}$$

Lattice $\mathcal{L}$ has several properties as follows:

a. The basis of $\mathcal{L}$ is given as $(b_1, \ldots, b_n)$ with dimension n;

b. The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \sqrt{\det U^T U}$ where U is the matrix of the u_i's in the canonical basis of $\mathbb{R}^n$; and

c. Euclidean norm of a vector $b \in \mathcal{L}$ is defined as $\|b\|$.

4.3.1 LLL Algorithm

The aim of the algorithm is to find the approximation of the 'short' vector which has small integers in its basis. The algorithm has many applications including in finding simultaneous approximations in rational form to real numbers and factoring polynomials with rational coefficients. It is an important tool used in Coppersmith's method. We show the useful properties of the LLL algorithm in the next theorem.

Theorem 4.3.2 (LLL algorithm)**.** *Let $\mathcal{L}$ has dimension of n. Given LLL reduced basis $\{b_1^*, b_2^*, \ldots, b_n^*\} \in \mathcal{L}$, its properties are including but not limited to:*

$$\prod_{i=1}^{n} \|b_i\| \leq 2^{\frac{n(n-1)}{4}} \det(\mathcal{L})$$

and

$$\|b_1\| \leq 2^{\frac{n-1}{4}} |\det(\mathcal{L})|^{1/n}$$

for all $1 \leq i \leq n$.

Proof. See Theorem 6.66 in 11. □

In the following theorem, we show that the running time of LLL algorithm is in the polynomial time.

Theorem 4.3.3 (Complexity of LLL algorithm)**.** *Let* $\mathcal{L}$ *be a lattice in* $\mathbb{Z}^n$ *with basis* $b_1, \ldots, b_n$. *Let* $1/4 < \delta < 1$. *Then the LLL algorithm with factor* δ *terminates and performs* $O(n^2 \log(X))$ *iterations where* $\|b_i\|^2 \leq X$ *for all* $1 \leq i \leq n$.

Proof. See 8, Theorem 17.5.1. □

4.3.2 Coppersmith's Method

Coppersmith's method was proposed by 4 and is basically used in order to find the integer roots of a univariate or bivariate polynomials modulo a given integer. Particularly, given a large integer N^δ for some δ such that $0 < \delta < 1$, let

$$F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

If there exists $x_0 < N^{\delta/n}$ such that $F(x_0) \equiv 0 \pmod{N^\delta}$, then 4 showed that x_0 can be found in polynomial time via LLL algorithm. The algorithm outputs a different polynomial f that is related to F that satisfy the conditions imposed for x_0 with smaller coefficients. The conditions are formulated by 12 who revisit Coppersmith's method. The conditions are as follow.

Theorem 4.3.4 (Howgrave-Graham)**.** *Let* $F \in \mathbb{Z}[x]$ *be a monic polynomial of degree* n *over the integers. Let* b_F *be the row vector that is related to* $F(x)$ *where* $\|b_F\| = \sqrt{\sum_{i=0}^{n} |a_i| X^i}$. *If*

(a) $F(x_0) \equiv 0 \pmod{N^\delta}$ *where* $|x_0| < X$

(b) $\|b_F\| < \frac{N^\delta}{\sqrt{n+1}}$

Then $F(x_0) = 0$.

Proof. For $x_i, y_i \in \mathbb{R}$, Cauchy-Schwarz inequality gives $(\sum_i^n x_i y_i)^2 \leq (\sum_i^n x_i)(\sum_i^n y_i)$. Taking x_i a positive integer and $y_i = 1$ for $1 \leq i \leq n$ yields

$$\sum_{i=1}^{n} x_i \leq \sqrt{n \sum_{i=1}^{n} x_i^2}.$$

Then, let

$$\begin{aligned} |F(x_0)| &= x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0 = \sum_{i=0}^{n} a_i x_0^i \leq \sum_{i=0}^{n} |a_i||x_0^i| \\ &\leq \sum_{i=0}^{n} |a_i| X^i \leq \sqrt{n+1 \sum_{i=0}^{n} |a_i| X^i} = \sqrt{n+1}\, \| b_F\| < N^\delta \end{aligned}$$

Thus, $-N^\delta < |F(x_0)| < N^\delta$. But $F(x_0) \equiv 0 \pmod{N^\delta}$, hence $F(x_0) = 0$. □

Next we define lattice $\mathcal{L}$ with basis corresponding to $n+1$ polynomials $f_i(x) = N^\delta x^i$ for $0 \leq i < n$ and $F(x)$. We can see that the polynomials have the solution $x \equiv x_0 \pmod{N}$ and each element in a row vector of the matrix M corresponding to $\mathcal{L}$ can be written as a polynomial $F(x)$ such that $F(x_0) \equiv 0 \pmod{N}$. The bases of $\mathcal{L}$ will be as follows.

$$M = \begin{bmatrix} N^\delta & 0 & \cdots & 0 & 0 \\ 0 & N^\delta X & \cdots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & N^\delta X^{n-1} & 0 \\ a_0 & a_1 X & \cdots & a_{n-1} X^{n-1} & X^n \end{bmatrix},$$

Now, we need to run the LLL algorithm to find b_F such that

$$\| b_F\| < \frac{N}{\sqrt{n+1}}. \tag{4.5}$$

From Theorem 17.2.12 in 8, the first vector $\underline{b}_1$ of the LLL-reduced basis satisfies

$$\underline{b}_1 \leq 2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}}.$$

This implies that if there exists $\mathcal{L}$ sith n-dimension such that

$$2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}} < \frac{N^\delta}{\sqrt{n+1}}$$

then we can find b_F that

$$\|b_F\| \leq 2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}} < \frac{N}{\sqrt{n+1}}.$$

and satisfies (4.5).

Remark 4.3.5. Since $\|b_F\| = \sqrt{\sum_{i=0}^{n} |a_i| X^i}$, by having a larger value of X, we can have a larger value of $2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}}$ and be closer to the bound of $\frac{N}{\sqrt{n+1}} \approx N^\delta$. Thus, two methods are considered to achieve the larger values of X.

- Increase the dimension n of $\mathcal{L}$ by adding new coefficient vector to $\mathcal{L}$. This method is known as "x-shift addition" works by adding $xF(x), x^2F(x), x^3F(x)$, to the basis while ensuring it changes $\det(\mathcal{L})$ at most N^δ.
- Increase the power of N^δ by using powers of $F(x)$.

Both methods mentioned in Remark 4.3.5 are utilized by attacks throughout this survey to obtain the basis vectors that works best in the attacks. Now we are ready to put forward the Coppersmith's method in an univariate form.

Theorem 4.3.6 (Coppersmith's method)**.** *Let $N = pq$ be an RSA modulus where $p < q < 2p$ and $p \geq N^\delta$. Suppose $F \in \mathbb{Z}[x]$ be an univariate, monic polynomial of degree n. Then we can find all solutions x_0 for the equation $F(x) \equiv 0 \pmod{N^\delta}$ with*

$$|x_0| \leq \frac{1}{2} N^{\frac{\delta^2}{n} - \epsilon}$$

in polynomial time where $\epsilon > 0$.

Proof. See 14, Theorem 6. □

4.4 Partially Known MSBs/LSBs of the RSA Primes

In the earliest result involving known bits of RSA primes, 5 showed that only 1/2 MSBs of RSA primes are required to factor N in polynomial time. Later, 3 showed the condition imposed on MSBs is also applied on LSBs of the primes.

Theorem 4.4.1. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Suppose at least 1/2 of the MSBs or LSBs of p or q are known, then N can be factored in polynomial time.*

Proof. See 10, Theorem 6.1. □

This result solely depends on the knowledge regarding the MSBs/LSBs of the primes. In the more recent results, a weaker condition than conditions in Theorem 4.4.1 can be obtained if the size of d is significantly smaller than N.

Theorem 4.4.2. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let e be an RSA public exponent and $d = N^{\delta}$ be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Given the RSA public keys tuple (N, e) and γ MSBs of p or q satisfies*

$$1 - 2\gamma < \delta \leq 1 - \sqrt{\gamma},$$

where $1/4 < \gamma \leq 1/2$ then N can be factored in polynomial time.

Proof. See 17, Theorem 4. □

Theorem 4.4.2 shows that for $d < N^{0.292}$, then at least 1/2 of MSBs of p or q are required. If the size of d is getting smaller, then less MSBs of the primes are needed to factor N in feasible time. The bound of d when $\gamma = 1/2$ in this result conforms to the result from 2 of small private exponent attacks which states that RSA modulus is vulnerable to lattice attack when $d < N^{0.292}$. The following theorem shows the result when d is moderately small but still larger than the size in Theorem 4.4.2.

Theorem 4.4.3. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let e be an RSA public exponent and $d = N^{\delta}$ be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Given the RSA public keys tuple (N, e) and γ MSBs of p or q satisfies*

$$\delta \leq \frac{\sqrt{16\gamma^2 - 4\gamma + 4} - (6\gamma - 2)}{5},$$

where $1/4 < \gamma \leq 1/2$ then N can be factored in polynomial time.

Proof. See 17, Theorem 5. □

Result from Theorem 4.4.3 gives an interesting outlook by pointing out that if d is slightly smaller than $N^{1/2}$ then an adversary only requires 1/4 MSBs of p or q. This shows significant reduces in the amount of MSBs that needs to be known in the case where the size of the private exponent is moderately small. It also shows the importance of keeping the size of d to be at least greater than $N^{1/2}$.

4.5 Partially Known MSBs of the RSA Exponents

In this section, we review attacks on the RSA cryptosystem when given partially known of MSBs of RSA exponents, (a) the size of the RSA private exponent, d is small; or (b) the size of the RSA public exponent, e is small.

4.5.1 Small Private Exponent

Let the adversary knows $\tilde{d}$ such that $|d - \tilde{d}| < N^{\beta}$, this implies β of MSBs of d are known. In the first attack on RSA with small private exponent, 6 modifies RSA key equation (Equation 4.1) to

$$F_A(u, v, w) = eu - Nv + vw + e\tilde{d} - 1 \tag{4.6}$$

since $d-\tilde{d}, k, p+q-1$ is a root of F_A over integers. By defining such parameters suited to the enabling conditions stated in Theorem 2.13 of 10, it enables Coppersmith's method to find two polynomial F_1 and F_2 with the same root (u_0, v_0, w_0). Using a heuristic assumption based on their experiments, they obtain $w_0 = p + q - 1$. This solves factorization of N. Their results are as follow.

Theorem 4.5.1 (Small d, large e)**.** *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let $e \approx N$ be an RSA public exponent and $d = N^{\delta}$ be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Suppose $0 < \beta < \delta < 1$. Suppose the $(\delta - \beta) \log N$ MSBs of d are known, then N can be factored in polynomial time if*

(a) $\beta \leq \frac{3}{16} - \epsilon$ *and* $\delta \leq \frac{11}{16}$, *or*

(b) $\beta \leq \frac{1+\delta-\sqrt{4\delta^2+2\delta-2}}{3} - \epsilon$ *and* $\delta \geq \frac{11}{16}$, *or*

(c) $\beta \leq \frac{5}{6} - \frac{1}{3}\sqrt{1+6\delta} - \epsilon$

for every $\epsilon > 0$.

Proof. See 6, Theorem 1. □

18 utilizes the same strategy as 6 but using shift-polynomials as 16. However, they change the selections of the shift-polynomials that yield basis matrices that are not triangular, hence deter the Coppermisth's method to work efficiently. To overcome this, Takayasu and Kunihiro utilize linearization method which also eliminates the unhelpful polynomials and create helpful polynomials in regards to $F(x)$. Their results are as follow.

Theorem 4.5.2. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let $e \approx N$ be an RSA public exponent and $d = N^{\delta}$ be an RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Suppose the most significant $(\delta - \beta) \log N$ bits of d are known then N can be factored in polynomial time if*

(a) $\beta \leq \frac{1+\delta-\sqrt{-1+6\delta-3\delta 2}}{2} - \epsilon$ *and* $\delta \leq \frac{1}{2}$, *or*

(b) $\beta \leq \frac{\kappa}{2} - \frac{\kappa^2}{3} + \frac{1}{12\kappa} \cdot \frac{(\kappa-2(\delta-\beta))^3}{1+\delta-2\delta} - \epsilon$, *and* $\kappa = 1 - \frac{2\delta-1}{1-2\sqrt{1+\beta-2\delta}}$ *and* $\frac{1}{2}\delta \leq \frac{9}{16}$

for every $\epsilon < 1$.

Proof. See 18, Theorem 1. □

4.5.2 Small Public Exponent

From the result by Coppersmith 5, Boneh et al. 3 showed that when e is less than $N^{1/4}$, given 3/4 MSBs of d, then a good approximation of $S = p+q$ using the values of RSA public keys, (N, e), k in RSA key equation and $\tilde{d}$ is obtained. Using the value of S, the approximation of the larger RSA prime can be computed in polynomial time. Based on Theorem 4.4.1, this results in the factorization of N in polynomial time. The attack is as follows.

Theorem 4.5.3. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let $e = N^{\alpha}$ be an RSA public exponent for any $0 < \alpha \leq 1/4$ and d be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Let $|p - q| > \frac{1}{\zeta} N^{1/4}$ for some $\zeta > 1$. Let $e = \mu k$ for some $\mu > 1$ and k in the RSA key equation. Suppose the 3/4 MSBs of d are known, then N can be factored in polynomial time with respect to $\log N, \zeta$ and μ.*

Proof. See Theorem 6.8 in 10. □

For a larger e, that is from $N^{1/4}$ to $N^{1/2}$, 3 showed that a good approximation of S can be obtained given that e is a prime number. The strategy is similar to the result from Theorem 4.5.3, but the impact is more profound since only 1/4 MSBs of d is necessary to be known for the attack to be successful. The attack is as follows.

Theorem 4.5.4. *Let p and q be the RSA primes that satisfies $p < q < 2p$ with RSA modulus $N = pq$. Let $e = N^{\alpha}$ be an RSA public exponent for any $1/4 < \alpha \leq 1/2$ and d be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Given the α MSBs of the private exponent the modulus can be factored in time polynomial in log(N).*

Proof. See Theorem 6.9 in 10. □

Following their results in Theorem 4.5.1, 6 obtained a partial information regarding k of RSA key equation defined as $\tilde{k}$. Again, they modified the RSA key equation to

$$F_A(u, v, w) = eu - Nv + vw + \tilde{k}w + e\tilde{d} - 1.$$

They also integrated x-shift method into their attack. The results are as follow.

Theorem 4.5.5. *Let $N = pq$ be an $\mathfrak{n}$-bit RSA modulus where $p < q < 2p$. Let $e = N^{\alpha}$ be an RSA public exponent and $d \approx N$ be an RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Let $0 < \beta < \frac{1}{2} < \alpha < 1$. Suppose the $(1 - \beta)n$ MSBs of d are known then Ncan be factored in polynomial time if*

$$\beta \leq \frac{1 + \alpha - \sqrt{2(2\alpha^2 + \alpha - 1)}}{3} - \epsilon.$$

for every $\epsilon > 0$.

Proof. See 6, Theorem 2. □

4.6 Partially Known LSBs of the RSA Exponents

In this section, we review attacks on RSA cryptosystem when β LSBs of d are known. Particularly, we assume the adversary is given $\hat{d}$ and some t such that $d = d_0 t + \hat{d}$. This also implies $\hat{d} = d \pmod{t}$. In the first result of such assumption, 3 showed that by assigning $t = 2^{\frac{\mathfrak{n}}{4}}$ for an $\mathfrak{n}$-bit RSA modulus, it is sufficient $\beta \geq 1/4$ LSBs of d is known to factor N in polynomial time. The attack required to perform at most j operations of Coppersmith's method where $k = Rj$ and R is an odd number. The result is as follows.

Theorem 4.6.1. *Let $N = pq$ be an $\mathfrak{n}$-bit RSA modulus where $p < q < 2p$. Let $1 < e, d < \phi(N)$ where e be an RSA public exponent and d be its corresponding RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Suppose the $1/4$ LSBs of d is known then N can be factored in polynomial time with respect to $\mathfrak{n}$ and e.*

Proof. See 3, Theorem 1. □

In LSB case, 6 inserted $\tilde{d}$ into a modified RSA key equation

$$F(u, v, w) = etu - Nv + vw + e\hat{d} - 1$$

which has the same monomials as (4.6). Thus, same strategy is applied onto $F(u, v, w)$ and produces the following result.

Theorem 4.6.2 (Small d)**.** *Let $N = pq$ be an $\mathfrak{n}$-bit RSA modulus where $p < q < 2p$. Let $e = N^{\alpha}$ be an RSA public exponent and $d \approx N^{\delta}$ be an RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Let $\alpha = \log N$ and $0 < \beta < \frac{1}{2} < \alpha < 1$. Suppose $(\delta - \beta)\mathfrak{n}$ LSBs of d are known, then N can be factored in polynomial time if*

$$\beta < \frac{5 - 2\sqrt{1 + 6\delta}}{6} - \epsilon$$

for every $\epsilon > 0$.

Proof. See 6, Theorem 3. □

In 2014, 18 utilized the basis matrix formed by 1 which is not triangular. Similar to the MSBs cases in the previous section, Takayasu and Kunihiro employed a strategy known as unravelled linearization by transformed Aono's basis matrix to a triangular form using linearization $w = 1 + uv$. The result is as follows.

Theorem 4.6.3. *Let $N = pq$ be an $\mathfrak{n}$-bit RSA modulus where $p < q < 2p$. Let $e = N^{\alpha}$ be an RSA public exponent and $d \approx N^{\delta}$ be an RSA private exponent which computes $ed \equiv 1 \pmod{\phi(N)}$. Suppose $(\delta - \beta)\mathfrak{n}$ of LSBs d is known, then N can be factored in polynomial time if*

$$\beta \leq \frac{1 + \delta - \sqrt{-1 + 6\delta - 3\delta^2}}{2} - \epsilon, \quad \textit{and} \quad \delta \leq \frac{9 - \sqrt{21}}{12}$$

for every $\epsilon > 0$.

Proof. See 18, Theorem 2. □

4.7 Conclusion

We survey a collection of partial key exposure attacks on the RSA cryptosystem. The attacks can be categorized into three namely, partially known MSBs and LSBs of the RSA primes, partially known MSBs of the RSA exponents and partially known LSBs of the RSA exponents. All of the attacks mainly utilized Coppersmith's method to find the small solutions to the polynomial equations of modulo N or divisor of N via LLL algorithm. The values of the small solutions then are used to factor RSA modulus in the polynomial time.

Acknowledgement

The present research was partially supported by the Putra Grant with Project Number GP-IPS/2018/9657300.

Bibliography

[1] Aono, Y. (2009). *A new lattice construction for partial key exposure attack for RSA*. In *International Workshop on Public Key Cryptography*, pages 34–53. Springer.

[2] Boneh, D. and Durfee, G. (2000). *Cryptanalysis of RSA with private key d less than* $N^{0.292}$. IEEE transactions on Information Theory, 46(4):1339–1349.

[3] Boneh, D., Durfee, G., and Frankel, Y. (1998). *Exposing an RSA private key given a small fraction of its bits.* Full version of the work from Asiacrypt, 98.

[4] Coppersmith, D. (1996). *Finding a small root of a bivariate integer equation; factoring with high bits known.* In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 178–189. Springer.

[5] Coppersmith, D. (1997). *Small solutions to polynomial equations, and low exponent RSA vulnerabilities.* Journal of Cryptology, 10(4):233–260.

[6] Ernst, M., Jochemsz, E., May, A., and De Weger, B. (2005). *Partial key exposure attacks on RSA up to full size exponents.* In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 371–386. Springer.

[7] FIPS, P. (2013). *186-4: Federal information processing standards publication. Digital Signature Standard (DSS).* Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD, pages 20899–8900.

[8] Galbraith, S. D. (2012). *Mathematics of public key cryptography.* Cambridge University Press.

[9] Hardy, G. H. and Wright, E. M. (1979). *An introduction to the theory of numbers.* Oxford university press.

[10] Hinek, M. J. (2009). *Cryptanalysis of RSA and its variants.* CRC press.

[11] Hoffstein, J., Pipher, J., Silverman, J. H., and Silverman, J. H. (2008). *An introduction to mathematical cryptography*, volume 1. Springer.

[12] Howgrave-Graham, N. (1997). *Finding small roots of univariate modular equations revisited*. In *IMA International Conference on Cryptography and Coding*, pages 131–142. Springer.

[13] Kocher, P. C. (1996). *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*. In *Annual International Cryptology Conference*, pages 104–113. Springer.

[14] May, A. (2003). *New RSA vulnerabilities using lattice reduction methods*. PhD thesis, University of Paderborn Paderborn.

[15] Rivest, R. L., Shamir, A., and Adleman, L. (1978). *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 21(2):120–126.

[16] Sarkar, S., Gupta, S. S., and Maitra, S. (2010). *Partial key exposure attack on RSA–improvements for limited lattice dimensions*. In *International Conference on Cryptology in India*, pages 2–16. Springer.

[17] Sarkar, S., Maitra, S., and Sarkar, S. (2008). *RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension.* IACR Cryptology ePrint Archive, 2008:315.

[18] Takayasu, A. and Kunihiro, N. (2014). *Partial key exposure attacks on RSA: achieving the boneh-durfee bound*. In *International Conference on Selected Areas in Cryptography*, pages 345–362. Springer.

Chapter 5

Application of the Keller-box Method to Magnetohydrodynamic Rotating Flow over a Permeable Shrinking Surface

Mohd Ezad Hafidz Hafidzuddin[1,*], Roslinda Nazar[2], Norihan Md Arifin[3]

[1] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre for Modelling & Data Science, Faculty of Science & Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia.
[3] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: ezadhafidz@upm.edu.my

Abstract

This chapter deals with the application of the Keller-box Method to numerically solve a problem of magnetohydrodynamics rotating boundary layer flow over a permeable shrinking sheet. We used the similarity transformations to reduce the system of partial differential equations (PDE) into a system of ordinary differential equations (ODE). The transformed equations are then solved using the Keller-box Method. All formulation and derivation processes are shown and elaborated in detail. The effects of the governing parameters involved, namely magnetic parameter, suction parameter and rotating parameter on both the velocity and lateral velocity fields are presented and discussed.

Keywords: MHD; Keller-box; Boundary layer flow; Rotating flow; Shrinking sheet.

5.1 Introduction

Since the work of Sakiadis [1], numerous aspects and conditions of boundary layer flow due to a stretching or shrinking sheet have been considered and studied. [1] was extended by Crane [2] for the two-dimensional problem. Later, the uniqueness of the exact analytical solution presented in [1] is discussed by McLeod and Rajagopal [3]. Gupta and Gupta [4] and Magyari and Keller [5] researched the heat and mass transfer over a stretching sheet where the flow is subjected to suction or blowing.

Meanwhile, problems involving magnetohydrodynamics related to the boundary layer flow become more and more significant in the industry. Pavlov [6] obtained an exact similarity solution for the problem of an electrically conducting fluid an elastic

stretching sheet in the existence of a uniform magnetic field. Anderson [7] found that the boundary layer thickness is reduced and the skin friction is increased with the introduction of the elasticity and magnetic field for the problem of MHD flow of a viscoelastic fluid past a stretching surface. On the other hand, the unsteady boundary layer flow due to a stretching surface in a rotating fluid is considered by Nazar et al. [8] while Ishak et al. [9] investigated the MHD boundary layer flow and heat transfer alongside to stretching vertical sheet with power law velocity. Wang [10] examined the rotating viscous fluid and heat transfer on a stretching sheet, while Abbas et al. [11] studied the unsteady magnetohydrodynamic flow and heat transfer on a stretching sheet in a rotating fluid.

All the above cited literatures deal with the viscous flow against the stretching surface. As for the flow against the shrinking surface, it is found that Wang [12] was the earliest to consider the unsteady viscous flow induced by a shrinking liquid film. Several years later, Miklavcic and Wang [13] verified the existence and non-uniqueness solution for steady viscous hydrodynamic flow due to a shrinking sheet for a specific value of suction. The MHD rotating flow of a viscous fluid over a shrinking sheet is studied by Sajid et al. [14], while Hayat et al. [15] considered the analytic solution for MHD rotating flow of a second grade fluid past a porous shrinking surface. Then, Faraz and Khan [16] studied the two-dimensional MHD steady rotating flow of a second grade fluid due to a porous shrinking surface. Recently, the effect of magnetohydrodynamic on three dimensional rotating flow and heat transfer of ferrofluid over an exponentially permeable stretching/shrinking sheet with suction effect is numerically studied by Jusoh et al. [17]. Furthermore, Nasir et al. [18] investigated the three dimensional rotational nanofluid flow that contains carbon nanotube with thermal radiation past a stretching sheet.

Our study in this chapter considers the idea in [14] by solving it numerically using the different method, namely the Keller-box method. This method was proposed by Keller and Cebeci [19] and used in many literatures such as in [20–24] to solve various boundary layer problems.

5.2 Problem Formulation

To formulate this problem mathematically, we consider the steady and laminar magnetohydrodynamic boundary layer flow of a viscous fluid caused by a two dimensional shrinking surface in a rotating fluid. Let (u, v, w) represent the velocity components along the (x, y, z) directions, respectively, with the angular velocity of the rotating fluid in the z-direction is represent by Ω.

In addition, we apply a constant magnetic field B_0 in the z-direction and assume the zero electric field and small magnetic Reynolds number. With that, and following [14], the boundary layer equations which govern this flow can be written as

$$\frac{\partial u}{\partial x} + \frac{\partial w}{\partial z} = 0, \tag{5.1}$$

$$u\frac{\partial u}{\partial x} + w\frac{\partial u}{\partial z} - 2\Omega v - \nu\frac{\partial^2 u}{\partial z^2} + \frac{\sigma B_0^2}{\rho}u = 0, \tag{5.2}$$

$$u\frac{\partial v}{\partial x} + w\frac{\partial v}{\partial z} - 2\Omega u - \nu\frac{\partial^2 v}{\partial z^2} + \frac{\sigma B_0^2}{\rho}v = 0, \tag{5.3}$$

where $\nu = \frac{\mu}{\rho}$ denotes the kinematic viscosity, σ is the electrical conductivity, and ρ is the density.

The boundary conditions for Eqs. (17.1)-(17.3) are

$$\begin{aligned} &u = -kx,\ v = 0,\ w = -W \text{ at } z = 0, \\ &u \to 0,\ v \to 0 \text{ as } z \to \infty. \end{aligned} \tag{5.4}$$

Here, $k(> 0)$ and $W(> 0)$ denote the shrinking constant and the suction velocity, respectively. Following [14], we propose the following similarity transformations

$$u = -kxf'(\eta),\ v = kxg(\eta),\ w = -\sqrt{k\nu}f(\eta),\ \eta = \sqrt{\frac{k}{\nu}}z. \tag{5.5}$$

Eq. (17.1) is satisfied, while Eqs. (17.2) and (17.3) are reduced to the following:

$$f''' = f'^2 - ff'' - 2\lambda g + M^2 f', \tag{5.6}$$

$$g'' = f'g - fg' + 2\lambda f' + M^2 g, \tag{5.7}$$

where primes denote the differentiation with respect to η, while $f = f(\eta)$ and $g = g(\eta)$ denote the velocity and lateral velocity, respectively.

The boundary conditions (5.4) become

$$\begin{aligned} &f(0) = s,\ f'(0) = -1,\ g(0) = 0, \\ &f'(\eta) \to 0,\ g(\eta) \to 0 \text{ as } \eta \to \infty, \end{aligned} \tag{5.8}$$

where $s = \frac{W}{m\sqrt{k\nu}}$ represents the suction parameter, $M^2 = \sigma B_0^2/\rho a$ is the magnetic parameter and $\lambda = \frac{\Omega}{a}$ represents the relation between the rate of shrinkage and the rotation rate.

The local skin friction coefficients in the $x-$ and $y-$directions are given by

$$C_{fx} = \frac{\tau_{wx}}{\rho u^2},\ C_{fy} = \frac{\tau_{wy}}{\rho u^2}, \tag{5.9}$$

where the shear stresses τ_{wx} and τ_{wy} are defined as

$$\tau_{wx} = \mu \left(\frac{\partial u}{\partial z}\right)_{z=0},\ \tau_{wy} = \mu \left(\frac{\partial v}{\partial z}\right)_{z=0}, \tag{5.10}$$

where ν is the dynamic viscosity.

Using (5.5) and (5.10), Eq. (5.9) becomes

$$C_{fx}Re_x^{1/2} = f''(0),\ C_{fy}Re_y^{1/2} = g'(0). \tag{5.11}$$

5.3 Numerical Procedure

Eqs. (5.6) and (5.7) that subject to the boundary conditions (5.8) are solved numerically using the finite-difference scheme known as the Keller-box method [25,26]. This method consists of the following steps:

1. reduce the Eqs. (5.6) and (5.7) to a first order system,
2. write the differential equations using central differences,
3. use Newton's method to linearize the resulting algebraic equations,
4. write the linearized equations in matrix-vector form,
5. solve the linear system by using the block-tridiagonal-elimination technique,

which will be discussed in detail in the following sections.

5.3.1 Finite Difference Scheme

Cebeci and Bradshaw [25, 26] and Na [27] stated that each equation to be resolved should be written in the form of first order equations. In this section, steps 1 and 2 are combined.

Therefore, the following new dependent variables $u(\eta)$, $v(\eta)$ and $w(\eta)$ are introduced as follows

$$f' = u,\ u' = v,\ g' = w, \tag{5.12}$$

so that Eqs. (5.6) and (5.7) can be written as

$$v' - u^2 + fv + 2\lambda g - M^2 u = 0, \tag{5.13}$$

$$w' - ug + fw - 2\lambda u - M^2 g = 0, \tag{5.14}$$

where $u = u(\eta)$, $v = v(\eta)$ and $w = w(\eta)$.

With the variables introduced above, the boundary conditions (5.8) become

$$\begin{aligned} &f(0) = s,\ u(0) = -1,\ g(0) = 0, \\ &u(\infty) = 0,\ g(\infty) = 0. \end{aligned} \tag{5.15}$$

In this study, Eqs. (5.13) and (5.14) subject to the boundary conditions (5.15) only has one independent variable, which is η. Therefore, consider a straight line in Fig. 5.1 and the points on the line are marked as:

$$\eta_0 = 0,\ \eta_j = \eta_{j-1} + h_j,\ j = 1, 2, \ldots, J,\ \eta_J = \eta_\infty, \tag{5.16}$$

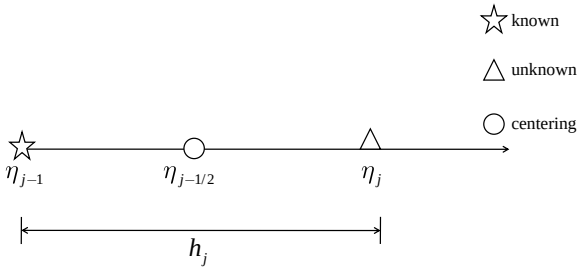

Figure 5.1: Line for difference approximations

where h_j and j are the $\Delta\eta-$spacing and the sequence of numbers that indicate the coordinate location, respectively.

For any function, the first derivative is estimated as

$$\frac{\partial u}{\partial \eta} = \frac{u_j - u_{j-1}}{h_j}, \tag{5.17}$$

and for any points, the finite difference form is

$$(\,)_{j-\frac{1}{2}} = \frac{(\,)_j + (\,)_{j-1}}{2}. \tag{5.18}$$

Using centered-difference derivatives, we write the finite difference form of Eq. (5.12) for the midpoint $\eta_{j-\frac{1}{2}}$ of the segment P_1P_2 and obtain the following:

$$f_j - f_{j-1} - \frac{1}{2}(u_j + u_{j-1})\, h_j = 0, \tag{5.19}$$

$$u_j - u_{j-1} - \frac{1}{2}\left(v_j + v_{j-1}\right) h_j = 0, \tag{5.20}$$

$$g_j - g_{j-1} - \frac{1}{2}\left(w_j + w_{j-1}\right) h_j = 0. \tag{5.21}$$

Eqs. (5.13) and (5.14) can be written in the finite difference form for the midpoint $\eta_{j-\frac{1}{2}}$ of the segment P_1P_2. If the LHS of Eqs. (5.13) and (5.14) are stated as L_1 and L_2, respectively, we will obtain

$$(L_1)_{j-\frac{1}{2}} = 0, \tag{5.22}$$

$$(L_2)_{j-\frac{1}{2}} = 0. \tag{5.23}$$

Using L_1 and L_2 from above, we obtain

$$\begin{aligned}
(L_1)_{j-\frac{1}{2}} &= \left[v' - u^2 + fv + 2\lambda g - M^2 u\right]_{j-\frac{1}{2}}, \\
&= \frac{v_j - v_{j-1}}{h_j} - \left(u_{j-\frac{1}{2}}\right)^2 + f_{j-\frac{1}{2}} v_{j-\frac{1}{2}} + 2\lambda g_{j-1/2} - M^2 u_{j-\frac{1}{2}}, \qquad (5.24) \\
(L_2)_{j-\frac{1}{2}} &= \left[w' - ug + fw - 2\lambda u - M^2 g\right]_{j-\frac{1}{2}}, \\
&= \frac{w_j - w_{j-1}}{h_j} - u_{j-\frac{1}{2}} g_{j-\frac{1}{2}} + f_{j-\frac{1}{2}} w_{j-\frac{1}{2}} - 2\lambda u_{j-\frac{1}{2}} - M^2 g_{j-\frac{1}{2}}. \qquad (5.25)
\end{aligned}$$

By substituting Eqs. (5.22) and (5.23) into Eqs. (5.24) and (5.25), we obtain

$$\begin{aligned}
v_j - v_{j-1} - \frac{1}{4} h_j (u_j + u_{j-1})^2 + \frac{1}{4} h_j \left(f_j + f_{j-1}\right)\left(v_j + v_{j-1}\right) + \\
h_j \lambda \left(g_j + g_{j-1}\right) - \frac{1}{2} M^2 h_j \left(u_j + u_{j-1}\right) = 0, \qquad (5.26) \\
w_j - w_{j-1} - \frac{1}{4} h_j \left(u_j + u_{j-1}\right)\left(g_j + g_{j-1}\right) + \frac{1}{4} h_j \left(f_j + f_{j-1}\right)\left(w_j + w_{j-1}\right) - \\
h_j \lambda \left(u_j + u_{j-1}\right) - \frac{1}{2} M^2 h_j \left(g_j + g_{j-1}\right) = 0. \qquad (5.27)
\end{aligned}$$

5.3.2 Newton's Method

In this section, the nonlinear equations obtained from the finite difference method will be linearized. To linearize the nonlinear system of equations (5.19)-(5.20), (5.26) and (5.27), we introduce the following iterates:

$$\begin{aligned}
&f_j^{(i+1)} = f_j^{(i)} + \delta f_j^{(i)},\ u_j^{(i+1)} = u_j^{(i)} + \delta u_j^{(i)},\ v_j^{(i+1)} = v_j^{(i)} + \delta v_j^{(i)}, \\
&g_j^{(i+1)} = g_j^{(i)} + \delta g_j^{(i)},\ w_j^{(i+1)} = w_j^{(i)} + \delta w_j^{(i)}.
\end{aligned} \tag{5.28}$$

Substituting (5.28) into Eqs. (5.19)-(5.20), (5.26) and (5.27) and then drop the quadratic and higher order terms in $\delta f_j^{(i)}$, $\delta u_j^{(i)}$, $\delta v_j^{(i)}$, $\delta g_j^{(i)}$ and $\delta w_j^{(i)}$, following by dropping the superscript (i) (for simplicity), we obtain the linear tridiagonal system

as the following:

$$\begin{aligned}
&\delta f_j - \delta f_{j-1} - \frac{1}{2}h_j\left(\delta u_j + \delta u_{j-1}\right) = (r_1)_{j-\frac{1}{2}},\\
&\delta u_j - \delta u_{j-1} - \frac{1}{2}h_j\left(\delta v_j + \delta v_{j-1}\right) = (r_2)_{j-\frac{1}{2}},\\
&\delta g_j - \delta g_{j-1} - \frac{1}{2}h_j\left(\delta w_j + \delta w_{j-1}\right) = (r_3)_{j-\frac{1}{2}},\\
&(a_1)_j\delta v_j + (a_2)_j\delta v_{j-1} + (a_3)_j\delta f_j + (a_4)_j\delta f_{j-1} + (a_5)_j\delta u_j +\\
&\qquad (a_6)_j\delta u_{j-1} + (a_7)_j\delta g_j + (a_8)_j\delta g_{j-1} = (r_4)_{j-\frac{1}{2}},\\
&(b_1)_j\delta w_j + (b_2)_j\delta w_{j-1} + (b_3)_j\delta f_j + (b_4)_j\delta f_{j-1} + (b_5)_j\delta u_j +\\
&\qquad (b_6)_j\delta u_{j-1} + (b_7)_j\delta g_j + (b_8)_j\delta g_{j-1} = (r_5)_{j-\frac{1}{2}},
\end{aligned} \tag{5.29}$$

where

$$\begin{aligned}
&(a_1)_j = 1 + \frac{1}{2}h_j f_{j-\frac{1}{2}},\ (a_2)_j = (a_1)_j - 2,\ (a_3)_j = \frac{1}{2}h_j v_{j-\frac{1}{2}},\\
&(a_4)_j = (a_3)_j,\ (a_5)_j = -\frac{1}{2}M^2 h_j - h_j u_{j-\frac{1}{2}},\ (a_6)_j = (a_5)_j,\\
&(a_7)_j = h_j\lambda,\ (a_8)_j = (a_7)_j.
\end{aligned} \tag{5.30}$$

$$\begin{aligned}
&(b_1)_j = 1 + \frac{1}{2}h_j f_{j-\frac{1}{2}},\ (b_2)_j = (b_1)_j - 2,\ (b_3)_j = \frac{1}{2}h_j w_{j-\frac{1}{2}},\\
&(b_4)_j = (b_3)_j,\ (b_5)_j = -h_j\lambda - \frac{1}{2}h_j g_{j-\frac{1}{2}},\ (b_6)_j = (b_5)_j,\\
&(b_7)_j = -\frac{1}{2}M^2 h_j - \frac{1}{2}h_j u_{j-\frac{1}{2}},\ (b_8)_j = (b_7)_j.
\end{aligned} \tag{5.31}$$

and

$$\begin{aligned}
&(r_1)_{j-\frac{1}{2}} = f_{j-1} - f_j + h_j u_{j-\frac{1}{2}},\\
&(r_2)_{j-\frac{1}{2}} = u_{j-1} - u_j + h_j v_{j-\frac{1}{2}},\\
&(r_3)_{j-\frac{1}{2}} = g_{j-1} - g_j + h_j w_{j-\frac{1}{2}},\\
&(r_4)_{j-\frac{1}{2}} = v_{j-1} - v_j + h_j u^2_{j-\frac{1}{2}} - h_j f_{j-\frac{1}{2}} v_{j-\frac{1}{2}} - h_j\lambda\left(g_j + g_{j-1}\right) + M^2 h_j u_{j-\frac{1}{2}},\\
&(r_5)_{j-\frac{1}{2}} = w_{j-1} - w_j + h_j u_{j-\frac{1}{2}} g_{j-\frac{1}{2}} - h_j f_{j-\frac{1}{2}} w_{j-\frac{1}{2}} +\\
&\qquad h_j\lambda\left(u_j + u_{j-1}\right) + M^2 h_j g_{j-\frac{1}{2}}.
\end{aligned} \tag{5.32}$$

The boundary conditions (5.15) can be satisfied without iteration to complete the system (5.29). Thus, to maintain these correct values in all iterations, we write

$$\delta f_0 = 0,\ \delta u_0 = 0,\ \delta g_0 = 0,\ \delta u_J = 0,\ \delta g_J = 0. \tag{5.33}$$

5.3.3 Block Elimination Scheme

The system of linear equations (5.29) has a block tridiagonal structure consists of variables or constants, but here in Keller-box method, it consists of block of matrices.

The elements of the matrices are defined as follows:

$$\begin{bmatrix} [A_1] & [C_1] & & & & & \\ [B_2] & [A_2] & [C_2] & & & & \\ & & \ddots & & & & \\ & & \ddots & & & & \\ & & \ddots & & & & \\ & & & [B_{J-1}] & [A_{J-1}] & [C_{J-1}] & \\ & & & & [B_J] & [A_J] & \end{bmatrix} \begin{bmatrix} [\delta_1] \\ [\delta_2] \\ \vdots \\ [\delta_{J-1}] \\ [\delta_J] \end{bmatrix} = \begin{bmatrix} [r_1] \\ [r_2] \\ \vdots \\ [r_{J-1}] \\ [r_J] \end{bmatrix}$$

that is

$$A\delta = r, \tag{5.34}$$

where

$$[A_1] = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ -\frac{1}{2}h_j & 0 & 0 & -\frac{1}{2}h_j & 0 \\ 0 & -\frac{1}{2}h_j & 0 & 0 & -\frac{1}{2}h_j \\ (a_2)_1 & 0 & (a_3)_1 & (a_1)_1 & 0 \\ 0 & (b_2)_1 & (b_3)_1 & 0 & (b_1)_1 \end{bmatrix}, \tag{5.35}$$

$$[A_j] = \begin{bmatrix} -\frac{1}{2}h_j & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & -\frac{1}{2}h_j & 0 \\ 0 & -1 & 0 & 0 & -\frac{1}{2}h_j \\ (a_6)_j & (a_8)_j & (a_3)_j & (a_1)_j & 0 \\ (b_6)_j & (b_8)_j & (b_3)_j & 0 & (b_1)_j \end{bmatrix}, \ 2 \le j \le J, \tag{5.36}$$

$$[B_j] = \begin{bmatrix} 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2}h_j & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2}h_j \\ 0 & 0 & (a_4)_j & (a_2)_j & 0 \\ 0 & 0 & (b_4)_j & 0 & (b_2)_j \end{bmatrix}, \ 2 \le j \le J, \tag{5.37}$$

$$[C_j] = \begin{bmatrix} -\frac{1}{2}h_j & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ (a_5)_j & (a_7)_j & 0 & 0 & 0 \\ (b_5)_j & (b_7)_j & 0 & 0 & 0 \end{bmatrix}, \ 1 \le j \le J-1, \tag{5.38}$$

$$[\delta_1] = \begin{bmatrix} \delta v_0 \\ \delta w_0 \\ \delta f_1 \\ \delta v_1 \\ \delta t_1 \end{bmatrix}, \quad [\delta_j] = \begin{bmatrix} \delta u_{j-1} \\ \delta g_{j-1} \\ \delta f_j \\ \delta v_j \\ \delta w_j \end{bmatrix}, \ 2 \le j \le J, \tag{5.39}$$

and

$$[r_j] = \begin{bmatrix} (r_1)_{j-\frac{1}{2}} \\ (r_2)_{j-\frac{1}{2}} \\ (r_3)_{j-\frac{1}{2}} \\ (r_4)_{j-\frac{1}{2}} \\ (r_5)_{j-\frac{1}{2}} \end{bmatrix}, \ 1 \leq j \leq J. \tag{5.40}$$

To solve Eq. (5.34), A is assummed as nonsingular matrix which can be factored into

$$A = LU, \tag{5.41}$$

where

$$L = \begin{bmatrix} [\alpha_1] & & & & \\ [\beta_2] & [\alpha_2] & & & \\ & & \ddots & & \\ & & \ddots & [\alpha_{J-1}] & \\ & & & [\beta_J] & [\alpha_J] \end{bmatrix} \text{ and } U = \begin{bmatrix} [I] & [\Gamma_1] & & & \\ & [I] & \ddots & & \\ & & \ddots & & \\ & & & [I] & [\Gamma_{J-1}] \\ & & & & [I] \end{bmatrix},$$

where $[I]$ is the identity matrix of order 5, while $[\alpha_i]$ and $[\Gamma_i]$ are 5×5 matrices. We define the following equations to determine the elements:

$$[\alpha_1] = [A_1], \tag{5.42}$$
$$[A_1][\Gamma_1] = [C_1], \tag{5.43}$$
$$[\alpha_j] = [A_j] - [B_j][\Gamma_{j-1}], \ j = 2, 3, \ldots, J, \tag{5.44}$$
$$[\alpha_j][\Gamma_j] = [C_j], \ j = 2, 3, \ldots, J-1. \tag{5.45}$$

By substituting Eq. (5.41) into Eq. (5.34), we get

$$LU\delta = r, \tag{5.46}$$

If we define

$$U\delta = \omega, \tag{5.47}$$

then Eq. (5.46) becomes

$$L\omega = r, \tag{5.48}$$

where

$$\omega = \begin{bmatrix} [\omega_1] \\ [\omega_2] \\ \vdots \\ [\omega_{J-1}] \\ [\omega_J] \end{bmatrix}, \tag{5.49}$$

and $[\omega_j]$ are 5×1 matrices. The elements of ω can be solved from Eq. (5.48)

$$[\alpha_1][\omega_1] = [r_1], \tag{5.50}$$
$$[\alpha_j][\omega_j] = [r_j] - [B_j][\omega_{j-1}], \ 2 \leq j \leq J. \tag{5.51}$$

Once the elements of ω are found, the solution δ is obtained from Eq. (5.47), where the elements are achieved by the following relations:

$$[\delta_J] = [\omega_J], \tag{5.52}$$

$$[\delta_j] = [\omega_j] - [\Gamma_j]\,[\delta_{j+1}]\,,\ 1 \leq j \leq J-1. \tag{5.53}$$

These iterations are repeated until we found some convergence criterion and stop when

$$\left|\delta v_0^{(i)}\right| < \epsilon_1$$

where ϵ is a small prescribed value.

5.4 Results and Discussion

Eqs. (5.6) and (5.7) subject to the boundary conditions (5.8) are solved numerically using an implicit finite difference scheme known as the Keller-box method, as explained thoroughly in Section 5.3. To authenticate the accuracy of the present method, we compare the present numerical results for $f''(0)$ and $g'(0)$ with the results obtained in [10] and [11]. The comparisons are found to be in good agreement (see Table 5.1), and thus we are confident with the accuracy of the present method.

Table 5.1: Comparison with those of [10] and [11].

	[10]		[11]		Present results	
λ	$f''(0)$	$g'(0)$	$f''(0)$	$g'(0)$	$f''(0)$	$g'(0)$
0	-1.0000	0.0000	-1.0000	0.0000	-1.0005	0.0000
0.5	-1.1384	-0.5128	-1.1384	-0.5128	-1.1385	-0.5127
1	-1.3250	-0.8371	-1.3250	-0.8371	-1.3250	-0.8371
2	-1.6523	-1.2873	-1.6523	-1.2873	-1.6524	-1.2873

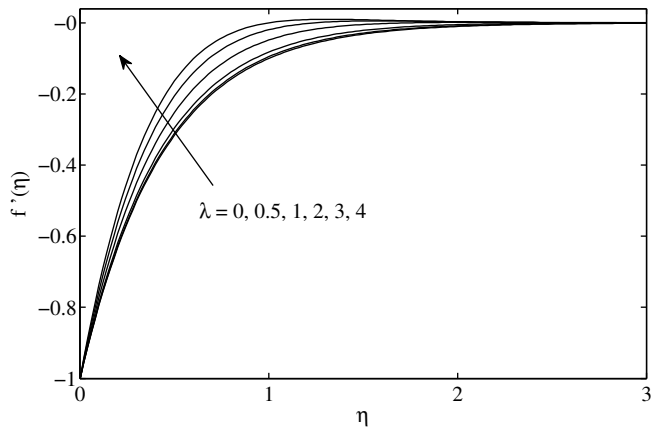

Figure 5.2: Effects of λ on $f'(\eta)$ when $s = 3, M = 2$

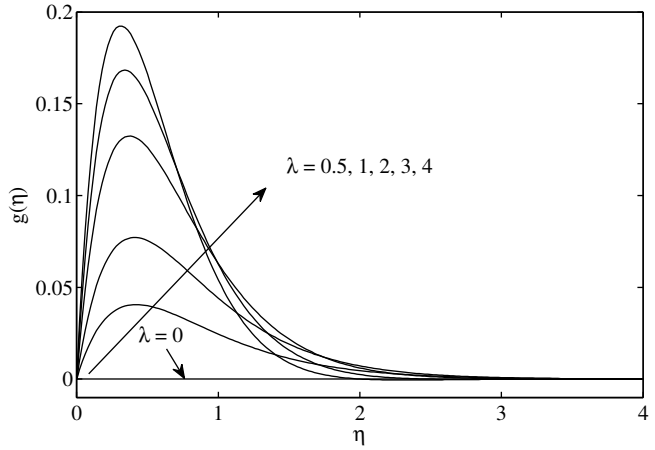

Figure 5.3: Effects of λ on $g(\eta)$ when $s = 3, M = 2, Pr = 0.7$

Figs. 5.2 and 5.3 display the effects of rotating parameter λ on the velocity and lateral velocity profiles $f'(\eta)$ and $g(\eta)$, respectively. Both profiles show decrement in boundary layer thickness with the increase of the λ. We also found that for small values of λ, the velocity increases exponentially, however for large values of λ, the oscillatory behaviour occurs.

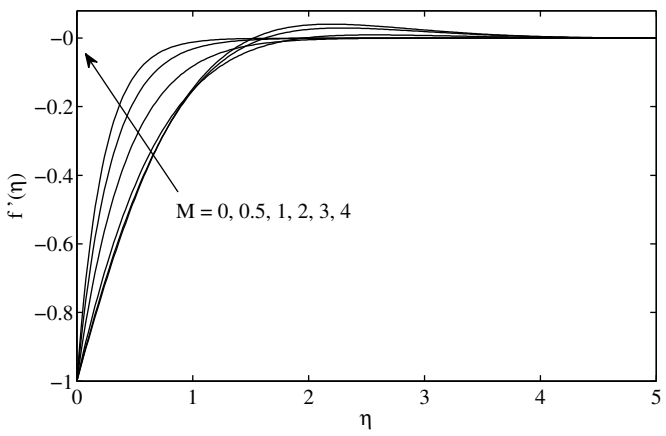

Figure 5.4: Effects of M on $f'(\eta)$ when $s = 3, \lambda = 2$

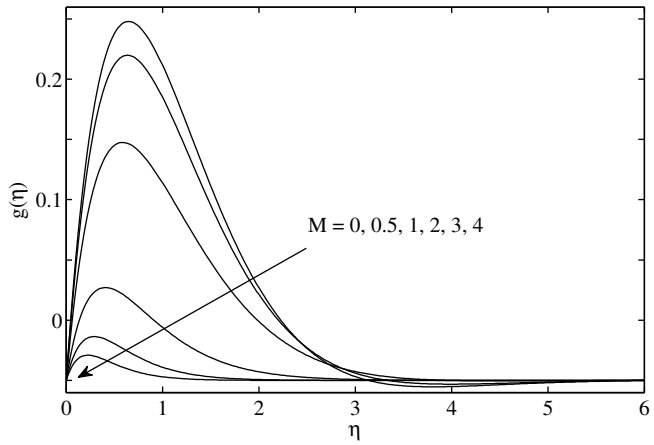

Figure 5.5: Effects of M on $g(\eta)$ when $s = 3, \lambda = 2$

Furthermore, the effects of the magnetic parameter M on $f'(\eta)$ and $g(\eta)$ are given in Figs. 5.4 and 5.5, respectively. Both figures show that the boundary layer thickness is smaller as M increases. This phenomenon is closely related to the relationship between the magnetic field and the resulting drag force called Lorentz force. The increase in magnetic field increases the Lorentz force and hence slows the fluid flow along the shrinking surface.

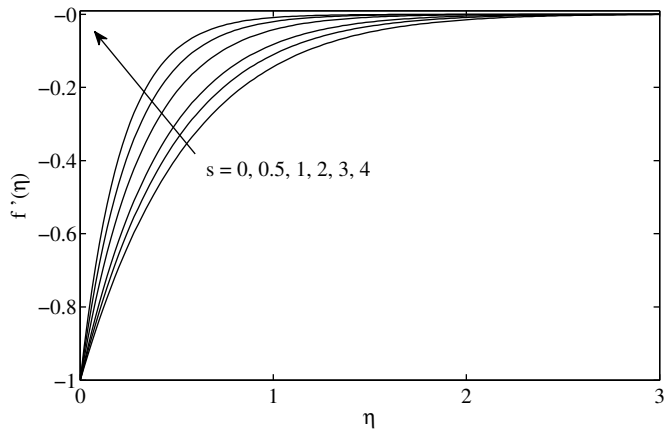

Figure 5.6: Effects of s on $f'(\eta)$ when $M = 2, \lambda = 2$

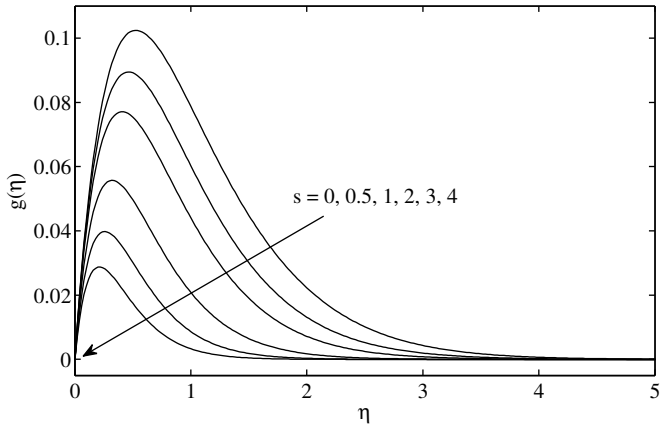

Figure 5.7: Effects of s on $g(\eta)$ when $M = 2, \lambda = 2$

In additional, graphs of $f'(\eta)$ and $g(\eta)$ for some values of suction parameter s are given in Figs. 5.6 and 5.7. Both figures display the reduction in boundary layer thickness with the increase of s. This reduction is caused by the suction itself, which plays a role in reducing the drag force, which in turns reducing the boundary layer thickness so that the boundary layer separation can be avoided.

5.5 Conclusion

In this study, the problem of magnetohydrodynamic rotating viscous flow over a permeable shrinking sheet is considered and solved numerically by using a Keller-box method. The effects of the governing parameters; namely suction parameter s, magnetic parameter M and rotating parameter λ have been presented graphically and discussed in detail. It is discovered that the boundary layer thickness for both velocity and lateral velocity profiles are decreasing with the increase of all governing parameters.

Acknowledgement

The authors would like to thank Universiti Putra Malaysia for the funding in the form of research grant (GP-IPM/2018/9619000).

Bibliography

[1] Sakiadis BC (1961) Boundary layer behaviour on continuous solid surfaces, *AIChE J* **7**, 26–28.

[2] Crane LJ (1970) Flow past a stretching plate. *Z Angew Math Mech* **21**, 645–647.

[3] McLeod JB, Rajagopal KR (1987) On the uniqueness of flow of a Navier-Stokes fluid due to a stretching boundary. *Arch Rat Mech Anal* **98**, 385–393.

[4] Gupta PS, Gupta AS (1977) Heat and mass transfer on a stretching sheet with suction or blowing. *Can J Chem Eng* **55**, 744–746.

[5] Magyari E, Keller B (2000) Exact solutions for self-similar boundary-layer flows induced by permeable stretching surfaces. *European Journal of Mechanics: B/Fluids* **19**, 109–122.

[6] Pavlov KB (1974) Magnetohydrodynamic flow of an incompressible viscous fluid caused by the deformation of a plane surface. *Magnitnaya Hidrodinamika* **4**, 146–147.

[7] Anderson Jr JD (1995) *Computational Fluid Dynamics: The Basics with Applications*, McGraw Hill Inc, NY.

[8] Nazar R, Amin N, Pop I (2004) Unsteady boundary layer flow due to a stretching surface in a rotating fluid. *Mech Res Commun* **31**, 121–128.

[9] Ishak A, Nazar R, Pop I (2008) Hydromagnetic flow and heat transfer adjacent to a stretching vertical sheet. *Heat and Mass Transfer* **44**, 921–927.

[10] Wang CY (1988) Stretching a surface in a rotating fluid. *J Appl Phys (ZAMP)* **39**, 177–185.

[11] Abbas Z, Javed T, Sajid M, Ali N (2010) Unsteady MHD flow and heat transfer on a stretching sheet in a rotating fluid. *Journal of the Taiwan Institute of Chemical Engineers* **41**, 644–650.

[12] Wang CY (1990) Liquid film on an unsteady stretching sheet. *Quart Appl Math* **48**, 601–610.

[13] Miklavcic M, Wang CY (2006) Viscous flow due to a shrinking sheet. *Quart Appl Math* **64**, 283–290.

[14] Sajid M, Javed T, Hayat T (2008) MHD rotating flow of a viscous fluid over a shrinking surface. *Nonlinear Dyn* **51**, 259–265.

[15] Hayat T, Javed T, Sajid M (2008) Analytic solution for MHD rotating flow of a second grade fluid over a shrinking surface. *Physics Letters A* **372**, 3264–3273.

[16] Faraz N, Khan Y (2011) Analytical solution of electrically conducted rotating flow of a second grade fluid over a shrinking surface. *Ain Shams Engineering Journal* **2**, 221–226.

[17] Jusoh R, Nazar R, Pop I (2018) Magnetohydrodynamic rotating flow and heat transfer of ferrofluid due to an exponentially permeable stretching/shrinking sheet. *Journal of Magnetism and Magnetic Materials* **465**, 365–374.

[18] Nasir S, Islam S, Gul T, Shah Z, Khan MA, Khan W, Khan AZ, Khan S (2018) Three-dimensional rotating flow of MHD single wall carbon nanotubes over a stretching sheet in presence of thermal radiation. *Applied Nanoscience* **8(6)**, 1361–1378.

[19] Keller HB, Cebeci T (1972) Accurate numerical methods for boundary layer flows, II: Two-dimensional turbulent flows. *AIAA Journal* **10**, 1193–1199.

[20] Yih KA (1999) Free convection effect on MHD coupled heat and mass transfer of a moving permeable vertical surface. *International Communications in Heat and Mass Transfer* **26**, 95–104.

[21] Ishak A, Nazar R, Pop I (2007) Magnetohydrodynamic stagnation-point flow towards a stretching vertical sheet in a micropolar fluid. *Magnetohydrodynamics* **43**(1), 83–97.

[22] Lok YY, Ishak A, Pop I (2011) MHD stagnation-point flow towards a shrinking sheet. *International Journal of Numerical Methods for Heat and Fluid Flow* **21**, 61–72.

[23] Rosali H, Ishak A, Nazar R, Pop I (2015) Rotating flow over an exponentially shrinking sheet with suction. *Journal of Molecular Liquids* **211**, 965–969.

[24] Daniel YS, Aziz ZA, Ismail Z, Salah F (2018) Effects of slip and convective conditions on MHD flow of nanofluid over a porous nonlinear stretching/shrinking sheet. *Australian Journal of Mechanical Engineering* **16(3)**, 213–229.

[25] Cebeci, T., Bradshaw, P. (1977) Momentum Transfer in Boundary Layers. New York: Hemisphere Publishing Corporation.

[26] Cebeci, T., Bradshaw, P. (1977) P. Physical and Computational Aspects of Convective Heat Transfer. New York: Springer-Verlag.

[27] Na, T.Y. (1979) Computational Methods in Engineering Boundary Value Problem. New York: Academic Press.

Chapter 6

The Effects of Assisting Flow and Buoyancy Ratio Parameters on Magnetohydrodynamics Newtonian Fluid Flow

Shahanaz Parvin[1], **Siti Suzilliana Putri Mohamed Isa**[1,2,*], Norihan Md Arifin[1,3]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of foundation Studies For Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: ctsuzilliana@upm.edu.my

Abstract

This study describes magnetohydrodynamics (MHD) Newtonian fluid flow caused by an exponentially streching sheet, and subjected to the parameters such as assisting flow and buoyancy ratio. The governing basic equations (flow, momentum, energy and concentration equations) are converted to nonlinear ordinary differential equations (ODEs) by using non-similarity method. Subsequently, the ODE are solved numerically by bvp4c program in Matlab software. Finally, the numerical results for the skin friction coefficient, the local Nusselt number and the local Sherwood number are obtained. Moreover, the variations of the velocity, temperature and concentration profiles are presented. The characteristis of the flow, heat and mass transfer are discussed in details.

Keywords: magnetohydrodynamics, stretching sheet, assisting flow, buoyancy ratio, Newtonian fluid.

6.1 Introduction

Mixed convection, which is defined as the combination of forced and natural convection exists when both of these convection mechanisms act together to transfer heat. Forced convection occurs when the fluids are forced to move, in order to enhance the heat transfer. This forcing can be done by using ceiling fan, a pump, suction device, or other. However, natural convection is a type of flow in which the fluid motion is generated by gravity (some regions of the fluid are heavier than the other regions). Therefore, there are two components in mixed convection: assisting and opposing

flows. Two-dimensional mixed convection with aiding flow occurs when the buoyant motion and the forced motion are in the same direction, which causes the natural convection to induce forced convection. Besides, two-dimensional mixed convection with opposing flow exists when natural convection acts in the opposite direction of the forced convection. The example of the opposing flow can be described by considering a fan forcing air upward over a cold plate. In this situation, the natural motion of the cold air is supposed to be fall due to the buoyant force. However, air is directed upward and opposes the natural motion of cold air [1]. As a result, the industrial applications of mixed convection can be observed in crystal growth, nuclear reactors and chemical processing [2].

The industrial applications of the fluid flow due to a stretching sheet are the production of glass fibre, paper and polymer sheet [3]. In addition, the multiple numerical solutions keeps happen in the mathematical model of convection with the presence of stretching sheet. As a results, a lot of findings are reported due to this type of flow, which induces convection. The dual numerical solutions for the stretching sheet model, with the presence of thermal radiation and slip effects are discussed Sulochana and Sandeep [4]. Naganthran and Nazar [5] described the dual numerical solutions in the magnetohydrodynamics (MHD) stagnation-point flow in a porous medium. Triple solutions have been arised in the problem of magnetohydrodynamic mixed convection which is subjected by convective boundary condition [6]. The report on dual solutions for the Prandtl fluid containing nanoparticles is presented by Mahanthesh and Gireesha [8]. Recently, dual solutions in stretching sheet model on a Casson fluid reported by Hamid et al. [9].

As a result, this paper describes dual numerical solutions of magnetohydrodynamics (MHD) Newtonian fluid flow induced by an exponentially stretching sheet, and controlled by the various values of assisting flow and buoyancy ratio parameters. The findings is obtained by using bvp4c Matlab program. This paper contains four large sections: 1) Introduction, 2) Mathematical Formulation, 3) Results and Discussion, and 4) Conclusion.

6.2 Mathematical Formulation

Consider the two-dimensional incompressible, viscous and electrically conducting magnetohydrodynamics Newtonian fluid over a permeable shrinking surface. Shrinking sheet is located along the x-axis, whereas transverse magnetic field is located at y-axis. For both parameters T and C refering to conditions at the outer edge of the boundary layer and at the wall is describe by the subscripts of ∞ and w. The mathematical formulation which represent the modeled problem written as:

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} = 0, \tag{6.1}$$

$$u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} = \nu\frac{\partial^2 u}{\partial y^2} + g\beta_T(T - T_\infty) + g\beta_C(C - C_\infty) + \frac{\sigma B_0^2}{\rho}u, \tag{6.2}$$

$$u\frac{\partial T}{\partial x} + v\frac{\partial T}{\partial y} = \alpha\frac{\partial^2 T}{\partial y^2} + \frac{DK_T}{C_s C_p}\frac{\partial^2 C}{\partial y^2}, \tag{6.3}$$

$$u\frac{\partial C}{\partial x} + v\frac{\partial C}{\partial y} = D\frac{\partial^2 C}{\partial y^2} + \frac{DK_T}{T_m}\frac{\partial^2 T}{\partial y^2}. \tag{6.4}$$

The appropriate boundary conditions are

$$u = u_w(0) = \lambda U_0 \exp(x/L), \quad v = v_w(0),$$

$$T_w(0) = T_\infty + T_0 \exp(x/2L), \quad C_w(0) = C_\infty + C_0 \exp(x/2L)$$

$$u \to 0, \quad T \to T_\infty, \quad C \to C_\infty \quad \text{as} \quad y \to \infty. \tag{6.5}$$

The term $\exp(x/2L)$ in temperature T_w and concentration distribution C_w are used in this [10, 11] for the case of two-dimensional flow exponential variation with the presence of Soret- Dufour effects and when concentration equation included in governing equations.

In this study, the stream function is written as:

$$\psi(x, y) = (2\nu L U_0)^{1/2} \exp(x/2L) f(\eta), \quad u = \frac{\partial \psi}{\partial y}, \quad v = -\frac{\partial \psi}{\partial x}. \tag{6.6}$$

Introducing new similarity variables:

$$\theta(\eta) = \frac{T - T_\infty}{T_w - T_\infty}, \quad \phi(\eta) = \frac{C - C_\infty}{C_w - C_\infty}, \quad \eta = y \left(\frac{U_0}{2\nu L} \right)^{1/2} exp(x/2L),$$

$$u = U_0 \exp(x/L) f'(\eta), \quad v = -\left(\frac{\nu U_0}{2L} \right)^{1/2} \exp(x/2L)[f(\eta) + \eta f'(\eta)] \tag{6.7}$$

When (10.7) is substituted into (10.1), the continuity equation is satisfied, proved that our similarity variables is accepted and can be proceed to produce ordinary differential equations ODE. Then, substituted (10.7) into (10.2)–(10.5), the following form are occured:

$$f''' + ff'' - 2(f')^2 + 2Ri \left[\exp\left(\tfrac{-3X}{2} \right) \right] (\theta + N\phi) - 2H[\exp(-X)] f' = 0. \tag{6.8}$$

$$\frac{1}{Pr} \theta'' + f\theta' - f'\theta + Db\phi'' = 0. \tag{6.9}$$

$$\frac{1}{Sc} \phi'' + f\phi' - f'\phi + Sr\theta'' = 0. \tag{6.10}$$

$$f'(\eta) = \lambda, \quad f(\eta) = S, \quad \theta(\eta) = 1, \quad \phi(\eta) = 1 \quad \text{at} \quad \eta = 0,$$
$$f'(\eta) \to 0, \quad \theta(\eta) \to 0, \quad \phi(\eta) \to 0, \quad \text{at} \quad \eta = \infty, \tag{6.11}$$

where the parameters involved in this problem are stretching parameter, λ with $\lambda > 0$,thermal Grashof number Gr, Reynolds number Re, mixed convection parameter $Ri = Gr/Re^2$, magnetic field parameter $H = 2\sigma L B_0^2/\rho U_0$, dimensionless coordinate along the plate parameter $X = x/L$, buoyancy ratio $N = \beta_c(C_0 - C_\infty)/\beta_T(T_0 - T_\infty)$, Prandtl number $Pr = \upsilon/\alpha$, Schmidt number $Sc = \upsilon/D$, Soret number $Sr = DK_T(T_0 - T_\infty)/T_m\upsilon(C_0 - C_\infty)$, Dufour number $Db = DK_T(C_0 - C_\infty)/C_sC_p\upsilon(T_0 - T_\infty)$ and suction parameter $S = (v_w(x)/\exp(x/2L))\sqrt{2L/\upsilon U_0}$. The opposing flow is when $Ri < 0$. Otherwise, the positive Ri indicates the case of aiding flow.

The physical parameters of skin friction coefficient C_f, local Nusselt number Nu_x and local Sherwood number Sh_x are presented as follow:

$$
\begin{aligned}
c_f &= \left(\frac{\mu}{\rho U_0^2}\right)\left(\frac{\partial u}{\partial y}\right), \\
Nu_x &= \left(\frac{L}{T_w - T_\infty}\right)\left(-\frac{\partial T}{\partial y}\right)_{y=0} \\
Sh_x &= \left(\frac{L}{C_w - C_\infty}\right)\left(-\frac{\partial C}{\partial y}\right)_{y=0}
\end{aligned} \tag{6.12}
$$

Substituting (10.7) into (10.12), then we get

$$
\begin{aligned}
C_f\sqrt{2Re_x}\exp\left(\frac{-3X}{2}\right) &= f''(0), \\
Nu_x\sqrt{\frac{2}{Re_x}}\exp\left(\frac{-X}{2}\right) &= -\theta(0), \\
Sh_x\sqrt{\frac{2}{Re_x}}exp\left(\frac{-X}{2}\right) &= -\phi'(0).
\end{aligned} \tag{6.13}
$$

6.3 Results and Discussion

The system of exponentially ordinary differential equations (10.8), (10.9) and (10.10) together with the boundary conditions (10.11) are solved numerically using Matlab programming. The accuracy of our numerical method is reached by comparing numerical data obtained with previous investigators, showed in Table 10.1. Table 10.1 shows the comparison of skin friction coeffcient $f''(0)$, local Nusselt number $-\theta(0)$ and local Sherwood number $-\phi(0)$ between our data and with Srinivasacharya and Ram Reddy [10]. In Table 10.1, the comparison is made for $H = 0$ and $N = 0.5$ for various values of Ri, Sr, Db and X. As a conclusion, the present value of the first solution for $f''(0)$, $-\theta(0)$ and $-\phi(0)$ are in good agreement with those obtained by Srinivasacharya and RamReddy [10]. Therefore, the good comparison gives as much confidence in our theoretical study and numerical computation.

Table 6.1: Effects of skin friction, heat and mass transfer coeffcients for various values of Ri when $Sr = 2.0$, $Db = 0.03$, $X = 3.0$, $Pr = 1.0$, $Sc = 0.22$,$N = 0.5$ and $H = 0$.

Ri	$f''(0)$		$-\theta'(0)$		$-\phi'(0)$	
	(a)	(b)	(a)	(b)	(a)	(b)
-0.5	-1.29399	-1.29384	0.94867	0.94896	-0.04882	-0.04638
-0.1	-1.28408	-1.29619	0.95561	2.65383	-0.03622	-1.12709
0.5	-1.27097	-1.29463	0.96278	0.86285	-0.02553	0.07932
3.0	-1.22243	-1.22249	0.98297	0.98290	-0.00241	-0.00207

Note :
(a)Srinivasacharya and RamReddy [10]
(b)Present

The figures for the function $f'(\eta)$ which corresponds to velocity, $\theta(\eta)$ which corresponds to temperature and $\phi(\eta)$ which corresponds to concentration are drawn

against η for different values of the parameter S, H, Ri, Sr, N and Db. All figures are correspond to the two-dimensional stretching cases in which it consists of two different solutions.

Figure 10.1, Figure 10.2 and Figure 10.3 show the influence of mixed convection parameter, Ri on velocity, temperature and concentration profiles respectively in the flow induced by stretching sheet $\lambda = 1$. From Figure 10.1, it is observed that as the value of mixed convection parameter, Ri rises, the values of velocity as well as the boundary layer thickness increase for the first solution. Besides, for the second solution, the boundary layer thickness increases for the small value of η. The temperature distribution decreases with the increasing value of mixed convection parameter, Ri for both first and second solution as observed in Figure 10.2. The concentration profile of the fluid has a significant decreases with mixed convection parameter for first solution, while for the second solution, the concentration profile increases for the small value of η and decreases for large value of η as illustrated in Figure 10.3.

Figure 10.4, Figure 10.5 and Figure 10.6 show the influence of buoyancy parameter, N on velocity, temperature and concentration profiles respectively in the flow induced by stretching sheet $\lambda = 1$. When the buoyancy value N increases, it is observed that the values of velocity as well as the boundary layer thickness increase for the first solution. However, for the second solution, the boundary layer thickness increases for a small value of η while it decreases as the value of η increases as depicted in Figure 10.4. From Figure 10.5, when the value of buoyancy parameter N increases, the temperature distribution decreases for the small values of η for both first and second solution. Moreover, when the value of N increases, the concentration profile of the fluid is decreasing for the first solution, while it is increasing for the second solution as shown in Figure 10.6.

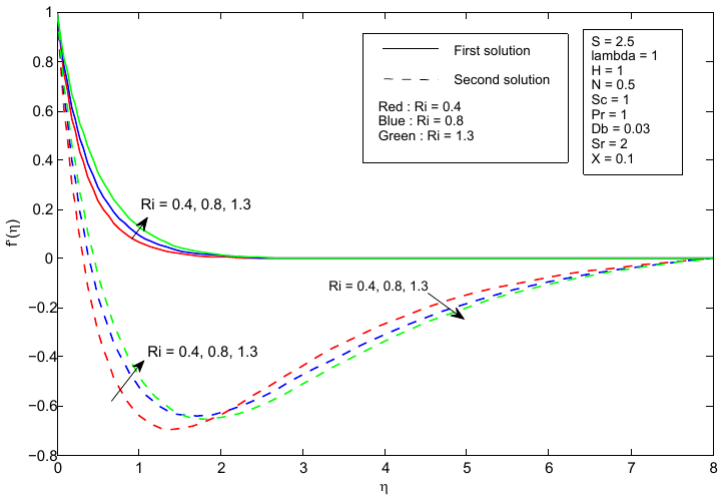

Figure 6.1: Different values of mixed convection parameter, Ri on velocity.

It is clear from Fig. 10.1 and 10.4 that velocity distribution is increased for the increment of mixed convection parameter Ri and buoyancy ratio parameter N. This is due to the fact that higher rate of mixed convection parameter is caused by

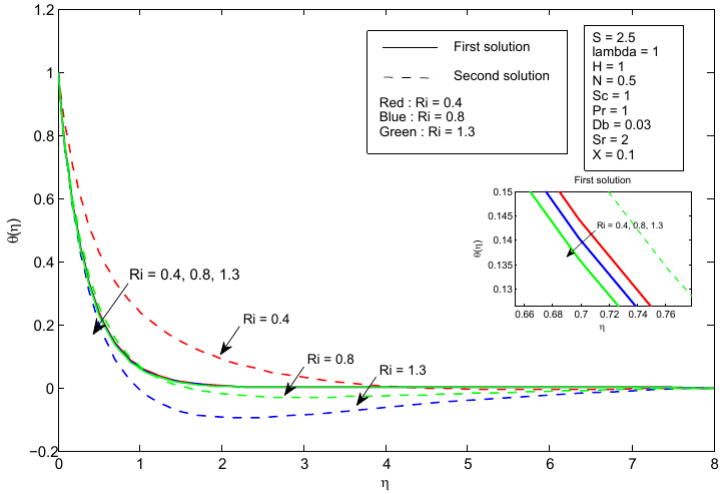

Figure 6.2: Different values of mixed convection parameter, Ri on temperature.

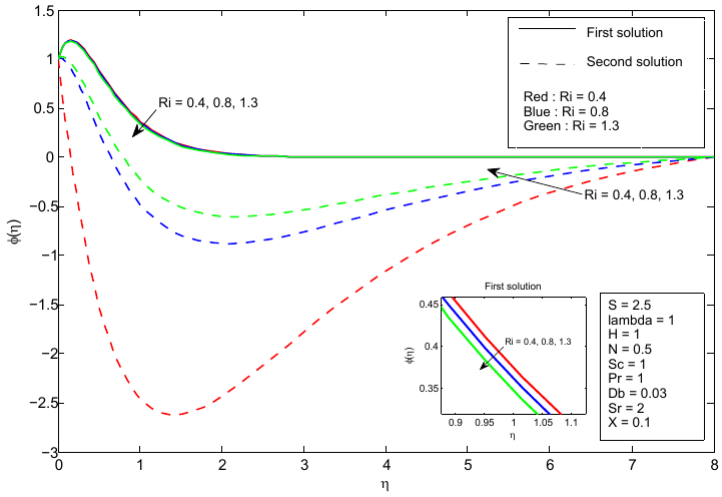

Figure 6.3: Different values of mixed convection parameter, Ri on concentration.

a greater buoyancy effects. Therefore, the fluid flow is accelerated and the instantaneous velocity increases. Fig. 10.2, 10.3, 10.5 and 10.6 show that the temperature and concentration decrease with increasing values of mixed convection parameter Ri and buoyancy ratio parameter N. When parameter Ri (i.e. buoyancy effects) increase, it contributes to the increment of the convection cooling effect and hence the temperature reduces. The tabulation of data skin friction coefficient, local Nusselt number and local Sherwood number are appropriate for the controlling parameters Ri and N by the small increment. Therefore, the physical effect also can be observed for the small ranges of Ri and N.

Table 10.2 shows the variation of $f''(0)$, $-\theta'(0)$ and $-\phi(0)$ for different values of mixed convection parameter Ri when $\lambda = 1$. From Table 10.2, as the value of mixed convection parameter Ri increases, the variation of $f''(0)$, $-\theta'(0)$ and $-\phi(0)$ increase for the first solution. However, for the second solution, $f''(0)$ is increasing and $-\theta'(0)$ is decreasing due to the impact of Ri.

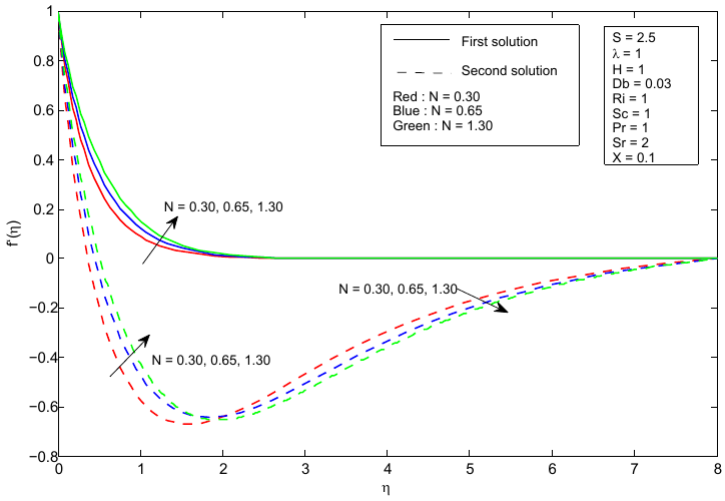

Figure 6.4: Different values of buoyancy parameter, N on velocity.

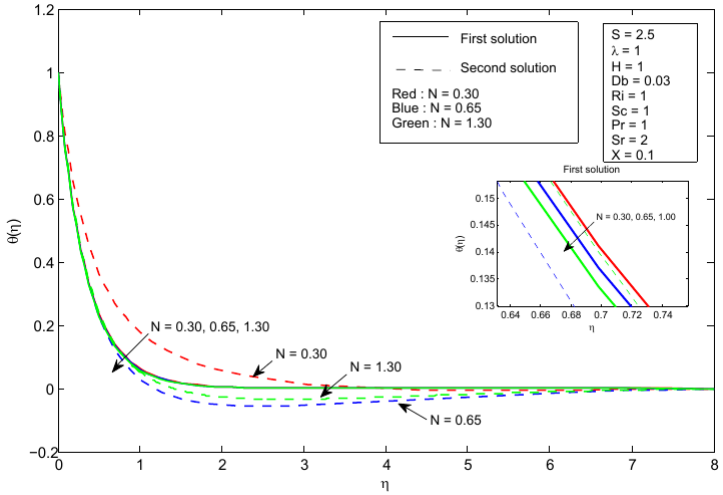

Figure 6.5: Different values of buoyancy parameter, N on temperature.

Table 6.2: Different values of mixed convection parameter Ri for $\lambda = 1$ and when $S = 2.5$, $N = 0.5$, $H = 1$, $Sc = 1$, $Pr = 2$, $Db = 0:03$, $Sr = 2$ and $X = 0:1$.

Solutions	Ri	$f''(0)$	$-\theta'(0)$	$-\phi(0)$
First	0.4	-3.061843418	2.927831454	-2.670440837
	0.8	-2.672006544	2.951646859	-2.644623301
	1.3	-2.204957221	2.978680269	-2.616465913
Second	0.4	-4.808811232	2.047790323	6.843471891
	0.8	-4.087089124	2.998250705	-0.497992296
	1.3	-3.538577652	2.815009227	-0.905391446

The values of $f''(0)$, $-\theta'(0)$ and $-\phi(0)$ is tabulated in Table 6.3 for $S = 2.5$, $Ri = 1$, $H = 1$, $Sc = 1$, $Pr = 2$, $Db = 0.03$, $Sr = 2$ and $X = 0.1$ with different values of

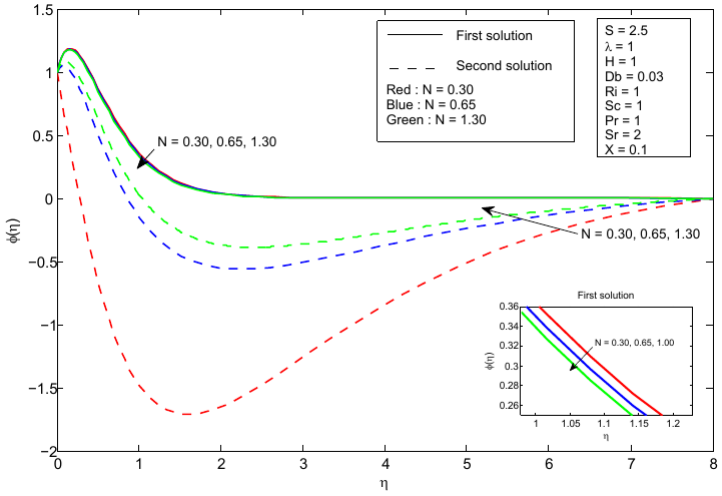

Figure 6.6: Different values of buoyancy parameter, N on concentration.

buoyancy parameter, N for $\lambda = 1$. The first solution shows the increments in the values of $f''(0)$, $-\theta'(0)$ and $-\phi(0)$ as the value of buoyancy parameter increases. However, both $f''(0)$ and $-\theta'(0)$ are increased and $-\phi(0))$ decreases for second solution.

Table 6.3: Different values of mixed convection parameter N for $\lambda = 1$ and when $S = 2.5$, $Ri = 1$, $H = 1$, $Sc = 1$, $Pr = 2$, $Db = 0:03$, $Sr = 2$ and $X = 0:1$.

Solutions	N	$f''(0)$	$-\theta'(0)$	$-\phi'(0)$
First	0.30	-2.690029688	2.948756169	-2.649158325
	0.65	-2.330926409	2.972797940	-2.621483604
	1.00	-1.987391865	2.994705802	-2.597170794
Second	0.30	-4.250492382	2.349396835	3.470653059
	0.65	-3.642519010	2.932549060	-1.318807235
	1.00	-3.210882376	2.901448305	-1.737593695

Acknowledgement

The present research was partially supported by the Putra Grant with Project Number GP-IPM/2018/9596900.

6.4 Conclusion

The problem of MHD Newtonian flow and heat transfer in the boundary layers on exponentially permeable stretching sheet with the presence of Soret and Dufour effects are solved numerically. The effectiveness of some parameter which are Soret number,Sr, Dufour number,Db, magnetic parameter,H, mixed convection parameter,Ri, buoyancy parameter,N, and suction parameter,S on velocity, temperature and concentration variation are tested by increasing the value of each

parameter. As a conclusion, it would appear that the values of $f''(0)$, $-\theta'(0)$ and $-\phi(0)$ is increasing as the value of mixed convection parameter and buoyancy parameter increases.

Bibliography

[1] Cengal, Yunus A., Afshin J., Ghajar. (2007), *Heat and Mass Transfer (4 ed.)*, McGraw-Hill, 548-–549.

[2] Mojumder S., Saha S., Rahman M. R., Rahman M. M., Rabbi K. M., Ibrahim T. A. (2017), *Numerical Study on Mixed Convection Heat Transfer in a Porous L-Shaped Cavity. Engineering Science and Technology* Eng. Sci. Technol. Int J. Vol 20(1), 272—282.

[3] Isa S. S. P. M., Arifn N. M., and Farooq U. (2019), *Effect of Soret and Dufour Numbers on Double Diffusive Mixed Convection Boundary Layer Flow Induced by a Shrinking Sheet*, Journal of Physics: Conf. Series. Vol 1298(1), 012024.

[4] Sulochana C., and Sandeep N. (2015), *Dual Solutions for Radiative MHD Forced Convection Flow of a Nanofluid over a Slandering Stretching Sheet in Porous Medium.*, Journal of Naval Architecture and Marine Engineering. Vol 12(2), 115–124.

[5] Naganthran K., and Nazar R. (2017), *Dual Solutions of MHD Stagnation-Point Flow and Heat Transfer Past a Stretching/Shrinking Sheet in a Porous Medium.*, AIP Conference Proceedings, Vol 1830(1).

[6] Isa S. S. P. M., Arifin N. M., Nazar R., Bachok N. and Ali F. M.(2017), *The Effect of Convective Boundary Condition on MHD Mixed Convection Boundary Layer Flow Over an Exponentially Stretching Vertical Sheet.*, IOP Conf. Series: Journal of Physics: Conf. Series. Vol 949(1),012016

[7] Mahanthesh B., and Gireesha B. J. (2018), *Dual Solutions for Unsteady Stagnation-Point Flow of Prandtl Nanofluid past a Stretching/shrinking Plate.*, Defect and Diffusion Forum, Vol 388, 124–134.

[8] Hamid M., Usman M., Khan Z.H., Ahmad R., Wang W. (2019), *Dual Solutions and Stability Analysis of Flow and Heat Transfer of Casson Fluid over a Stretching sheet.*, Physics Letters A, Vol 383(20), 2400–2408.

[9] Srinivasacharya, D. and RamReddy, Ch. (2011), *Soret and Dufour Effects on Mixed Convection from an Exponentially Stretching Surface.*, International Journal of Nonlinear Science, Vol 12(1),60–68.

[10] Sreenivasulu, P. and Redddy, N., B. (2012), *Soret and Dufour Effects on Boundary Layer Flow past an Exponential Stretching Sheet with Thermal Radiation and Viscous Dissipation.*, Appl. Math., vol (51), 10809-–10816.

Chapter 7

The Exponential Variation of Heated Extending Sheet in Casson Fluid Flow

Kartini Ahmad[1,*], Siti Suzilliana Putri Mohamed Isa[2,3]

[1] Department of Science in Engineering, Kulliyyah of Engineering, International Islamic University Malaysia, Gombak,50728 Kuala Lumpur, Malaysia.
[2] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM, Serdang Selangor, Malaysia.
[3] Centre of foundation Studies For Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: kartini@iium.edu.my

Abstract

The mathematical model of the following case is developed: The magnetohydrodynamics (MHD) of Casson fluid flow with heated at the surface due to Newtonian heating. This study takes into account in a concentrated Casson fluid flow with existence of thermal radiation. Similarity transformation is used, to convert the governing equations (continuity, momentum, energy, mass diffusion equations) into ordinary differential equations (ODE). Later on, these ODE is determined by applying the finite-difference method. The profiles of velocity, temperature, concentration and concentration gradient are depicted for certain values of controlling parameters. The consenquences of the controlling parameters on the system are described in details.

Keywords: magnetohydrodynamics, Casson fluid, Newtonian heating, extending/stretching sheet.

7.1 Introduction

The broad applications of non-Newtonian fluid is widely used in the field of cosmetics, pharmaceuticals, chemicals, oil, gas, food and several others. Therefore, the models of non-Newtonian fluid have been developed such as Brinkman type, Jeffrey, Maxwell, Bingham plastic, Oldroyd-B, power law, second grade, viscoplastic and Walters-B [1]. However, the most popular model of non-Newtonian fluid is known as Casson model [2], and the pioneer investigator indicated that the yield stress for blood is nonzero at low shear rates. To be noted, Casson fluid model is extensively used for modeling blood flow in narrow arteries [3, 4]. Besides, the model of

boundary layer flow, the rate transfer of heat and mass beyond an extending surface has large contributions in the following: condensation process of metallic plate in a cooling bath, aerodynamic extrusion of plastic sheets and extrusion of a polymer sheet from a dye [5]. Moreover, the final products of industrial field are significantly influenced by the extending/stretching rate, the cooling rate in the process and the process of extending sheet itself. As a results, many studies have been conducted to carried out numerical study to the effects of extending sheet in Casson fluid. The Hall effects on the flow of Casson fluid due to an extending sheet with thermal radiation and mixed convection are studied by Bilal Ashraf et al. [6]. Ullah et al. [7] investigated the heat and mass transfer free convection flow of Casson fluid over an extending sheet in the presence of chemical reaction. The impact of melting heat transfer in a porous medium on magnetohydrodynamic (MHD) Casson fluid flow over an extending sheet, influenced by thermal radiation is investigated by Mabood and Das [8]. Abd El-Aziz and Afifi [9] reported the numerical analysis of the MHD Casson fluid over an extending surface with velocity slip factor on the impacts of entropy generation and Hall current.

Recently, Newtonian heating gets more interest instead of constant surface temperature because of its effectiveness in many physical situations. Newtonian heating is usually termed conjugate convective flow is defined as the heat transfer rate from the bounding surface with a finite heat capacity is proportional to the local surface temperature [10]. Merkin [11] was the first who studied the characteristics of Newtonian heating, which is one type of temperature distributions at wall. The influence of Newtonian heating with existence of thermal radiation and chemical reaction in unsteady hydromagnetic flow of a Casson fluid past a vertical plate is studied by Das et al. [12]. Hussanan et al [13] investigated the non-Newtonian Casson fluid on unsteady heat transfer flow over an oscillating vertical plate with Newtonian heating on the wall in the presence of thermal radiation. Further, Ullah et al. [14] performed numerical analysis of MHD flow of non-Newtonian fluid under the effect of slip condition over an extending sheet saturated in porous medium with Newtonian heating. Recently, Ahmad et al. [15] analyzed Casson fluid flow over extending sheet in the presence of viscous dissipation and Newtonian heating.

As a conclusion, this paper concentrates on the magnetohydrodynamics (MHD) of Casson fluid flow over a heated surface due to Newtonian heating and thermal radiation. Results are presented through graphs of velocity, temperature, concentration and concentration gradient profiles. This study is organized by the following: Section 2 is Problem Formulation, Section 3 is Results and Discussion, and final section which is Section 5 is Conclusion.

7.2 Problem Formulation

Two-dimensional concentrated Casson fluid flow over a heated extended sheet is investigated. The Casson fluid is electrically conducting and radiating. A non-uniform magnetic field $B(x) = B_o e^{(Nx/2L)}$ is imposed transverse to the exponentially extending sheet with velocity $u_w = U_o e^{(Nx/L)}$ and the concentration of the Casson fluid near the sheet is $C_w = C_\infty + C_o e^{(Nx/2L)}$. B_o, U_o and C_o, are the reference magnetic, velocity and concentration respectively, C_∞ is the concentration of the Casson fluid in the ambient flow, N is the exponential parameter and L is the reference length. The sheet is heated due to Newtonian heating $h_s = h_o e^{(Nx/2L)}$ where h_o is constant. Fig. 7.1 illustrates the flow configuration of this problem.

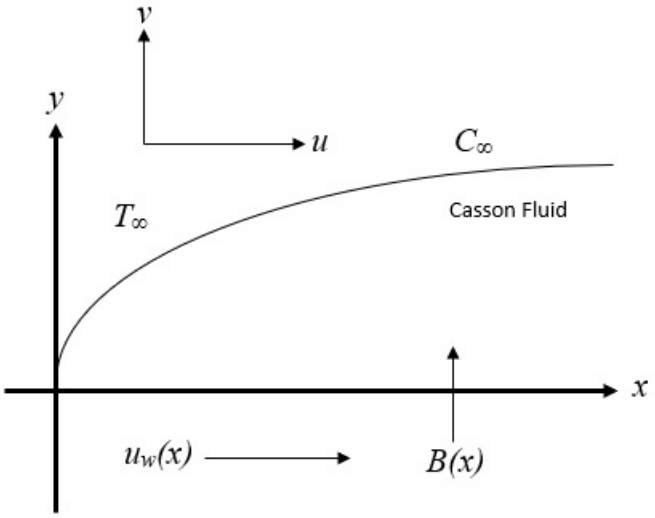

Figure 7.1: A sketch of physical model and coordinate system

Making use of the Boussinesq together with boundary layer approximations, the developed governing boundary layer equations are:

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} = 0, \tag{7.1}$$

$$u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} = \nu\left(1 + \frac{1}{\beta}\right)\frac{\partial^2 u}{\partial y^2} - \frac{\sigma B^2(x)}{\rho}u, \tag{7.2}$$

$$u\frac{\partial T}{\partial x} + v\frac{\partial T}{\partial y} = \frac{1}{\rho c_p}\left(k\frac{\partial^2 T}{\partial y^2} - \frac{\partial q_r}{\partial y}\right) \tag{7.3}$$

$$u\frac{\partial C}{\partial x} + v\frac{\partial C}{\partial y} = D\frac{\partial^2 C}{\partial y^2}, \tag{7.4}$$

with boundary conditions:

$$u = u_w, \quad v = 0, C = C_w, \quad \frac{\partial T}{\partial y} = -h_s T(NH) \quad \text{at} \quad y = 0,$$

$$u \to 0, C \to C_\infty, T \to T_\infty, \quad \text{at} \quad y \to \infty. \tag{7.5}$$

Here, u and v are the velocity components with respect to the horizontal (x) and vertical (y)-axes, respectively. β is the non-Newtonian (Casson) fluid parameter, u is the kinematic fluid viscosity, σ is the electrical conductivity, ρ is the fluid density, T is the fluid temperature, D is the solutal diffusivity of the medium, c_p is the specific heat at constant pressure, k is the thermal conductivity, , q_r is the radiative heat flux given by the Rosseland approximation [17, 18].

$$q_r = -\frac{4\sigma^*}{3k^*}\frac{\partial T^4}{\partial y} \tag{7.6}$$

where σ^* and k^* is refering to the Stefan-Boltzman constant and mean absorption, respectively and

$$T^4 \cong 4T_\infty^3 T - 3T_\infty^4 \tag{7.7}$$

Making use (10.6) and (10.7) into (10.3), we get

$$u\frac{\partial T}{\partial x}+v\frac{\partial T}{\partial y}=\frac{1}{\rho c_p}\left(k+\frac{16\sigma^* T_\infty^3}{3k^*}\right)\frac{\partial^2 T}{\partial y^2} \tag{7.8}$$

Applying the following transformation:

$$u=U_o e^{(Nx/L)}f'(\eta),\quad v=-N\sqrt{\frac{\upsilon U_o}{2L}}e^{(Nx/2L)}[f(\eta)+\eta f'(\eta)],$$

$$\eta=\sqrt{\frac{U_o}{2\upsilon L}}e^{(Nx/2L)}y,\quad \theta(\eta)=\frac{T-T_\infty}{T_\infty},\quad c=c_\infty+c_o e^{(Nx/2L)}\phi(\eta) \tag{7.9}$$

into (10.1), (10.2), (10.8) and (10.4) , we obtain

$$\left(1+\frac{1}{\beta}\right)f'''+Nff''-2N(f')^2-H^2f'=0, \tag{7.10}$$

$$\left(1+\frac{4}{3}R\right)\theta''+NPrf\theta'=0, \tag{7.11}$$

$$\phi''+NSc(f\phi'-f'\phi)=0, \tag{7.12}$$

while the boundary conditions (10.5) reduced to

$$f(0)=0,\quad f'(0)=1,\quad \theta'(0)=-Bi[1+\theta(0)],\quad \phi(0)=1,$$

$$f'(\infty)=0,\quad \theta(\infty)=0,\quad \phi(\infty)=0, \tag{7.13}$$

where prime indicates differentiation with respect to η, $H^2=\frac{2\sigma B_o^2 L}{\rho U_o}$ is the Hartmann number, $R=\frac{4\sigma^* T_\infty^3 L}{k^* k}$ is the radiation number, $Pr=\frac{\mu c_p}{k}$ is the Prandtl number, $Sc=\frac{\upsilon}{D}$ is the Schmidt number and $Bi=h_o\sqrt{\frac{2\upsilon L}{U_o}}$ is the conjugate parameter for the Newtonian heating.

7.3 Results and Discussion

From engineering perspective, the quantities of interest are the values of $f''(0)$, $\theta'(0)$ and $\phi'(0)$ which can be used to calculate the skin friction coefficient, the local Nusselt number and the local Sherwood number. Opting the method described by Cebeci and Bradshaw [16], Eqs. (10.10) – (10.13) are solved numerically for few values of Casson fluid parameter β, exponential extending parameter N, Hartmann number H^2, radiation parameter R, Schmidt number Sc, Biot number Bi when Prandtl number Pr is held fixed at 7. It is important to note that β, N and H^2 play significant role in determining the behaviour of the velocity f' (refer Eq. 10.10), which later affect the generated values of $f''(0)$. The rest of the parameters only react on the distribution where they occur, i.e R, Pr and Bi dominate only on the temperature distribution and Sc controls the concentration distribution due to decoupled of Eqs. (10.11) and (10.12).

Table 10.1 shows the values of $-f''(0)$, $\theta'(0)$ and $-\phi'(0)$ for certain values of H^2 and N when $\beta'=1$, $Pr=7$, $R=Sc=Bi=1.5$. The increment of Hartmann number H^2 increases the magnitude of $f''(0)$ and contrary phenomenon occur for $\theta'(0)$ and magnitude of $\phi'(0)$. The effect of exponentially extending parameter given by N gives the increment in both magnitude of $f''(0)$) and magnitude of $\phi'(0)$.

Table 7.1: Values of $f''(0)$, $\theta'(0)$ and $\phi'(0)$ for certain values of β, H^2 and N when $\beta' = 1$, $Pr = 7$, $R = Sc = Bi = 1.5$.

H^2	N	$-f''(0)$	$\theta(0)$	$-\phi(0)$
0.5	1	1.0369	78.6862	1.2867
	3	1.6490	33.9284	2.2680
	5	2.0886	25.7696	2.9387
5	1	1.8251	45.8619	1.0684
	3	2.2328	46.2877	2.1088
	5	2.5759	34.2546	2.8083

For the sake of brevity, the velocity, temperature, concentration and profiles of gradient concentration are only depicted for $\beta = R = Sc = Bi = 1$ for certain values of N when $H^2 = 0.5$ and 100 respectively, as displayed in Figs. 10.1-10.4.

To be noted, the exponential extending effect given by N makes no impact on the velocity distribution when the magnetic effect denoted by the Hartmann number H^2 is high ($= 100$). As we can see, the difference between the various values of N for the profiles of velocity, temperature and concentration (Figs.10.1-10.3) are significant for a very large H^2 (between 0.5 and 100). Unlike for $H^2 = 0.5$, the extending effect N reduces the velocity motion within the boundary layer as seen in Fig. 10.1. Opposite phenomenon occur for the temperature and concentration distributions given by $\theta(0)$ and $\phi(0)$ respectively, see Figs. 10.2-10.3. Here, the increment of H^2 increases the temperature and concentration within the layer. However, the increment of N decreases the temperature and concentration which in turned quicken the formation of the thermal and concentration boundary layer respectively. As the sheet is heated due to Newtonian heating, it is noted that the initial temperature of the sheet which is given by $\theta(0)$ starts at a certain value depending on the value of N and asymptotically decreases to zero once the thermal boundary layer is formed. The concentration gradient profile $\phi'(\eta)$ is depicted in Fig.10.4. Adding the effect of magnetic H^2 results to decrement of the $|\phi'(\eta)|$ at the sheet. The influence of N is seen to increase the $|\phi'(\eta)|$, regardless of the values of H^2. However, this scenario does not persistent; i.e at certain concentration gradient thickness η opposite behaviour eventuated.

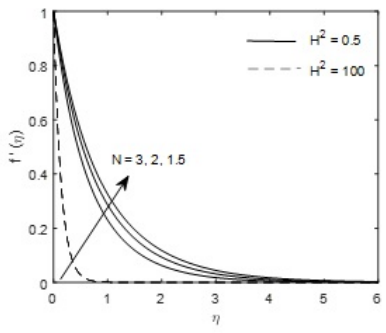

Figure 7.2: Velocity profile for certain values of N when $\beta = R$, $Sc = Bi = 1$.

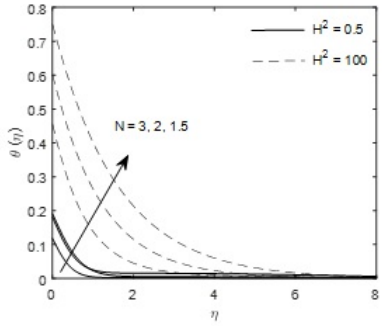

Figure 7.3: Temperature profile for certain values of N when $\beta = R$, $Sc = Bi = 1$.

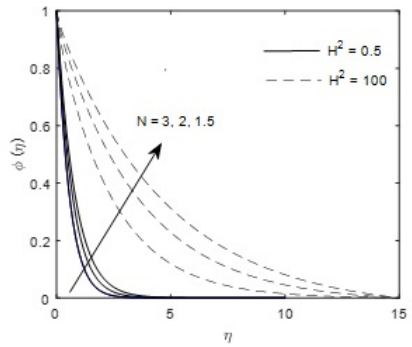

Figure 7.4: Concentration profile for certain values of N when $\beta = R$, $Sc = Bi = 1$.

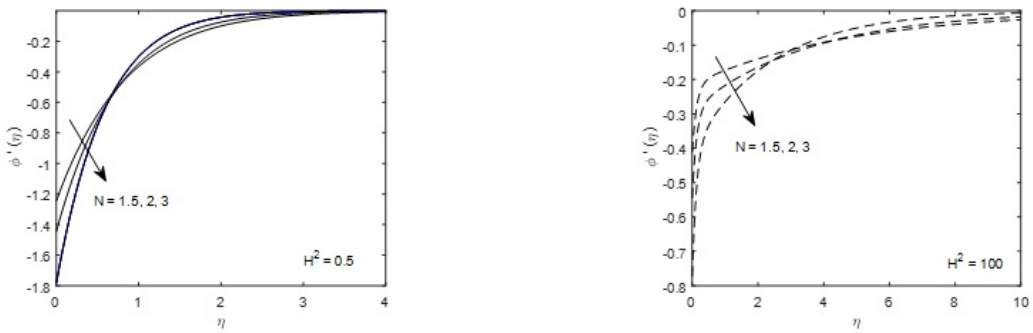

Figure 7.5: Concentration gradient profile for certain values of N when $\beta = R$, $Sc = Bi = 1$.

7.4 Conclusion

The current study was designed to determine the influence of various values of controlling parameters. The analysis leads to the following conclusions:

- The magnitude of $f''(0)$ is increasing while opposite phenomenon occur for $\theta'(0)$ and $\phi'(0)$ when the Hartmann number, H^2 is increase.

- The velocity motion within the boundary layer is reduce affected by extending of N.
- Temperature and concentration within the layer is increase by increment of H^2 and decrease by increment of N.

Acknowledgement

The present research was partially supported by the Putra Grant with Project Number GP-IPM/2018/9596900.

Bibliography

[1] Abro, K. A., Shaikh, H. S., and Khan, I. (2017). *A mathematical study of magnetohydrodynamic Casson fluid via special functions with heat and mass transfer embedded in porous plate*, arXiv preprint arXiv:1706.03829.

[2] Casson N. (1959). *"Rheology of disperse systems," in Flow Equation for Pigment Oil Suspensions of the Printing Ink Type. Rheology of Disperse Systems,* C. C. Mill, Ed., 84-–102.

[3] G. W. S. Blair,. (1959). *An equation for the flow of blood, plasma and serum through glass capillaries,*Nature, Vol 183(4661), 613—614, .

[4] Copley, A. L. (1960).*Apparent viscosity and wall adherence of blood systems*, Pergamon Press, Oxford, UK, 97–111).

[5] Alinejad, J., and Samarbakhsh, S. (2012). *Viscous Flow over Nonlinearly Stretching Sheet with Effects of Viscous Dissipation*, Journal of Applied Mathematics Vol 2012.

[6] Ashraf, M. B., Hayat, T., and Alsaedi, A. (2017). *Mixed convection flow of Casson fluid over a stretching sheet with convective boundary conditions and Hall effect*, Boundary Value Problems, Vol 2017(1), 137.

[7] Ullah, I., Shafie, S., and Khan, I. (2017). *MHD free convection flow of Casson fluid over a permeable nonlinearly stretching sheet with chemical reaction*, Malaysian Journal of Fundamental and Applied Sciences, Vol 13(3).

[8] Mabood, F., and Das, K. (2019). *Outlining the impact of melting on MHD Casson fluid flow past a stretching sheet in a porous medium with radiation*, Heliyon, 5(2), e01216.

[9] Abd El-Aziz, M., and Afify, A. A. (2019). *MHD Casson Fluid Flow over a Stretching Sheet with Entropy Generation Analysis and Hall Influence*, Entropy, 21(6), 592.

[10] Awais, M., Hayat, T., Nawaz, M., and Alsaedi, A. (2015). *Newtonian heating, thermal-diffusion and diffusion-thermo effects in an axisymmetric flow of a Jeffery fluid over a stretching surface*, Brazilian Journal of Chemical Engineering, Vol 32(2), 555–561.

[11] Merkin, J. H. (1994). *Natural-convection boundary-layer flow on a vertical surface with Newtonian heating*, International Journal of Heat and Fluid Flow, Vol 15(5), 392–398.

[12] Das, M., Mahato, R., and Nandkeolyar, R. (2015). *Newtonian heating effect on unsteady hydromagnetic Casson fluid flow past a flat plate with heat and mass transfer*, Alexandria Engineering Journal, Vol 54(4), 871–879.

[13] Hussanan, A., Salleh, M. Z., Khan, I., and Tahar, R. M. (2016). *Unsteady heat transfer flow of a Casson fluid with Newtonian heating and thermal radiation*, Jurnal Teknologi, Vol 78(4-4).

[14] Ullah, I., Shafie, S., and Khan, I. (2017). *Effects of slip condition and Newtonian heating on MHD flow of Casson fluid over a nonlinearly stretching sheet saturated in a porous medium*, Journal of King Saud University-Science, Vol 29(2), 250–259.

[15] Ahmad, K., Wahid, Z., and Hanouf, Z. (2019). *Heat transfer analysis for Casson fluid flow over stretching sheet with Newtonian heating and viscous dissipation*, Journal of Physics: Conference Series, Vol. 1127(1),012028.

[16] Brewster, M. Q. (1992). *Thermal radiative transfer and properties* . John Wiley and Sons.

[17] Isa, S. S. P. M., Arifin, N. M., and Farooq, U. (2018). *The impact of slip conditions on magnetohydrodynamics radiating fluid beyond an exponentially extended sheet. In Journal of Physics: Conference Series*, Vol 1039(1), 012015.

[18] Cebeci, T. Bradshaw, P. (1988). *Physical and Computational Aspects of Convective Heat Transfer*, New York: Springer.

Chapter 8

On the Variants of RSA Cryptosystem and Its Related Algebraic Cryptanalysis

Wan Nur Aqlili Ruzai[1], Muhammad Rezal Kamel Ariffin[1,2], **Muhammad Asyraf Asbullah**[1,3,*]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: ma_asyraf@upm.edu.my

Abstract

The RSA cryptosystem is the earliest public key cryptosystem which came into existence since 1978 and has become the most broadly used public key cryptosystem in the world. So far, RSA is being implemented as a default cryptosystem in most of web browsers and also most commonly used feature to secure internet banking systems. For decades, studies on improving the efficiency of RSA in terms of its encryption and decryption time, and also its security were conducted. Hence, many variants of RSA were proposed to overcome such said issues. Essentially this review article attempts to analyze the variants of RSA cryptosystem which shared a similarity of possessing its public key e and private key d satisfying this particular key equation of the form $ed - k(p^2-1)(q^2-1) = 1$ where the product of $(p^2-1)(q^2-1)$ is referred as modified Euler totient function. This review article also emphasizes on the algebraic cryptanalysis methods proposed on those variants cryptosystems specifically via the continued fractions method and the lattice reduction method.

Keywords: variants of RSA, algebraic cryptanalysis, continued fractions method, lattice reduction method.

8.1 Introduction

Back in 1976, the idea of using different keys for encryption and decryption process between the communicating parties was introduced in the influential work of Diffie and Hellman [9]. However, the notion of asymmetric cryptography is not yet realized

by many until the introduction of the very first practical public key cryptosystem– the RSA cryptosystem. It is made widely known in 1978 and the acronym of RSA was initially from the names of its inventors; Rivest, Shamir, and Adleman [23].

This cryptosystem is being implemented in most of web servers with the goals of providing privacy, authenticity and also the security of digital data. RSA is employed to secure web traffic, e-mail, e-commerce also smart cards. For more than four decades, research on improving the efficiency of RSA in terms of its encryption and decryption time, and also its security were vastly conducted. Hence, numerous variants of RSA cryptosystem were proposed to overcome all the possible vulnerabilities. Previously, there are many reviews and surveys were published discussing on RSA and its variants also its related cryptanalysis such as in [1,3,12,17]. The author in [1] excellently discussed on the attacks previously launced on RSA cryptosystem which mentioned that these attacks mostly tackled on the pitfalls to be averted when implementing RSA. While in [3], the authors discussed in details on some variants of RSA with the purpose of speeding up the RSA decryption in software. This kind of system is suitable to be enforced on small devices and web servers.

In this paper, we specifically survey on three variants of RSA of the shape $N = pq$; that are designed with the condition of its public exponent e and private exponent d fulfilled a particular key equation of the form $ed - k(p^2 - 1)(q^2 - 1) = 1$. For simplicity, we referred the term $(p^2 - 1)(q^2 - 1)$ as modified Euler totient function throughout this article. Among the cryptosystems being reviewed are the instances of RSA cryptosystem based on ellipitic curves, domain of Gaussian integers and Lucas sequences. As concluded in [10], the extension of RSA cryptosystem based on Gaussian integers possesses benefit over the original RSA in term of the security purpose. This is due to the Euler totient function which is in the form of $(p - 1)(q - 1)$ of the original RSA cryptosystem is extended to $(p^2 - 1)(q^2 - 1)$ which provides more security to the system. According to [7], the variant of RSA based on Lucas sequences serves as the alternative to the cryptosystems based on the hard problems similar to RSA. The advantage of the cryptosystem proposed in [7] is on the computational cost which is smaller as compared to El-Gamal elliptic curves cryptosystem.

The layout of this review article is as follows. A brief review on the basic of RSA cryptosystem is presented in Section 8.2. In Section 8.3, the selected variants of RSA cryptosystem are discussed in details. The proposed algebraic attacks launched on the selected variants of RSA mentioned previously are compiled in Section 13.4. This review article is summed up in Section 8.5.

8.2 A Basic Review on RSA Cryptosystem

In this section, we present the construction algorithms of the textbook RSA cryptosystem [23]. RSA is made up of three constituents which are the key generation, encryption and decryption that can be defined as in Algorithm 1. Refer to [13, 19] for more information on this cryptosystem.

The Correctness of RSA Decryption.
In order to prove that the decryption process of RSA reverses its encryption process, first, express the modular relation $ed \equiv 1 \pmod{\phi(N)}$ into an equation of the form $ed = 1 + k\phi(N)$ for some positive integer k. Then, by Euler's theorem; which

Algorithm 1: The RSA Cryptosystem.

Key Generation Algorithm
Input: t-bits size of chosen primes.
Output: Public key pair (N, e) and its respective private key tuple (p, q, d).
1. Selects randomly two distinct primes p and q such that $2^t < p, q < 2^{t+1}$.
2. Calculates $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Chooses an integer e which satisfies $e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
4. Calculates a respective integer d such that $d \equiv e^{-1} \pmod{\phi(N)}$.
5. Keeps private keys (p, q, d) and publicizes public keys (N, e).

Encryption Algorithm
Input: The plaintext $M \in \mathbb{Z}_N^*$ and public key pair (N, e).
Output: The ciphertext C.
1. Calculates $C \equiv M^e \pmod{N}$.
2. Sends ciphertext C.

Decryption Algorithm
Input: The private keys (p, q, d) and ciphertext C.
Output: The plaintext M.
1. Calculates $M \equiv C^d \pmod{N}$.
2. Recovers back plaintext message M.

state that for any positive integer M with $\gcd(M, N) = 1$, this modular relation $M^{\phi(N)} \equiv 1 \pmod{N}$ holds. Thus, the proof of correctness for RSA decryption is given as follows.

$$C^d \equiv (M^e)^d \equiv M^{1+k\phi(N)} \equiv M \cdot (M^{\phi(N)})^k \equiv M \pmod{N} \tag{8.1}$$

Hence, it is proven that from 8.1, for a given ciphertext C, we can always retrieve back the corresponding plaintext M.

In RSA cryptosystem, an integer N is known as RSA modulus, parameter e is the public exponent while d is its respective private exponent. An integer e and d are associated by the equation of the form $ed - k(p-1)(q-1) = 1$ for some $k \in \mathbb{Z}$. The product of $(p-1)(q-1)$ is well-known as Euler totient function (i.e. often denoted by $\phi(N)$).

Essentially, the security of RSA relies on the hardness of integer factorization problem of the shape $N = pq$ together with the modular e^{th} root problem and the difficulty of solving the key equation problem. These hard problems are briefly defined as follows.

Definition 8.2.1. Integer Factorization Problem.
Given an RSA modulus $N = pq$. Then, the integer factorization problem is to find the prime factors p and q.

Definition 8.2.2. Modular e^{th} Root Problem.
Given an RSA public key pair (N, e) where $N = pq$ and $e \geq 3$. Then, the modular e^{th} root problem is to solve for an integer M from C which is related by $C \equiv M^e \pmod{N}$.

Definition 8.2.3. Key Equation Problem.
Given an RSA modulus $N = pq$ and $e \in \mathbb{Z}$ which satisfies the equation $ed - k\phi(N) = 1$ where $\phi(N) = (p-1)(q-1)$. Then, the key equation problem is to solve for integers $\phi(N), k$, and d.

It is worth to note that the security of many variants of RSA also relies on the hard problems of the original RSA.

8.3 Survey on Variants of RSA with Particular Key Equation

In this section, we scrutinize our analysis on the existing extended versions of RSA cryptosystem with the special form of key equation and of modulus $N = pq$. Observe that the public exponent e and its respective private exponent d of these variants cryptosystem satisfy the modified key equation of the form $ed - k(p^2-1)(q^2-1) = 1$ for some $k \in \mathbb{Z}$. We put forward reviews for selected RSA variants in the following next subsections.

8.3.1 RSA Variant Based on Elliptic Curves

In 1995, Kuwakado et al. [16] suggested the idea of adapting singular elliptic curves into RSA cryptosystem with modulus of the shape $N = pq$. The related elliptic curves used in this public key cryptosystem is

$$E_N(b) : y^2 \equiv x^3 + bx^2 \pmod{N} \tag{8.2}$$

which defined over $\mathbb{Z}_{\mathbb{N}}$ (i.e. the ring of integers modulo N); such that (x, y) is the set of points in $\mathbb{Z}_N^2$ and $b \in \mathbb{Z}/N\mathbb{Z}$.

Briefly, in the process of encryption and decryption of this cryptosystem, the plaintext M and ciphertext C can be represented by point $\rho = (x, y)$ which lies on elliptic curves (8.2) where the proof of correctness of the decryption algorithm is due to the following relation

$$(p^2 - 1)(q^2 - 1)\rho = \mathcal{O}_N, \tag{8.3}$$

such that $\mathcal{O}_N$ is defined as the additive identity of the curve or can be denoted as the point at ∞. The following Algorithm 2 summarizes the cryptosystem in [16].

Remark 8.3.1. The computation of plaintext point M and ciphertext point C is performed over the curve $y^2 \equiv x^3 + bx^2 (\text{mod } N)$.

Observe from step 4 in key generation of Algorithm 2, the modular relation $d \equiv e^{-1} \pmod{(p^2-1)(q^2-1)}$ can be expressed equivalently in the key equation form $ed - k(p^2-1)(q^2-1) = 1$. From this point, an attack on this form of key equation can be launced.

Algorithm 2 The Kuwakado et al. Cryptosystem

Key Generation Algorithm
Input: t-bits size of selected primes.
Output: The private key tuple (p, q, d) and public key pair (N, e).
1. Chooses randomly p and q which are the distinct primes where $2^t < p, q < 2^{t+1}$.
2. Calculates $N = pq$.
3. Selects an integer e which has $\gcd(e, (p^2-1)(q^2-1)) = 1$.
4. Calculates the corresponding integer d where $d \equiv e^{-1} \pmod{(p^2-1)(q^2-1)}$.
5. Returns the private key tuple (p, q, d) and public key pair (N, e).

Encryption Algorithm
Input: The plaintext M and public key pair (N, e).
Output: The ciphertext C.
1. Transforms the message $M = (M_x, M_y) \in \mathbb{Z}_N^2$.
2. Calculates $b = \frac{M_y^2 - M_x^3}{M_x^2} \pmod{N}$.
3. Calculates ciphertext point $C = (C_x, C_y) = e(M_x, M_y)$.

Decryption Algorithm
Input: The private key d and ciphertext (C_x, C_y).
Output: The plaintext M.
1. Computes $b = \frac{C_y^2 - C_x^3}{C_x^2} \pmod{N}$.
2. Computes the point $M = (M_x, M_y) = d(C_x, C_y)$.

8.3.2 RSA Variant Based on Gaussian Integers

In 2002, Elkamchouchi et al. [10] proposed an idea to extend RSA cryptosystem into the domain of Gaussian integers. By definition, a Gaussian integer is a complex number whose the real and imaginary parts are both integers. Recall the form of a complex number is $x + iy$ where x is the real part, y is the imaginary part and $i = -1$. Considering the case of ordinary addition and multiplication of complex numbers, Gaussian integers formed an integral domain or can be expressed as $\mathbb{Z}[i]$. Hence, we have

$$\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\} \tag{8.4}$$

The Euclidean norm of (10.4) is defined as $|x + iy| = x^2 + y^2$. Any Gaussian integer is called a Gaussian prime if its only divisor is a unit (i.e. all units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$); which also has norm equal to 1. Among the properties of a Gaussian prime are as follows:

- If $x + iy \in \mathbb{C}$ is a Gaussian prime, then $x^2 + y^2 \in \mathbb{Z}$ is a prime holds.
- If an integer q is an ordinary prime, then the Gaussian integers q and qi are Gaussian primes iff the modular relation $q \equiv 3 \pmod 4$ holds.
- Let β is a Gaussian integer. The modular relation $\beta^{|P|-1} \equiv 1 \pmod{P}$ holds when $\beta \not\equiv 0 \pmod{P}$ if P is a Gaussian prime.
- Let β is a Gaussian integer. The modular relation $\beta^{(|P|-1)(|Q|-1)} \equiv 1 \pmod{N}$ holds when $\beta \not\equiv 0 \pmod{N}$ if $N = PQ$ is the product of two Gaussian primes.
- Let β is a Gaussian integer. The modular relation $\beta^{(p^2-1)(q^2-1)} \equiv 1 \pmod{N}$ holds when $\beta \not\equiv 0 \pmod{N}$ if $N = pq$ is the product of two ordinary primes.

By considering all properties of Gaussian integers mentioned into account, Elkamchouchi et al. [10] introduced a new variant of RSA cryptosystem as described in Algorithm 3.

Algorithm 3 The Elkamchouchi et al. Cryptosystem

Key Generation Algorithm
Input: t-bits size of security parameter.
Output: The private parameters (P, Q, d) and public parameters (N, e).
1. Selects Gaussian primes P and Q of similar norm such that $P \neq Q$.
2. Calculates $N = PQ$.
3. Selects $e \in \mathbb{Z}$ which has $\gcd(e, (|P| - 1)(|Q| - 1)) = 1$.
4. Calculates the corresponding $d \in \mathbb{Z}$ where $d \equiv e^{-1} \pmod{(|P| - 1)(|Q| - 1)}$.
5. Keeps parameters (P, Q, d) and publicizes parameters (N, e).

Encryption Algorithm
Input: The public parameters (N, e) and plaintext M.
Output: The ciphertext C.
1. Converts the plaintext M to Gaussian integer (i.e. $M \in \mathbb{Z}[i]$).
2. Calculates $C \equiv M^e \pmod{N}$.

Decryption Algorithm
Input: The private parameter d and ciphertext $C \in \mathbb{Z}[i]$.
Output: The plaintext $M \in \mathbb{Z}[i]$.
1. Calculates $M \equiv C^d \pmod{N}$.

Observe that from the key generation of Algorithm 3, if the modulus $N \in \mathbb{Z}$ is the product of two ordinary prime numbers p and q (i.e. $N = pq$), then yields the modular inverse e of an integer d or can be written as $d \equiv e^{-1} \pmod{(p^2 - 1)(q^2 - 1)}$ which also can be expressed in key equation form as

$$ed - k(p^2-)(q^2 - 1) = 1. \tag{8.5}$$

Again, the key equation as in (8.5) is equivalent to the key equation used in cryptosystem suggested by Kuwakado et al. [16].

8.3.3 RSA Variant Based on Lucas Sequences

In 2006, Castagnos [7] designed a probabilistic version of RSA-variants that works in environment of quadratic fields quotients. The idea behind this public key cryptosystem was to utilize the properties of Lucas sequences in the encryption and decryption algorithms. Suppose r is an integer. Briefly, the Lucas sequences is defined as the following.

$$V_0(r) = 2, \quad V_1(r) = r, \quad V_{k+2}(r) = rV_{k+1}(r) - V_k(r), \quad \text{where} \quad k \geq 0.$$

Note that, square and multiply algorithm is considered the efficient method to compute Lucas sequences. In the next Algorithm 4, be reminded that $\left(\frac{x}{p}\right)$ represents the Jacobi symbol that can be found in details in [26].

Algorithm 4 The Castagnos Cryptosystem

Key Generation Algorithm
Input: t-bits size of security parameter.
Output: The private keys p, q and public key pair (N, e).
1. Selects distinct and of the same bit-sizes primes p and q.
2. Calculates $N = pq$.
3. Selects $e \in \mathbb{Z}$ which has $\gcd(e, (p^2-1)(q^2-1)) = 1$.
4. Keeps the private keys p, q and publishes the public key pair (N, e).

Encryption Algorithm
Input: The public key pair (N, e) and plaintext M.
Output: The ciphertext C.
1. Converts the original plaintext to $M \in \mathbb{Z}/N\mathbb{Z}$.
2. Selects a random integer r from the set $\{1, \cdots, N-1\} \backslash \{2, N-2\}$.
3. Calculates ciphertext C such that $C \equiv (1+MN)V_e(r) \pmod{N^2}$.

Decryption Algorithm
Input: The private keys p, q, d and ciphertext C.
Output: The plaintext M.
1. Calculates $i_p = \left(\frac{C^2-4}{p}\right)$ and $d(p, i_p) \equiv e^{-1} (\text{mod } p - i_p)$.
2. Calculates $i_q = \left(\frac{C^2-4}{q}\right)$ and $d(q, i_q) \equiv e^{-1} (\text{mod } q - i_q)$.
3. Calculates $r_p \equiv V_{d(p,i_p)} (\text{mod } p)$ and $r_q \equiv V_{d(q,i_q)} (\text{mod } q)$.
4. Calculates $p' \equiv p^{-1} (\text{mod } q)$ and $r = r_p + p(r_p - r_q)p' (\text{mod } N)$.
5. Calculates $t_p \equiv \frac{C}{V_e(r)} (\text{mod } p^2)$ and $M_p \equiv q^{-1} \cdot \frac{t_p - 1}{p} (\text{mod } p)$.
6. Calculate $t_q \equiv \frac{C}{V_e(r)} (\text{mod } q^2)$ and $M_q \equiv p^{-1} \cdot \frac{t_q - 1}{p} (\text{mod } q)$.
7. Calculates the plaintext M such that $M \equiv M_p + p(M_q - M_p)p' (\text{mod } N)$.

Observe that from the key generation of Algorithm 4, the corresponding inverse of an integer e (i.e. an integer d) is not computed directly by the algorithm. However, as mentioned in [7], the private exponents d are represented by the vectors

$$d = \{d_{(p,1)}, d_{(p,-1)}, d_{(q,1)}, d_{(q,-1)}\} \tag{8.6}$$

where $d_{(p,i)} \equiv e^{-1} (\text{mod } p - i)$ for $i = \pm 1$, the same argument holds for the prime q.

Hence, the key equation having the shape $ed - k(p^2-)(q^2-1) = 1$ is deduced and the proposed attacks designed on this particular key equation also work on this cryptosystem when d is specifically small.

8.4 Algebraic Cryptanalysis on Particular Key Equation of Variants of RSA

We devoted this section to discuss the cryptanalytic works proposed upon the variants of RSA cryptosystem previously mentioned in Section 8.3. We are interested on the cryptanalysis technique via the continued fractions method and the lattice reduction method. In the first part, we present the previous cryptanalytic works which utilized the continued fractions properties to find the approximation of modified Euler totient function (i.e. the term $\omega(N) = (p^2-1)(q^2-1)$). Then, we show

the application of the Coppersmith's theorem [8] in the previously cryptanalytic works.

We begin by reviewing the fundamental knowledge of continued fractions and its related concepts.

Definition 8.4.1. (Continued fractions, [20]) The continued fractions expansion of $x \in \mathbb{R}$ can be defined and written in the following form

$$x = [x_0, x_1, x_2, \cdots] = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}}$$

such that $x_0 \in \mathbb{Z}$ and $x_i \in \mathbb{Z}^+$ for $i > 0$.

From Definition 8.4.1,

I. The numbers $x_1, x_2, x_3, \cdots$ are known as partial quotients.

II. For $i \geq 0$, the fractions $\frac{r_i}{s_i} = [x_0, x_1, x_2, \cdots, x_i]$ are known as convergents of continued fractions expansion of $\frac{r_i}{s_i}$.

III. For $x = \frac{a}{b}$, the continued fractions algorithm (i.e. the Euclidean Algorithm) computes the convergents in polynomial time; $\mathcal{O}(\log b)$.

Consequently, the following theorem is the significant result on continued fractions that can be found in most of literatures related to cryptanalysis of RSA via diophantine approximations.

Theorem 8.4.2. (Legendre's Theorem, [11]) Let $x \in \mathbb{Q}$ and $y, z \in \mathbb{Z}^+$ where $\gcd(y, z) = 1$. If

$$\left| x - \frac{y}{z} \right| < \frac{1}{2z^2}, \tag{8.7}$$

then $\dfrac{y}{z}$ is a convergent of the continued fractions expansion of x.

Since 1990, Wiener [25] pioneered a prominent attack upon RSA cryptosystem when the secret exponent d is suitably small. Wiener proved that the secret parameters k and d can be found efficiently using the continued fractions algorithm to find the associated convergents of public value $\frac{e}{N}$. The attack is elaborated by the next theorem.

Theorem 8.4.3. Suppose $N = pq$ and $\phi(N) = (p-1)(q-1)$ such that $q < p < 2q$. Suppose the exponents d and $e < \phi(N)$ satisfying an equation $ed - k\phi(N) = 1$ for some $k \in \mathbb{Z}$. If $d < \frac{1}{3}N^{0.25}$, then $\frac{k}{d}$ is a convergent of continued fractions expansion of $\frac{e}{N}$.

Proof. See (Wiener, [25]).

Then, one can retrieve the prime factors p and q by finding the roots X_1 and X_2 of polynomial $X^2 - (N - \phi(N) + 1)X + N = 0$ (i.e. $X_1 = p$ and $X_2 = q$).

Inspired by Wiener's attack on RSA, in 2016, Bunder et al. [4] suggested an attack upon variants of RSA cryptosystem mentioned in [7, 10, 16], also using the

continued fractions method to find $\frac{k}{d}$ among the convergents of $\frac{e}{N^2-\frac{9}{4}N+1}$. The attack is described in the following theorem.

Theorem 8.4.4. Let (N, e) be a public key in cryptosystems by [7, 10, 16] such that modulus $N = pq$ with $q < p < 2q$. Let $\omega(N) = (p^2-1)(q^2-1)$. If $e < \omega(N)$ satisfies an equation $ed - k\omega(N) = 1$ whenever $d < \sqrt{\frac{2N^3-18N^2}{e}}$, then the prime factors p and q can be found in polynomial time.

Proof. See (Bunder et al., [4]).

Lemma 8.4.5. Suppose an RSA modulus $N = pq$ such that $q < p < 2q$. If $\phi_1 = N^2 - \frac{5}{2}N + 1$ and $\phi_2 = N^2 - 2N + 1$, then $\phi_1 < (p^2-1)(q^2-1) < \phi_2$.

Proof. See (Bunder et al., [4]).

Previously, [4] proved that $\omega(N) = (p^2-1)(q^2-1)$ is bounded by certain interval as in Lemma 8.4.5. Based on the attack in Theorem 8.4.4, the unknown term $\omega(N)$ is approximated to the public value $N^2 - \frac{9}{4}N + 1$ which actually the midpoint of interval $(N^2 - \frac{5}{2}N + 1, N^2 - 2N + 1)$. Upon obtaining the values of d and k, one can find the factorization of modulus N by solving the roots X_1 and X_2 of polynomial $X^2 - (N^2 - \omega(N) + 1)X + N^2 = 0$ (i.e. $X_1 = \sqrt{p}$ and $X_2 = q$).

Later, Tonien [24] extends the work in [4] by introducing the new attack also based on the continued fractions method. The attack is applicable upon the cryptosystems having its public exponent e and secret exponent d that are associated by modular relation $ed \equiv 1 (\mathrm{mod}\ (p^2-1)(q^2-1))$. The proposed attack is summarized as follows.

Theorem 8.4.6. Suppose $t \in \mathbb{N} - \{0\}$ is fixed and $\omega(N) = (p^2-1)(q^2-1)$. The unknowns $\frac{k}{d}$ can be found among the convergents of $\frac{e}{N_i}$ for some $1 \leq i \leq t$ via the continued fractions algorithm with time complexity $\mathcal{O}(t \log(N))$ if the following requirements are met;

- $q < p < 2q, \quad 0 < e, d < \omega(N), \quad ed - k\omega(N) = 1,$
- $d < \sqrt{\frac{2t(N^2-\frac{5}{2}N)^2}{e(N+4t)}} \approx 2tN^3$ and
- $N_i = N^2 - \frac{5}{2}N + (2i-1)\frac{N}{4t} + 1, \quad i \in [1, t].$

Proof. See (Tonien, [24]).

Recently in 2018, Bunder et al. [6] published another new attack upon the same variants of RSA cryptosystem as in [7, 10, 16]. This time, the authors contemplated on case where the distinct primes p and q are said to be unbalanced (i.e. the primes are of arbitrary sizes satisfying $q < p < \mu q$). Note that a chosen parameter μ takes the value $\mu > 2$. If a chosen parameter $\mu = 2$, then the two distinct primes p and q are of the same-bit-size or they are said to be balanced primes. The attack can be described as follows.

Theorem 8.4.7. Suppose an RSA modulus $N = pq$ such that $q < p < \mu q$ and e be the public values in cryptosystems by [7, 10, 16]. Let $\omega(N) = (p^2 - 1)(q^2 - 1)$. If $e < \omega(N)$ satisfies the key equation $ed - k\omega(N) = 1$ wherever $d < \frac{N(N-(\mu+\frac{1}{\mu}))}{\sqrt{e(\frac{(\mu-1)^2}{\mu}N+2)}}$, then the unknown $\frac{k}{d}$ is among the convergents of $\frac{e}{N^2+1-\frac{(\mu-1)^2}{2\mu}N}$ via the continued fractions algorithm and leads to factorization of N in poly-time.

Proof. See (Bunder et al., [6]).

Lemma 8.4.8. Suppose an RSA modulus be presented by $N = pq$ with $q < p < \mu q$. Let $\alpha_1 = N^2 - (\mu + \frac{1}{\mu})N + 1$ and $\alpha_2 = N^2 - 2N + 1$. Then $\alpha_1 < \omega(N) < \alpha_2$.

Proof. See (Bunder et al., [6]).

Similar to the approach in [4], the term $\omega(N) = (p^2 - 1)(q^2 - 1)$ is proven to be within the interval as stated in Lemma 8.4.8. Based on the attack in Theorem 8.4.7, the denominator term of public number $\frac{e}{N^2+1-\frac{(\mu-1)^2}{2\mu}N}$ represents midpoint of interval $(N^2 - (\mu + \frac{1}{\mu})N + 1, N^2 - 2N + 1)$ and the approximation of the unknown value $\omega(N)$.

In the next part, we present the previous cryptanalytic works which applied the theory established by Coppersmith [8] as in the following Theorem 8.4.9. One can apply this theorem to prove that if for an RSA modulus $N = pq$ with the same -bit-size primes p and q satisfying the condition of $|p - q| < N^{0.25}$, then leads to solve for the unknown factors p and q.

Theorem 8.4.9. Suppose the product of two distinct primes be denoted by $N = pq$ with $q < p < 2q$. If p is approximated to ϱ with the difference between the terms is $|p-\varrho| < N^{0.25}$, then the unknowns p and q can be found in poly-time ($i.e.\mathcal{O}(\log N)$).

Proof. See (Copppersmith, [8]).

Boneh and Durfee [2] suggested an influential result over Wiener's bound. As a result, one can obtain the unknown primes p and q wherever $d < N^{0.292}$ within polynomial time. This result is due to Coppersmith's method on solving the small roots for modular polynomial equations with one variable. Another contribution of Coppersmith is by introducing an algorithm for solving small roots of integer polynomial equations with two variables. Interested readers may refer to [18] for the details on the Coppersmith's approach.

Bunder et al. [5] continue the work in [4] by considering more general form of key equation such that $eu-(p^2-1)(q^2-1)v = w$. The new suggested attack is as follows.

Theorem 8.4.10. Suppose an RSA modulus be presented by $N = pq$ with $q < p < 2q$. If a public value e satisfies an equation $eu-(p^2-1)(q^2-1)v = w$ with $\gcd(u, v) = 1$. If

$$uv < 2N - 4\sqrt{2}N^{0.75} \quad \text{and} \quad |w| < (p - q)N^{0.25}v,$$

then one can obtain the prime factorization of N in polynomial time ($i.e.\mathcal{O}(\log N)$).

Proof. See (Bunder et al., [5]).

Based on the attack in Theorem 8.4.10, the unknown positive integers u and v can be found among the convergents of public rational number $\frac{e}{N^2-\frac{9}{4}N+1}$ via the continued fractions algorithm. Then, the Coppersmith's method is applied to factor primes p and q. Recalled that the bound of δ of Theorem 8.4.10 is simplified to

$$\delta < \frac{3-\beta}{2}, \tag{8.8}$$

when assuming $e = N^{\beta}$, $u = N^{\delta}$ and $|w| = N^{\gamma}$.

Next after, Nitaj et al. [21] proposed an attack upon the generalized key equation of the shape

$$eu - (p^2-1)(q^2-1)v = w, \tag{8.9}$$

by utilizing the Coppersmith's theory on finding the modular roots of multivariate polynomials. In comparison with the result in [5], Nitaj et al. improved the previous result by proposing a better bound of δ to

$$\delta < \frac{7}{3} - \gamma - \frac{2}{3}\sqrt{1+3\beta-3\gamma} - \epsilon. \tag{8.10}$$

By letting $|w| = 1$, then the only possible value for γ is zero. Then, equation 8.10 becomes

$$\delta < \frac{7}{3} - \frac{2}{3}\sqrt{1+3\beta} - \epsilon. \tag{8.11}$$

Then, to compare the bound in [5] and [21] by finding the difference denoted δ_1 between equation 8.11 and equation 8.8 which yields

$$\delta_1 = \frac{5}{6} + \frac{\beta}{2} - \frac{2}{3}\sqrt{1+3\beta} - \epsilon \tag{8.12}$$

By omitting the ϵ term in equation 8.12, it is cleared that $\delta_1 \geq 0$. Thus, the bound of δ in [21] improves as compared to the result in [5].

In contrary, Peng et al [22] suggested an attack to solve for an equation

$$ed - k(p^2-1)(q^2-1) = 1 \tag{8.13}$$

by adopting the Coppersmith's technique to solve for the secret parameters k, p, q by firstly transforming the equation 8.13 into the modular equation of the form

$$k(p^2-1)(q^2-1) + 1 \equiv 0 \pmod{e}. \tag{8.14}$$

Then, under certain circumstances, [22] improves the results of δ which previously proposed in [5, 21] to

$$\delta < 2 - \sqrt{\beta}, \quad \text{where} \quad \beta \geq 1. \tag{8.15}$$

By finding the difference between the bound of δ in equation 8.15 and equation 8.12 denoted by δ_2 which yields

$$\delta_2 = \frac{2}{3}\sqrt{1+3\beta} - \beta - \frac{1}{3} - \epsilon. \tag{8.16}$$

By disregarding ϵ term in equation 8.16, it is cleared that $\delta_2 \geq 0$. Thus, the bound of δ in [22] improves as compared to the result in [5, 21].

In different setting, Zheng et al. [27] for the first time proposed results on multiple secret keys attack and partial key exposure attack upon variants of RSA cryptosystem with particular key equation with the shape of equation 8.13. The authors utilized the lattice-based methods and compared their result with the original RSA cryptosystem. Remark that the authors consider the maximum size of public keys (i.e. $e \approx N$-original RSA and $e \approx N^2$-variants of RSA) in showing the respective δ. The respective result in [27] is summarized in the following Table 1.

Attack	Original RSA Cryptosystem [23]	Variants of RSA [7, 10, 16]
Small secret key attack	$\delta < 0.292$ [2]	$\delta < 0.585$
Multiple secret keys attack	$\delta < 1 - \sqrt{\frac{2}{3n+1}}$ [14]	$\delta < 2 - \sqrt{\frac{8}{3n+1}}$
Partial key exposure attack	$\delta < \frac{2+\gamma-\sqrt{2-3\gamma^2}}{2}$ [15]	$\delta < \frac{7+3\gamma-2\sqrt{7+3\gamma}}{3}$

Table 8.1: The attacks proposed in [27] and its respective result on bound of δ.

Observing from Table 1, note that for the multiple secret keys attack, parameter n is the number of given key-pairs whilst for partial key exposure attack, parameter γ is the known key exposure.

8.5 Conclusion

In this article, we have reviewed several variants of RSA cryptosystem constructed based on various algebraic structures –such as the instances of RSA extended with elliptic curves, Gaussian integers and Lucas sequences. Remark that this article specifically focus on the variants of RSA having its public and corresponding private keys e and d respectively and satisfying this particular key equation (i.e. key equation with the shape $ed - k(p^2 - 1)(q^2 - 1) = 1$). We scrutinize all cryptanalytic works proposed especially via the continued fractions method and the Coppersmith's method.

As for the future work, interested readers may consider to explore the case for simultaneous diophantine approximations of this particular key equation and improvise the use of lattice reduction method (i.e. the Coppersmith's approach) to improve the previously proposed bound of secret exponent.

Acknowledgement

The present research was partially supported by the Putra Grant with Project Number GP-IPS/2018/9657300.

Bibliography

[1] Boneh D. (1999) *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the AMS, Vol. 46(2), 203–213.

[2] Boneh D., Durfee G. (2000) *Cryptanalysis of RSA With Private Key d Less Than* $N^{0.292}$, IEEE Transactions on Information Theory, Vol. 46(4), 1339–1349.

[3] Boneh D., Shacham H. (2002) *Fast Variants of RSA*, CryptoBytes, Vol. 5(1), 1–9.

[4] Bunder M., Nitaj A., Susilo W., Tonien J. (2016) *A New Attack on Three Variants of the RSA Cryptosystem*, Australasian Conference on Information Security and Privacy, 258–268.

[5] Bunder M., Nitaj A., Susilo W., Tonien J. (2017) *A Generalized Attack on RSA Type Cryptosystems*,Theoretical Computer Science, Vol. 704(3), 74–81.

[6] Bunder M., Nitaj A., Susilo W., Tonien J. (2018) *Cryptanalysis of RSA-Type Cryptosystems Based on Lucas Sequences, Gaussian Integers and Elliptic Curves*, Journal of Information Security and Applications, Vol. 40, 193–198.

[7] Castagnos G. (2007) *An Efficient Probabilistic Public-Key Cryptosystem Over Quadratic Fields Quotients*, Finite Fields and Their Applications, Vol. 13(3), 563–576.

[8] Coppersmith D. (1997) *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities*, Journal of Cryptology, Vol. 10(4), 233–260.

[9] Diffie W., Hellman M. (1976), *New Directions in Cryptography*, IEEE transactions on Information Theory, Vol. 22(6), 644–654.

[10] Elkamchouchi H., Elshenawy K., Shaban H. (2002) *Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers*, Proceedings of the 8th International Conference on Communication Systems, 91–95.

[11] Hardy G.H., Wright E.M. (1965) *An Introduction to the Theory of Numbers*, Oxford University Press.

[12] Hinek M. J. (2009) *Cryptanalysis of RSA and its Variants*, CRC Press.

[13] Hoffstein J., Pipher J., Silverman J.H. (2008) *An Introduction to Mathematical Cryptography*, Vol.1, New York: Springer.

[14] Takayasu A., Kunihiro N. (2014) *Cryptanalysis of RSA With Multiple Small Secret Exponents*, In Australasian Conference on Information Security and Privacy, Springer, Cham, Vol. 8544, 176–191.

[15] Takayasu A., Kunihiro N. (2014) *Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound.*, In International Conference on Selected Areas in Cryptography, Springer, Cham, Vol. 8781, 345–362.

[16] Kuwakado H., Koyama K., Tsuruoka Y. (1995) *A New RSA-Type Scheme Based on Singular Cubic Curves* $y^2 = x^3 + bx^2 \ (mod\ n)$, IEICE Transactions on Fundamentals of Electronics, Vol. 78(1), 27–33.

[17] Long D.T., Thu D.T., Thuc D.T. *RSA and Its Variants.*

[18] May A. (2003) *New RSA Vulnerabilities Using Lattice Reduction Methods*, Doctor of Philosophy dissertation, University of Paderborn.

[19] Menezes A., Oorschot P., Vanstone S. (1997) *Handbook of Applied Cryptography*, CRC Press.

[20] Nitaj A. (2013) *Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem*, In Artificial Intelligence, Evolutionary Computing and Metaheuristics, 139–168.

[21] Nitaj A., Pan Y., Tonien J. (2019) *A Generalized Attack on Some Variants of the RSA Cryptosystem*, In International Conference on Selected Areas in Cryptography,Springer, Cham, 421–433.

[22] Peng L., Hu L., Lu Y., Wei H. (2016) *An Improved Analysis on Three Variants of the RSA Cryptosystem*, In International Conference on Information Security and Cryptology, Springer, Cham, 140–149.

[23] Rivest R., Shamir A., Adleman L. (1978) *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21(2), 120–126.

[24] Tonien J. (2018) *Continued Fractions and Their Applications*, Doctor of Philosophy thesis, School of Mathematics and Applied Statistics, University of Wollongong.

[25] Wiener M.J. (1990) *Cryptanalysis of Short RSA Secret Exponents*, IEEE Transactions on Information Theory, Vol. 36(3), 553–558.

[26] Williams H. (1980) *A Modification of The RSA Public-Key Encryption Procedure*, IEEE Transactions on Information Theory, Vol. 26(6), 726–729.

[27] Zheng M., Kunihiro N., Hu H. (2018) *Cryptanalysis of RSA Variants with Modified Euler Quotient*, In International Conference on Cryptology in Africa, Springer, Cham, 266–281.

Chapter 9

Effect of a Cubic Temperature Gradient on the Onset of Rayleigh-Benard Convection in a Micropolar Fluid

Nurul Afiqah Mohd Isa[1], **Ahmad Nazri M. Som**[2,*], Norihan Md Arifin[1,3], Norfifah Bachok[1,3]

[1] Department of Mathematics, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of foundation Studies For Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang Selangor, Malaysia.

*Corresponding author: nazrims@upm.edu.my

Abstract

The qualitative effect of a cubic temperature gradient on the linear stability analysis on the onset of Rayleigh-Benard convection in an Eringen's micropolar fluid is studied by using a single term Galerkin technique. In the case of Rayleigh-Benard convection, the eigenvalues is obtain for free-free, rigid-free, rigid-rigid velocity boundary combinations with isothermal and adiabatic temperature conditions on the spin-vanishing boundaries. The influence of various parameters has been analysed. Two cubic temperature gradient and a linear temperature profile are considered in this paper and their comparative influence on onset of convection is discussed.

Keywords: Rayleigh-Benard Convection; Micropolar; Cubic temperature gradient.

9.1 Introduction

The problem of thermal convection in a fluid layer driven by buoyancy (Benard) effects has recently been assumed importance in material processing. Thermal energy can be described as energy that is transferred from hot places to cold places by convection. Then, convection will occurs when warmer areas of a liquid or gas rise to cooler areas in the liquid or gas. Cooler liquid or gas then takes the place of the warmer areas which have risen higher. This results in a continuous circulation pattern. We can see that, water boiling in a pan is a one good example of these convection currents. Another good example of convection is in the atmosphere. This

phenomenon occur when the earth's surface is warmed by the sun, the warm air rises and cool air moves in.

Evolution of convection in a fluid has been greatly studied by many authors such as Roberts [1], Char and Chiang [2], Idris et al. [3], Mahmud et al. [4], Idris and Hashim [5, 6], and Tanasawa [7]. Convection is the transfer of internal energy into or out of an object by the physical movement of a surrounding fluid that transfers the internal energy along with its mass. Although the heat is initially transferred between the object and the fluid by conduction, the bulk transfer of energy comes from the motion of the fluid. In general, there are two types of convective heat transfer may be distinguished. That was free or natural convection and forced convection. Forced convection is a mechanism in which fluid motion is generated by an external source like a pump, fan, or other device. The familiar examples of natural convection are the upward flow of air due to a fire or hot object and the circulation of water in a pot that is heated from below.

Micropolar fluids are fluids with microstructure. They belong to a class of fluids with non-symmetric stress tensor that we shall call polar fluids, and include, as a special case, the well-established Navier-Stokes model of classical fluids that we shall call ordinary fluids. Physically, micropolar fluids may represent fluids consisting of rigid, randomly oriented (or spherical) particles suspended in a viscous medium, where the deformation of fluid particles is ignored. The model of micropolar fluids introduced in Eringen [8] is worth studying as a very well balanced one. Based on Eringen [8], micropolar fluids is a subclass of microfluids. The theory of microfluids introduced by Eringen [8] deals with a class of fluids which exhibit certain microscopic effects arising from the local structure and micro-motions of the fluid elements. These fluids can support stress moments and body moments and are influenced by the spin inertia. Onset of Rayleigh-Benard convection in horizontal micropolar fluid has been studied by Siddeshwar and Pranesh [10] with six types of temperature gradient, which are linear, piecewise linear (heated from below), piecewise linear (cooled from above), inverted parabola, step function and parabola and the fluid is bounded by free-free, rigid-free and rigid-rigid velocity boundary combinations with isothermal and adiabatic. Later, Siddeshwar and Pranesh [10] studied Benard-Marangoni magnetoconvection with suspended particles confined between an upper free/adiabatic and a lower rigid/isothermal boundary.

The objective of the present study is to analyze the effect of various hydrodynamic boundary condition on the onset of Rayleigh-bénard convection of a horizontal layer of micropolar fluids is heated from below with cubic temperature profile. Most of the previous authors considered only the six type of non-uniform temperature profiles of the present problem. To the best of our knowledge, this problem has not been studied before and the results reported here are new and original.

9.2 Mathematical Formulation

Consider an infinite horizontal micropolar fluid of an electrically conducting fluid with depth,d. Let ΔT be the temperature different between upper and lower boundary layer. A Cartesian coordinate system is taken with origin in the lower boundary and the $z-$axis vertically upwards. The no-spin boundary condition is assumed for microtation. The governing equations for the Rayleigh-Benard situation in a Boussinesquian micropolar fluid are:

$$\nabla \cdot q = 0, \tag{9.1}$$

$$\rho_0\left(\frac{\partial q}{\partial t}+(q\cdot\nabla)q\right)=-\nabla p-\rho g\hat{k}+(2\zeta+\eta)\nabla^2 q+\zeta\left(\nabla\times\omega\right), \tag{9.2}$$

$$\rho_0 I\left(\frac{\partial \omega}{\partial t}+(q\cdot\nabla)\,\omega\right)=\left(\lambda'+\eta'\right)\nabla\left(\nabla\cdot\omega\right)+\eta'\nabla^2\omega+\zeta\left(\nabla\times q-2\omega\right), \tag{9.3}$$

$$\frac{\partial T}{\partial t}+(q\cdot\nabla)\,T=\frac{\beta}{\rho_0 C_v}\left(\nabla\times\omega\right)\cdot\nabla T+\kappa\nabla^2 T, \tag{9.4}$$

$$\rho=\rho_b\left[1-\alpha\left(T-T_b\right)\right], \tag{9.5}$$

where g is acceleration due to gravity, λ and η are the bulk and shear kinematic viscosity coefficients, λ' and η' are the bulk and shear spin velocity coefficients, ς is the coupling viscosity coefficient or vortex viscosity, β is the micropolar heat conduction coefficient, C_v is the specific heat, ρ_0 is the density of the fluid at temperature $T=T_0$ and I is the moment of inertia. The upper boundary is assume to be non-deformable and the basic state of the fluid is quiescent (at rest) described by

$$q_b=(0,0,0),\ \omega_b=(0,0,0),\ p=p_b(z),\ -\frac{dT_b}{dz}=f(z), \tag{9.6}$$

where the subscript b indicates the basic state. Here, $f(z)$ is the basic non-uniform temperature gradient. The cubic temperature gradient consider in this paper are Cubic 1 and Cubic 2. Let the basic state be disturbed by an infinitesimal thermal perturbation:

$$q=q_b+q',\ \omega=\omega_b+\omega',\ p=p_b+p',\ \rho=\rho_b+\rho',\ T=T_b+T'. \tag{9.7}$$

The primes indicate that the quantities are infinitesimal perturbation. In the present problem, we assume the principle exchange of stability is valid and deal only with stationary convection. Substituting Eq. (9.7) into Eqs. (9.1)-(9.5), we get linearized governing equations to the infinitesimal perturbations in the form

$$0=\nabla\cdot q, \tag{9.8}$$

$$0=-\nabla p'-\rho' g\hat{k}+(2\zeta+\eta)\nabla^2 q'+\zeta\nabla\times\omega', \tag{9.9}$$

$$0=\left(\lambda'+\eta'\right)\nabla\left(\nabla\cdot\omega'\right)+\eta'\nabla^2\omega'+\zeta\left(\nabla\times q'-2\omega'\right), \tag{9.10}$$

$$-W\frac{\Delta T}{d}f(z)=\frac{\beta}{\rho_0 C_v}\left[\nabla\times\omega'\cdot\left(-\frac{\Delta T}{d}f(z)\right)\hat{k}\right]+\kappa\nabla^2 T', \tag{9.11}$$

$$\rho'=-\alpha\rho_0 T', \tag{9.12}$$

The perturbation Eqs. (9.8)-(9.12) are non-dimensionalised using the following definitions:

$$(x^*,y^*,z^*)=\left(\frac{x}{d},\frac{y}{d},\frac{z}{d}\right),\ W^*=\frac{W'}{x/d},\ \Omega^*=\frac{\left[\nabla\times\omega'\right]_z}{x/d^3},\ T^*=\frac{T'}{\Delta T}, \tag{9.13}$$

Substituting Eq. (9.13) into Eqs. (9.8)-(9.12), eliminating the pressure term by operating curl twice on the resulting equation of (9.10), operating curl on (9.11) and retaining the $z-$component, we obtain

$$(1+N_1)\nabla^4 W+N_1\nabla^2\Omega+R\left(\frac{\partial^2 T}{\partial x^2}+\frac{\partial^2 T}{\partial y^2}\right)=0, \tag{9.14}$$

$$N_3\nabla^2\Omega-2N_1\Omega-N_1\nabla^2 W=0, \tag{9.15}$$

$$\nabla^2 T+f(z)\left(W-N_5\Omega\right)=0, \tag{9.16}$$

where $R = \frac{g\alpha\nabla T\rho_b d^3}{(\eta+\zeta)\chi}$ is the Rayleigh number that represent the measure of buoyancy force to the dissipation force of viscous and the thermal dissipation, $N_1 = \frac{\zeta}{\eta+\zeta}; (0 \leq N_1 \leq 1)$ is the coupling parameter that represent the concentration of suspended particles in the fluid, $N_3 = \frac{n'}{(\eta+\zeta)d^2}; (0 \leq N_3 \leq \infty)$ is the couple stress parameter that represent the parameter which reduces the rate flow of fluid and lastly $N_5 = \frac{\beta}{\rho_b C_v d^2}; (0 \leq N_5 \leq \infty)$ is the micropolar heat conduction parameter that represent the heat induced into the fluid due to the microelements. If $\zeta = 0$, the above Rayleigh number identifies itself with classical definition. In this paper, we consider the steady-state temperature profile as given by (see Dupont et al. [11] and Chiang [12]):

$$T_b = \bar{T}_{OS} - a_1\left(\bar{z} - d\right) - a_2(\bar{z} - d)^2 - a_3(\bar{z} - d)^3, \tag{9.17}$$

where $(\bar{})$ denotes dimensional quantities, $\bar{T}_{OS}$ as the temperature at upper free surface horizontal fluid layer, and a_i, $i = 1, 2, 3$ are constants. In non-dimensional form, the $f(z)$ in Eq. (9.16) is given by (see Dupont et al. [11] and Chiang [12])

$$f(z) = a_1^* + 2a_2^*\left(z - 1\right) + 3a_3^*(z - 1)^2. \tag{9.18}$$

Then, the special case $a_1^* = 1$, $a_2^* = 0$, $a_3^* = 0$ enclosed the classical linear temperature distribution. We point out that the Model 1 (Cubic 1) is the theory of this model while Model 2 (Cubic 2) is the experimental conditions of Dupont et al. [11]. Three basic temperature gradients are considered for this thesis as mentioned in Table 9.1.

Table 9.1: Reference steady-state temperature gradients

Model	Reference steady-state temperature gradient	$f(z)$	a_1^*	a_2^*	a_3^*
1	Cubic 1	$3(z-1)^2$	0	0	1
2	Cubic 2	$0.6 + 1.02(z-1)^2$	0.6	0	0.34
3	Linear	1	1	0	0

The infinitesimal perturbations W, T and Ω are assumed to be periodic waves and hence these permit normal mode solution in the form suggested by Chandrasekhar [13]

$$(W, T, \Omega) = [W(z), \Theta(z), G(z)] \exp\left[i\left(a_x x + a_y y\right)\right], \tag{9.19}$$

where $W(z)$,$\Theta(z)$ and $G(z)$ are amplitudes of the perturbations vertical velocity, temperature, and spin respectively. In addition, $a = \sqrt{a_x^2 + a_y^2}$ is the wave number of the disturbances on the fluid layer while x and y are the horizontal component of the wave number α. After that, we substitute equation (9.19) into equations (9.14) to (9.16) and neglecting terms of the second and higher orders in the perturbations, we obtain the corresponding linearized equations involving only the $z-$components of the velocity, micro-rotation and temperature denoted by Θ, W, and G, respectively, we obtained

$$(1 + N_1)\left(D^2 - a^2\right)^2 W + N_1\left(D^2 - a^2\right)G - Ra^2\Theta = 0, \tag{9.20}$$

$$N_3\left(D^2 - a^2\right)G - 2N_1 G - N_1\left(D^2 - a^2\right)W = 0, \tag{9.21}$$

$$\left(D^2 - a^2\right)\Theta + f(z)\left(W - N_5 G\right) = 0, \tag{9.22}$$

where $= \frac{d}{dz}$. Eqs. (9.20) to (9.22) are solved subject to the appropriate boundary combinations as described in Table 9.2.

Table 9.2: Different Boundary combination for Rayleigh-Benard Convection

Case	Boundary Combination	Boundary condition
1	Lower free isothermal and upper	$W = \frac{d^2W}{dz^2} = \theta = G = 0$
	free isothermal, no spin (FIFI)	$W = \frac{d^2W}{dz^2} = \theta = G = 0$
2	Lower free isothermal and upper	$W = \frac{d^2W}{dz^2} = \theta = G = 0$
	free adiabatic, no spin (FIFA)	$W = \frac{d^2W}{dz^2} = D\theta = G = 0$
3	Lower free isothermal and upper	$W = \frac{d^2W}{dz^2} = \theta = G = 0$
	rigid adiabatic, no spin (FIRA)	$W = \frac{dW}{dz} = D\theta = G = 0$
4	Lower rigid isothermal and upper	$W = \frac{dW}{dz} = \theta = G = 0$
	free isothermal, no spin (RIFI)	$W = \frac{d^2W}{dz^2} = \theta = G = 0$
5	Lower rigid isothermal and upper	$W = \frac{dW}{dz} = \theta = G = 0$
	free adiabatic, no spin (RIFA)	$W = \frac{dW}{dz} = D\theta = G = 0$
6	Lower rigid isothermal and upper	$W = \frac{dW}{dz} = \theta = G = 0$
	rigid adiabatic, no spin (RIRA)	$W = \frac{dW}{dz} = D\theta = G = 0$

To find the critical eigenvalue, we apply the Galerkin technique method. The variables are written in a series of basis function as

$$W(z) = \sum_{i=1}^{n} A_i W_i(z),\ \Theta(z) = \sum_{i=1}^{n} B_i \Theta_i(z), \text{ and } G(z) = \sum_{i=1}^{n} C_i G_i(z), \tag{9.23}$$

where the trial function will be chosen respective to the boundary. The single term Galerkin expansion technique is used to find the critical eigenvalue. Substitute equation (9.23) into equations (9.20) to (9.22) and multiply equation (9.20) by $W_j(z)$, equation (9.21) by $G_j(z)$, equation (9.22) by $\Theta_j(z)$, perform integration by part with respect to z between $z = 0$ and 1, using the boundary conditions in Table 9.2 and trial functions as shown in Table 9.3, we obtain the following expression for Rayleigh number, R:

$$R = \frac{P\left\{A\left\langle WB^2W\right\rangle\left[N_3C - 2N_1\left\langle G^2\right\rangle\right] + DN_1^2C\right\}}{\alpha^2\left\langle\Theta W\right\rangle\left\{N_1N_5F\left\langle f(z)\Theta G\right\rangle - \left(N_3C + 2N_1\left\langle G^2\right\rangle\right)\left\langle f(z)\Theta W\right\rangle\right\}} \tag{9.24}$$

where

$$A = (1+N_1), B = \left(D^2-\alpha^2\right), C = \left\langle G\left(D^2-\alpha^2\right)G\right\rangle, D = W\left(D^2-\alpha^2\right)W,$$
$$E = \left\langle W\left(D^2-\alpha^2\right)G\right\rangle, F = \left\langle G\left(D^2-\alpha^2\right)W\right\rangle, P = \left\langle\Theta\left(D^2-\alpha^2\right)\Theta\right\rangle.$$

The angle bracket $\langle\ldots\rangle$ indicates the integration by parts with respect to z from 0 to 1, as for an example $\langle\Theta, W\rangle = \int_0^1 \Theta(z)W(z)dz$.

The trial functions which satisfy the combination of boundary conditions in Table 9.2 are shown in Table 9.3.

Table 9.3: Different Boundary combination for Rayleigh-Benard Convection

Case	Boundary Combination (lower and upper surface)	Trial Function
1	FIFI	$W_1 = Z^4 - 2Z^3 + Z$, $\Theta_1 = Z^2 - 2Z$, $G_1 = Z\,(1 - Z)$
2	FIFA	$W_1 = Z^3 - Z$, $\Theta_1 = Z^2 - 2Z$, $G_1 = Z\,(1 - Z)$
3	FIRA	$W_1 = Z^4 - 2Z^3 + 2Z$, $\Theta_1 = Z^2 - 2Z$, $G_1 = Z\,(1 - Z)$
4	RIFI	$W_1 = 2Z^4 - 5Z^3 + 3Z^2$, $\Theta_1 = Z^2 - Z$, $G_1 = Z\,(1 - Z)$
5	RIFA	$W_1 = 2Z^4 - 5Z^3 + 3Z^2$, $\Theta_1 = Z^2 - 2Z$, $G_1 = Z\,(1 - Z)$
6	RIRA	$W_1 = Z^4 - 2Z^3 + Z^2$, $\Theta_1 = Z^2 - 2Z$, $G_1 = Z\,(1 - Z)$

9.3 Results and Discussion

Numerical results in order to analyse the effect of basic temperature profile on the onset of Rayleigh-Benard convection will be discussed in detail. The value of critical Rayleigh number depends on the boundaries and its boundary combination as described in Table 9.2. To validate the analytical solution used, the comparison have been made with Siddeshwar and Pranesh [10] in the case of linear temperature gradient, $f(z) = 1$ for free-free isothermal boundaries as shown in Table 9.4.

Table 9.4: Critical Rayleigh number R_c for uniform temperature gradient.

	R_c	
N_1	Siddeshwar and Pranesh [10]	Present results
0.5	2700.05	2700.142
1.0	–	4743.604
1.5	–	8466.876
2	–	16978.105

We note that there is a close agreement between the results of present analysis and those obtained by Siddeshwar and Pranesh [10]. So, we can point out that the present study yields sufficiently accurate results. Table 9.4 also shows that as N_1 increases, the critical Rayleigh number R_c increases and it indicates the increase in the concentration of the microelements.

Fig. 17.1 is the plots of critical Rayleigh number, R_c as a function of coupling parameter N_1 for FIFI, FIFA, and FIRA boundaries, respectively and with two different cubic and a linear temperature gradients. As we can see, R_c increases with N_1 clearly. We note that, increasing in N_1 designated the increasing in the concentration of microelements. Increasing the number of microelements withN_1, greater part of the energy is consumed by these elements in evolving the gyrational velocities of the fluid and as a result onset of convection is delayed. The graphs of R_c as a function of couple stress parameter N_3 for FIFI, FIFA, and FIRA boundaries, respectively and with two different cubic and linear temperature gradients were

illustrated in Fig. 17.2. Clearly R_c decreases with increasing N_3 and ultimately levels off to a Newtonian value. We point out that, at only small values of N_3 couple stresses are operative and hence we observe that micro-rotations (small values of N_3) stabilise the system in comparison with the Newtonian value.

Fig. 17.3 is plots of R_c versus the micropolar heat conduction parameter N_5, for FIFI, FIFA, and FIRA boundaries, respectively and with a linear and two different cubic temperature gradients. From the graph, we can clearly see when N_5 increases, the heat induced into the fluid due to these microelements is also increased, thus reducing the heat transfer from bottom to the top. We can conclude that decreasing in heat transfer is responsible for delaying the onset of instability. Thus, increasing N_5 increases R_c.

From Figs. 17.1 to 17.3, we can observe the Cubic 1 is the most stable temperature gradient compare to Cubic 2 and linear. As a results, we find that the boundaries are:

$$R_c^{\mathrm{FIFA}} > R_c^{\mathrm{FIFI}} > R_c^{\mathrm{FIRA}}$$

where the superscripts correspond to the FIFA, FIFI and FIRA velocity boundary combinations respectively. We also show that the critical wave number is not sensitive to the changes of micropolar parameters.

We also compared Figs. 17.1 to 17.3 with Figs. 17.4 to 17.6 for different boundary conditions that was (RIFI, RIFA and RIRA). We observe that that the boundaries are:

$$R_c^{\mathrm{RIRA}} > R_c^{\mathrm{RIFI}} > R_c^{\mathrm{RIFA}}$$

where the superscripts correspond to the RIRA, RIFI and RIFA velocity boundary combinations. We also found that Cubic 1 temperature gradient is more stable than Cubic 2 and linear temperature gradient.

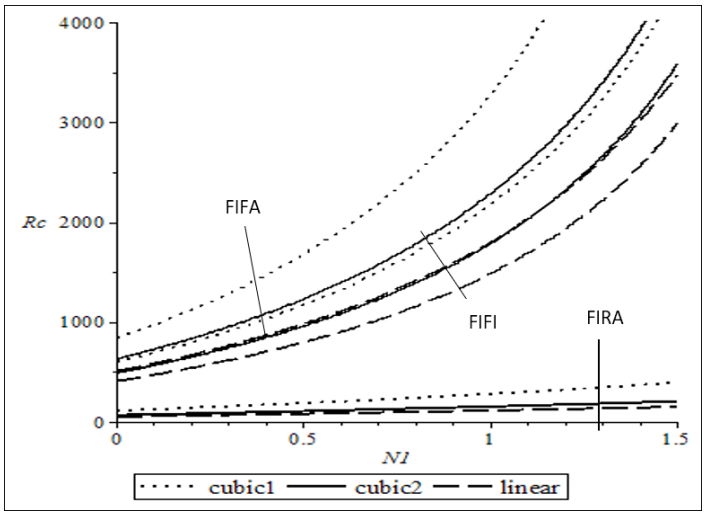

Figure 9.1: Plot of R_c versus N_1 with $N_3 = 2$, $N_5 = 1$ for FIFI, FIFA, and FIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

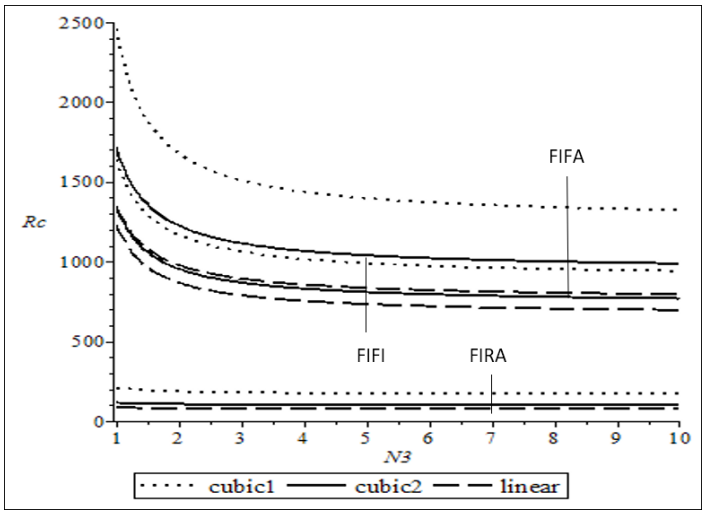

Figure 9.2: Plot of R_c versus N_3 with $N_1 = 0.5$, $N_5 = 1$ for FIFI, FIFA, and FIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

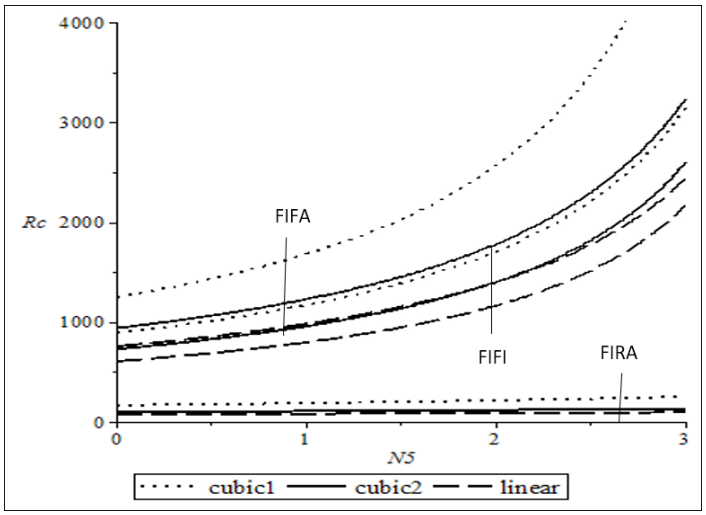

Figure 9.3: Plot of R_c versus N_5 with $N_1 = 0.5$, $N_3 = 2$ for FIFI, FIFA, and FIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

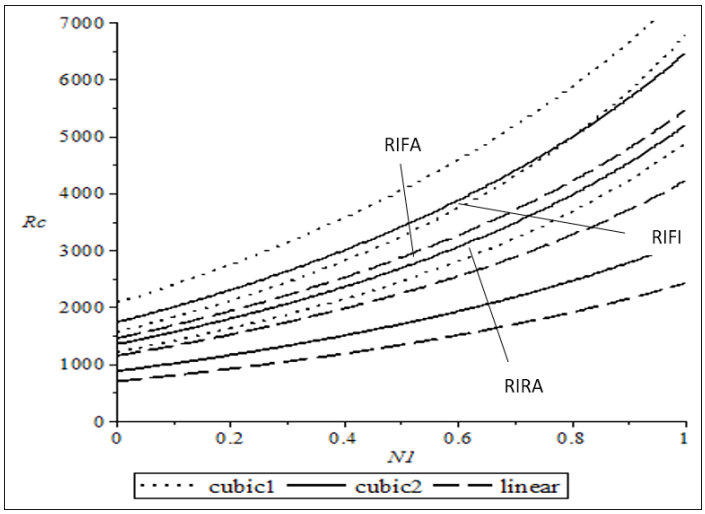

Figure 9.4: Plot of R_c versus N_1 with $N_3 = 2$, $N_5 = 1$ for RIFI, RIFA, and RIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

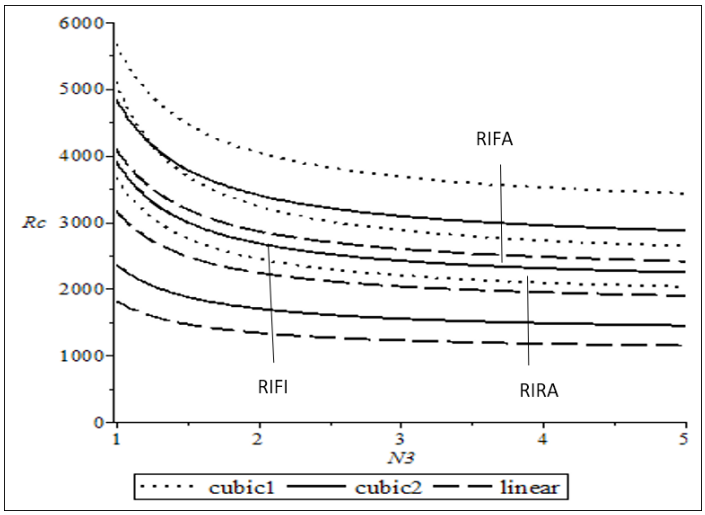

Figure 9.5: Plot of R_c versus N_3 with $N_1 = 0.5$, $N_5 = 1$ for RIFI, RIFA, and RIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

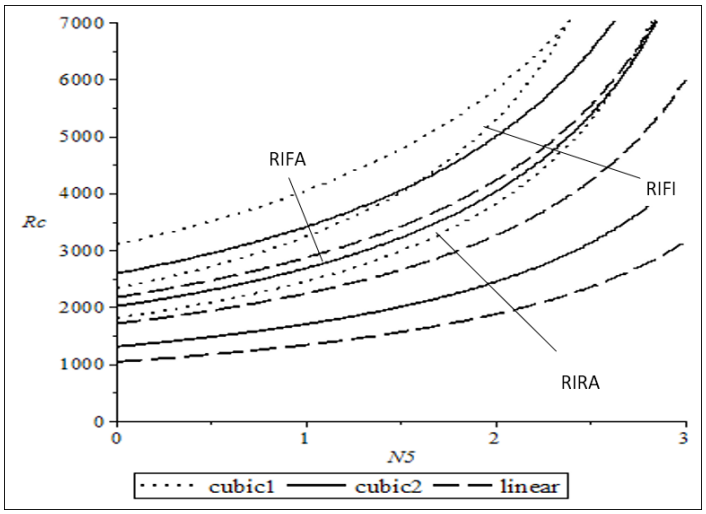

Figure 9.6: Plot of R_c versus N_5 with $N_1 = 0.5$, $N_3 = 2$ for RIFI, RIFA, and RIRA boundaries condition for Linear, Cubic 1, and Cubic 2 temperature gradients.

9.4 Conclusion

In this study, we use Single term Galerkin method to obtain the explicit analytical expression for the Rayleigh number which is use to perform the classical linear stability of Rayleigh-Bénard convection in horizontal micropolar fluids with cubic temperature profiles. The system is heated from below and various boundary conditions that are FIFI, FIFA, FIRA, RIFI, RIFA, RIRA horizontal boundaries are considered. We found the critical values of the Rayleigh number for system with FIRA horizontal boundaries is the most unstable boundaries combination while RIFA horizontal boundaries combination is the most stable boundaries combination. The coupling parameter, N_1, couple stress parameter, N_3, and micropolar heat conduction, N_5, has a significant effect on the onset of the Rayleigh-Benard convection. We also found that the Cubic 1 temperature profile shows the highest critical Rayleigh number, while Linear shows the lowest Rayleigh number. Thus, it is proven that Cubic 1 temperature profile can act as stabilizing system and the increase of the microelement concentration, N_1 and N_5 helps in delaying the onset of convection.

Bibliography

[1] Roberts PH (1969) Electrohydrodynamic convection. *Quarterly Journal of Mechanics and Applied Mathematics* **22**, 211–220.

[2] Char MI, Chiang KT (1994) Boundary effects on the Benard-Marangoni instability under an electric field. *Applied Scientific Research* **52**, 331–354.

[3] Idris R, Othman H, Hashim I (2009) On effect of non-uniform basic temperature gradient on Benard-Marangoni convection in micropolar fluid. *International Communications in Heat and Mass Transfer* **36**, 255–258.

[4] Mahmud MN, Hashim I, Idris R (2009) Effects of magnetic field and nonlinear temperature profile on Marangoni convection in micropolar fluid. *Differential Equations and Nonlinear Mechanics* **ID 748794**, 1–11.

[5] Idris R, Hashim I (2010) Effects of controller and cubic temperature profile on onset of Benard-Marangoni convection in ferrofluid. *International Communications in Heat and Mass Transfer* **37**, 624–628.

[6] Idris R, Hashim I (2011) On the effects of a cubic temperature profile on oscillatory Rayleigh-Benard convection in a viscoelastic fluid-filled high-porosity medium. *Journal of Porous Media* **14**, 437–447.

[7] Tanasawa I (1995) Experimental techniques in natural convection. *Experimental Thermal and Fluid Science* **10**, 503–518.

[8] Eringen AC (1966) Theory of micropolar fluids. *Journal of Mathematics and Mechanics* **16**, 1–35.

[9] Siddheshwar PG, Pranesh S (1997) Effect of a non-uniform basic temperature gradient on Rayleigh-Benard convection in a micropolar fluid. *Int. Journal of Eng. Science* **36**, 1183–1196.

[10] Siddeshwar PG, Pranesh S (2002) Magnetoconvection in fluids with suspended particles under 1g and μg. *Journal of Magnetism and magnetic materials* **219(2)**, 153–162.

[11] Dupont O, Hennenbergs M, Legrosy JC (1992) Marangoni-Benard instabilities under non-steady conditions. Experimental and theoretical results. *International Journal Heat Mass Transfer* **35**, 3237–3244.

[12] Chiang KT (2005) Effect of a non-uniform basic temperature gradient on the onset of Benard-Marangoni convection: stationary and oscillatory analyses, *International Communication in Heat and Mass Transfer* **32**, 192–203.

[13] Chandrasekhar S (1961) Hydrodynamic and Hydromagnetic Stability, Oxford University Press, Oxford.

Chapter 10

Effect of Cubic Temperature Gradient and Internal Heat Generation on the Onset of Marangoni Electro Convection with Feedback Control in a Micropolar Fluid

Nurul Afiqah Mohd Isa[1], **Siti Suzilliana Putri Mohamed Isa**[2,*], Norihan Md Arifin[1,3], Norfifah Bachok[1,3]

[1] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: ctsuzilliana@upm.edu.my

Abstract

The linear stability analysis is carried out to investigated the influence of non-uniform basic temperature gradients in the presences of internal heat generation, electric field and feedback control on the onset of Marangoni convection in a micropolar fluid. For an upper free adiabatic and lower rigid isothermal boundaries, the eigenvalue are obtained. Then, Galerkin method is applied to solved the eigenvalue. The effect of internal heat generation, Q, electric number, L and feedback control on the onset of Marangoni convection has been figure out. Three non-uniform basic profiles of the temperature are studied and several general conclusions about their destabilizing effects are revealed. Different value of internal heat generation, Q , electric number and feedback control are add together to investigate their existence either it will delay or enhance the onset of electro convection.

Keywords: Marangoni convection, feedback control, internal heat generation, electric field, micropolar fluid.

10.1 Introduction

The convective in a thin fluid is occured when the fluid is heated from below. Therefore, the industrial applications of thin fluid convection can be seen in material processing technologies. In addition, Marangoni convection arises due to the various

rate of surface tension, where this variation is caused by the existence of temperature distribution. The contribution of Marangoni convection can be observed in the production of detergents, molten salts and crystal growth. Pearson [1]produced the first report on Marangoni convection, and followed by the others with the case of magnetohydrodynamic Marangoni convection: Smith [2], Rudraiah and Ramachanramurthy [3], Wilson [4], Hashim and Arifin [5, 6] and Arifin and Hashim [7].

The influence ofvarious types of temperature gradients (uniform and non-uniform) on Marangoni convection was studied by Vidal [8], Debler [9], and Nield [10]. Friedrich [11] performed numerical analysis the effect of non-uniform basic temperature gradient on rotating Marangoni convection. Idris et al. [12] considered the influence of cubic basic state temperature profile on their report. Isa et al. [13] and Gupta [14] studied on Marangoni convection in a boundary slab of finite conductivity and relatively hotter or cooler layer of liquid respectively. The magnetohydrodynamics Marangoni convection with non-linear basic temperature gradient was analysed by Shivakumara [15] and Mahmud [16]. The impact of feedback control on Rayleigh-Benard-Marangoni convection in dielectric Eringens micropolar fluid was treated by Azmi and Idris [17], subjected by the existence of non-uniform basic temperature gradients.

From the previous works, the model of Marangoni electro convection in the presence of feedback control and internal heat generation in micropolar fluid as well as the effects of cubic basic temperature gradient is still not being reported. Therefore, the main objective of this research work is analyse the influence of linear and two cubic basic temperature gradients on the onset of electro convection with internal heat generation in the presence of feedback control in a horizontal micropolar fluid.

10.2 Mathematical Formulation

Let consider the infinite horizontal layer of a Boussinesquian micropolar fluid layer of depth, d where the fluid is heated from below by internal heat generation with existence of an electric field. The stability of micropolar fluid at horizontal layer in the presence of internal heat generation, feedback control, and electric field is analysed. The electric field towards to z-axis is in uniform state. A cartesian co-ordinate system (x, y, z) is taken with origin in the lower boundary and z-axis vertically upwards. Next, the temperature difference at the boundaries which is the upper and lower surface denotes as ΔT. The body forces acting on the fluid are electric field, surface tension, internal heat generation and feedback control. The governing equations for the Marangoni situation in a micropolar fluid with internal heat generation are

Continuity equation:

$$\nabla \cdot q = 0, \tag{10.1}$$

Conservation of linear momentum:

$$\rho_0 \left[\frac{\partial q}{\partial t} + (q \cdot \nabla) q \right] = -\nabla p + (2\zeta + \eta)\nabla^2 q + \zeta(\nabla \times \omega) + (P \cdot \nabla)E, \tag{10.2}$$

Conservation of angular momentum:

$$\rho_0 I\left[\frac{\partial \omega}{\partial t}+(q\cdot\nabla)\omega\right]=(\lambda'+\eta')\nabla(\nabla\cdot\omega)+(\eta'\nabla^2\omega)+\zeta(\nabla\times q-2\omega), \tag{10.3}$$

Conservation of energy:

$$\frac{\partial T}{\partial t}+(q\cdot\nabla)T=\frac{\beta}{\rho_0 C_v}(\nabla\times\omega)\cdot\nabla T+\chi\nabla^2 T+h_g, \tag{10.4}$$

Equation of state:

$$\rho=\rho_0[1-\alpha(T-T_0)], \tag{10.5}$$

Equation of state for dielectric constant:

$$\varepsilon_r=(1+\chi_e)-e(T-T_0), \tag{10.6}$$

Faraday's law:

$$\begin{aligned}\nabla\times E&=0,\\ E&=-\nabla\phi,\end{aligned} \tag{10.7}$$

Equation of polarization field:

$$\begin{aligned}\nabla\cdot(\varepsilon_0 E+P)&=0,\\ P&=\varepsilon_0(\varepsilon_r-1)E,\end{aligned} \tag{10.8}$$

where $\vec{q}$ is the velocity, ρ_0 is the density at of the fluid at a reference temperature $T=T_0$, t is the time, T is the temperature, p is the pressure term, ρ is the density, $\hat{k}$ is the unit vector in z-direction, g is the acceleration due to gravity, ζ is the coupling viscosity coefficient, I is the moment of inertia, η is the shear kinematic viscosity coefficient, ω is the spin, λ' and η' are the bulk and shear spin viscosity coefficient, β is the micropolar heat conduction coefficient, C_v is the specific heat, χ is the thermal conductivity, α is the coefficient of thermal expansion, χ_e is the thermal susceptibility, h_g is the overall uniformly distributed volumetric internal heat generation within micropolar fluid layer, ϕ is the electrostatic potential, ε_0 is electric permeability of free space, ε_r is dielectric constant, P is dielectric polarization, E is the electric field.

The basic state of the fluid is quiescent and describe by:

$$\begin{aligned}&q_b=0,\quad \omega_b=0,\quad p=p_b(z),\quad \rho=\rho_b(z),\quad E=E_b(z),\\ &T=T_b(z),\quad \frac{-d}{\Delta T}\frac{dT_b}{dz}=f(z).\end{aligned} \tag{10.9}$$

Here $f(z)$ is shows the non-uniform basic temperature gradient. Linear, cubic 1 and cubic 2 temperature gradients are considered in this paper as illustrated in Table 1. Equation (10.1)-(10.8) in the basic state specified by Equation (10.9) will become:

$$\begin{aligned}\frac{dp_b}{dz}&=P_b\frac{\partial E_b}{\partial z},\\ \frac{d^2T_b}{dz^2}&=-\frac{h_g}{\chi},\end{aligned}$$

Table 10.1: Reference steady-state temperature gradient

Model	Reference steady-state temperature gradient	$f(z)$	a_1^*	a_2^*	a_3^*
1	Linear	1	1	0	0
2	Cubic 1	$3(z-1)^2$	0	0	1
3	Cubic 2	0.6+1.02(z-1)ˆ2	0.6	0	0.34

$$\begin{aligned} \rho_b &= \rho_0[1-\alpha(T_b-T_0)], \\ \varepsilon_r &= (1+\chi_e)e(T_b-T_0), \\ E_b &= \left[\frac{(1+\chi_e)E_0}{(1+\chi_e)+\frac{e\Delta T}{h}z}\right], \\ P_b &= \varepsilon_0 E_0(1+\chi_e)\left[1-\frac{1}{(1+\chi_e)+\frac{e\Delta T}{h}z}\right]. \end{aligned} \tag{10.10}$$

Consider the basic state be disturbed by an infinitesimal thermal perturbation, then

$$\begin{aligned} q = q_b + q', \omega = \omega_b + \omega', p = p_b + p', E = E_b + (E_1' + E_3'), \\ \rho = \rho_b + \rho', T = T_b + T', P = P_b + (P_1' + P_3'). \end{aligned} \tag{10.11}$$

The subscript b denotes as basic state value and the primes referring to the quantities are infinitesimal perturbations. From Equations (10.8), on linearization yields

$$\begin{aligned} P_i' &= \varepsilon_0\chi_e E_i' \quad \text{for} \quad i = 1,2 \\ P_3' &= \varepsilon_0\chi_e E_3' - e\varepsilon_0 E_0 T' \end{aligned} \tag{10.12}$$

The second equation of Equation (10.7) can be written as $E = -\nabla\phi'$, where ϕ' is the perturbed electric scalar potential. Acquainting the electric potential ϕ' and substituting Equation (10.11) into Equation (10.1)-(10.8) by using Equation (10.10). Then, the equation reduce in the form:

$$\nabla \cdot q' = 0, \tag{10.13}$$

$$\rho_0\left[\frac{\partial q'}{\partial t}\right] = -\nabla p + (2\zeta+\eta)\nabla^2 q' + \zeta(\nabla\times\omega') + (P_b\cdot\nabla)E' + (P'\cdot\nabla)E_b, \tag{10.14}$$

$$\rho_0 I\left[\frac{\partial\omega'}{\partial t}\right] = (\lambda'+\eta')\nabla(\nabla\cdot\omega') + (\eta'\nabla^2\omega') + \zeta(\nabla\times q' - 2\omega'), \tag{10.15}$$

$$-W\frac{\Delta T}{d}f(z) = \frac{\beta}{\rho_0 C_v}\left[\nabla\times\omega'\cdot\left(-\frac{\Delta T}{d}f(z)\hat{k}\right)\right]\cdot\nabla T + \chi\nabla^2 T' + \left(\frac{zh_q}{\chi} - \frac{dh_q}{2\chi} + \frac{\Delta T}{d}\right)W, \tag{10.16}$$

$$\rho' = -\alpha\rho_0 T', \tag{10.17}$$

$$\varepsilon' = -\varepsilon_0 e T', \tag{10.18}$$

$$\nabla\cdot(\varepsilon_0 E' + P') = 0. \tag{10.19}$$

Next, using Equation (10.17) in Equation (10.14), operating curl twice on the resulting equation, operating curl on Equation (10.15), using Equation (10.12) on Equation (10.19). The perturbation Equation (10.13)-(10.16) are non dimensionalised using the following definition:

$$(x^*, y^*, z^*) = \frac{(x, y, z)}{d}, \quad W^* = \frac{W'}{(\chi/d)}, \quad \omega^* = \frac{\omega'}{(\chi/d^2)}, \quad t^* = \frac{t}{(d^2/\chi)},$$

$$T^* = \frac{T'}{\Delta T}, \quad \phi^* = \frac{\phi'}{(eE_0\Delta T d/1+\chi_e)}, \quad \Omega^* = \frac{\nabla \times w}{(\chi/d^3)}. \tag{10.20}$$

We get,

$$(1+N_1)\nabla^4 W + N_1\nabla^2\Omega_z + L\nabla_1^2 T f(z) - L\frac{\partial}{\partial z}(\nabla_1^2\phi)f(z) = 0, \tag{10.21}$$

$$N_3\nabla^2\Omega_z - N_1\nabla^2 W - 2N_1\Omega_z = 0, \tag{10.22}$$

$$\nabla^2 T + [1 - Q(1-2z)]Wf(z) - N_5\Omega_z f(z) = 0, \tag{10.23}$$

$$\nabla^2\phi - \frac{\partial T}{\partial z} = 0, \tag{10.24}$$

where the asterisks have been dropped for simplicity. Here, the non-dimensional parameters N_1, N_3, N_5, L and Q are defined as

$$N_1 = \frac{\zeta}{\zeta+\eta} \quad \text{(Coupling Parameter)},$$
$$N_3 = \frac{\eta}{(\zeta+\eta)d^2} \quad \text{(Couple Stress Parameter)},$$
$$N_5 = \frac{\beta}{\rho_0 C_v d^2} \quad \text{(Micropolar Heat Conduction Parameter)},$$
$$L = \frac{\varepsilon_0 e^2 E_0^2 \Delta T d^2}{(1+\chi_e)(\zeta+\eta)\chi} \quad \text{(Electric number)},$$
$$Q = \frac{h_g d^2}{2\chi\nabla T} \quad \text{(Heat source strength)}.$$

Next, the perturbation quantities are

$$(W, \Omega_z, T, \phi) = [W(z), G(z), T(z), \phi(z)]\exp[i(l_x x + m_y y)], \tag{10.25}$$

where $W(z), G(z), T(z)$ and $\phi(z)$ are amplitudes of the perturbation of vertical velocity, spin, temperature and electrostatic potential. l and m are the horizontal component of the wave number $\boldsymbol{a}$.

Substituting Equation (10.25) into Equation (10.21)-(10.24), we get

$$(1+N_1)(D^2-a^2)^2 W + N_1(D^2-a^2)G - La^2 T f(z) + La^2 D\phi f(z) = 0, \tag{10.26}$$

$$N_3(D^2-a^2)G - N_1(D^2-a^2)W - 2N_1 G = 0, \tag{10.27}$$

$$(D^2-a^2)T + [1-Q(1-2z)]Wf(z) - N_5\Omega_z f(z) = 0, \tag{10.28}$$

$$(D^2-a^2)\phi - DT = 0, \tag{10.29}$$

where $D = \frac{d}{dz}$. According to Bau [19] in their proportional feedback control strategy, in order to let the sensor to locate any undesirable disturbances, several types of individually controlled actuators equipped positioned directly beneath it. $q(t)$ known as

the determination of a control can be accomplished using the proportional-integral-differential (PID) controller of the form

$$q(t) = r + K[e(t)] \quad \text{where} \quad e(t) = \hat{m}(t) + m(t), \tag{10.30}$$

where $e(t)$ is an error or deviation from the measurement, r is the calibration of the control,, $m(t)$, $K = K_p + K_D d/dt + K_l \int_0^t dt$ with K_p is the proportional gain, $\hat{m}(t)$ from some desired or reference value, K_D is the differential gain and K_l is the integral gain. Refer to Bau [19], the actuator modifies the heated surface temperature using a proportional relationship between the upper, $z = 1$ and the lower, $z = 0$ thermal boundaries for perturbation field for one sensor plane and proportional feedback control

$$T'(x, y, 0, t) = -KT'(x, y, 1, t), \tag{10.31}$$

where T' indicates the deviation of the fluid's temperature from its conductive state and the scalar controller gain in terms of K will be used to control our system.

Equation (10.26)-(10.29) are solved subject to the following boundary conditions:

$$W = DW = T = G = T(0) + KT(1) = 0, \quad \text{at} \quad z = 0, \tag{10.32}$$

$$W = D^2W + a^2MT = DT = G = 0, \quad \text{at} \quad z = 1, \tag{10.33}$$

The single term Galerkin expansion technique is used to find the critical eigenvalue. Multiply Equation (10.26) by W, Equation (10.27) by G, Equation (10.28) by T, and Equation (10.29) by ϕ respectively. The resulting equations is solved by integration by parts with respect to z between $z = 0$ and $z = 1$. Then, by applying the boundary condition in Equation (10.32)-(10.33) and the trial function where $W = AW_1, G = BG_1, T = CT_1$ and $\phi = \phi_1$, reduce to Marangoni number M:

$$M = \frac{La^2C_3C_4 - C_2[< T_1(D^2 - a^2)T_1 > + KT(1)]}{(1 + N_1)a^2T(1)DW(1)C_3}, \tag{10.34}$$

where

$$\begin{aligned}
C_1 &= N_3\langle G_1(D^2 - a^2)G_1\rangle - 2N_1\langle G_1^2\rangle,\\
C_2 &= (1 + N_1)\langle W_1(D^2 - a^2)^2W_1\rangle C_1 + N_1^2\langle G_1(D^2 - a^2)W_1\rangle\langle W_1(D^2 - a^2)G_1\rangle,\\
C_3 &= N_1N_5\langle G_1(D^2 - a^2)W_1\rangle\langle T_1G_1f(z)\rangle - Q\langle T_1W_1f(z)\rangle C_1,\\
C_4 &= \langle W_1T_1f(z)\rangle - \frac{\langle W_1D\phi_1f(z)\rangle\langle\phi_1DT_1\rangle}{\langle\phi_1(D^2 - a^2)\phi_1\rangle}.
\end{aligned}$$

In the equation (10.34), $\langle ... \rangle$ denotes the integration by parts with respect to z between $z = 0$ and $z = 1$.

We choose the trial functions for lower rigid isothermal and upper free adiabatic. The trial functions that satisfying boundary condition are:

$$W_1 = Z^4 - \tfrac{5}{2}Z^3 + \tfrac{3}{2}Z^2, \quad T_1 = Z(Z - 2), \quad G_1 = Z(1 - Z), \phi_1 = Z^2(3 - 2Z), \tag{10.35}$$

Such that they all satisfy the boundary conditions in (10.31) and (10.32). But, $D^2W + a^2MT = 0$ at $z = 1$ is the only one not satisfy the boundary conditions.

However, the residual from this is included in the residual from the differential equations.

10.3 Results and Discussion

This study set out to determine the effects of cubic basic temperature gradient on the onset of Marangoni electro convection with the presence of internal heat generation and feedback control in a micropolar fluid. One uniform (Linear) and two non-uniform (Cubic 1 and Cubic 2) temperature gradient are considered in this paper. We choose upper free adiabatic and lower rigid isothermal surface boundaries in this work. First, we consider the results of non-uniform temperature gradient without the effect of feedback control, internal heat generation and Rayleigh Benard number ($Q = 0, K = 0, R = 0$). The results of comparison between the present results and Mokhtar et al. [18] are shown in Table 1. The table provides the comparison of the critical value of Marangoni number, M_c with various N_1 and internal heat generation, Q for linear temperature gradient cases when, $N_3 = 2, N_5 = 1$ and $L = 0$ in a micropolar fluid layer. In this table, we compared our result with Mokhtar et al. [18] for $K = 0, R = 0$ and the present study for $Q = 0$, thus the findings are in good agreement. We continue our finding by substituting $Q = 2, 4, 6$ and our finding revealed that for all N_1 values considered, the critical number of Marangoni decreases when we increase the value of Q. Thus, the results reveal the onset of Marangoni convection will destabilize the system if and only if the Q increase in micropolar fluid by the presence of electric field.

The variation of critical Marangoni number M_c againts the coupling parameter N_1 for lower rigid isothermal and upper free adiabatic boundaries for $L = 100$, $Q = 2, 4$, $K = 0, 2, 4$ and for three types of different non-uniform basic temperature gradients (linear, cubic 1, cubic 2) are shown in Figure 10.1 to 10.3. In these figures shown that increasing N_1 has the effect of increment in critical marangoni number. Hence, we can conclude that the onset of convection is delayed.

Table 10.2: Comparison of critical Marangoni number when $N_3 = 2$, $N_5 = 1$ and $L = 0$.

N_1	M_c				
	Mokhtar et. al. [18]	Present Study			
	$K = 0, R = 0$	$Q = 0$	$Q = 2$	$Q = 4$	$Q = 6$
0.5	98.573	98.573	54.146	37.325	28.478
1.0	-	129.884	62.337	41.009	30.555
1.5	-	185.464	72.718	45.215	32.807
2.0	-	309.917	86.299	50.078	35.266

Moreover, the onset of convection will be also delayed when the internal heat generation value increase as critical marangoni number decrease. This mean, the internal heat generation can control the stabilization in the system. As we can see, the system be more stable if only if the feedback control value is increasing. We also observed that the increasing of internal heat generation and electric number, the number of critical marangoni will decrease. Then, as a results electric number will destabilizes the system. Besides that, from the graph we can see that Cubic 1

temperature gradient with $a_1^* = 0$, $a_2^* = 0$, $a_3^* = 1$ is the most stable among linear and cubic 2 temperature gradients. Thus, we find that,

$$M_L < M_{C2} < M_{C1}$$

Figure 10.4 to 10.6 are the illustrations of the critical Marangoni number againts couple stress parameter N_3 for lower rigid isothermal and upper free adiabatic boundaries for certain values of electric number $L = 100$, internal heat generation, $Q = 2, 4$, feedback control, $K = 0, 2, 4$, and for different types of non-uniform basic temperature gradients (linear, cubic 1, cubic 2). We note that couple stress in the conservation of angular momentum equation played a role by the shear stress in the same equation. From our observation, we can see that the value of N_3 increase will decrease the value of critical marangoni number, M_c. Thus from this incident, the couple stress of the fluid will decrease and affected the decreasing in micro-rotation hence it will make the system becomes unstable. The internal heat generation will delay the onset of convection and control the stability of the system because when the values of internal heat generation increase as critical marangoni number decrease. Meanwhile, the increasing value of feedback control will make the system becomes more stable. But the internal heat generation and electric number have the same effect as the previous study that was increasing in both parameters will decrease the critical marangoni number thus it will destabilize the system. Then, from the graph we can conclude that linear temperature gradient with $a_1^* = 1$, $a_2^* = 0$, $a_3^* = 0$ is the most destabilizing temperature gradients compared to cubic 1 and cubic 2.

The plots of critical Marangoni number againts couple stress parameter N_5 for lower rigid isothermal and upper free adiabatic boundaries for certain values of electric number $L = 100$, internal heat generation, $Q = 2, 4$ with feedback control, $K = 0, 2, 4$, and for different types of non-uniform basic temperature gradients (linear, cubic 1, cubic 2) is shown in figure 10.7 to 10.9. We noted that N_5 indicates the micropolar heat conduction parameter. From the graph, we can observe that increasing N_5 will increase the value of critical marangoni number. This incident can causes the increasing of the microelements in the system and it also influenced the increment of heat induced into the fluid. Thus, the heat transfer from bottom to the upper will reduce and we can conclude the onset of convection will be delayed. The internal heat generation can act as controller of the stability of the system because when the values of internal heat generation increase, the critical marangoni number will decrease. Thus, it will enhance the onset of convection of every temperature gradient. From the graph, we also find out that the increasing value of feedback control will make the system becomes more stable. Hence, the presence of feedback control will enhance the stability of the system. But the presence of internal heat generation and electric number play role as destabilizing effect on the system because whenever the value of electric number increase, the critical marangoni number will decrease. Then, from the graph also we can conclude that linear temperature gradient with $a_1^* = 1$, $a_2^* = 0$, $a_3^* = 0$ is the most destabilizing temperature gradient and cubic 1 with $a_1^* = 0$, $a_2^* = 0$, $a_3^* = 1$ is the most stabilizing temperature gradient.

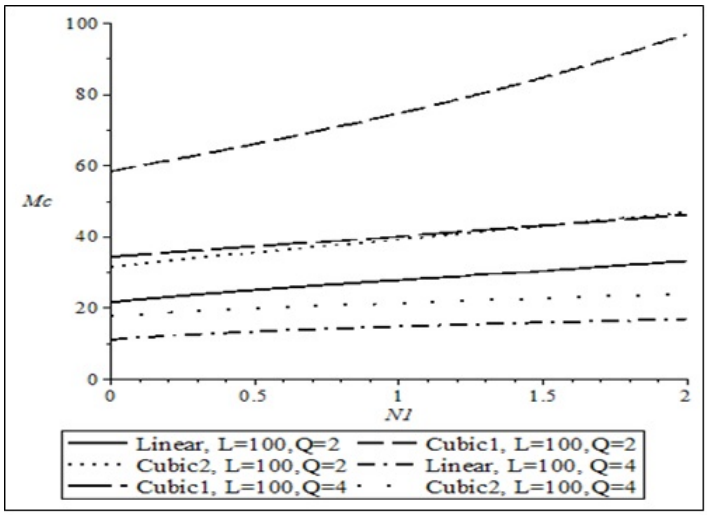

Figure 10.1: Plot of M_c versus N_1 for $Q = 2, 4$ with $N_3 = 2$, $N_5 = 1$ for $K = 0$ and $L = 100$.

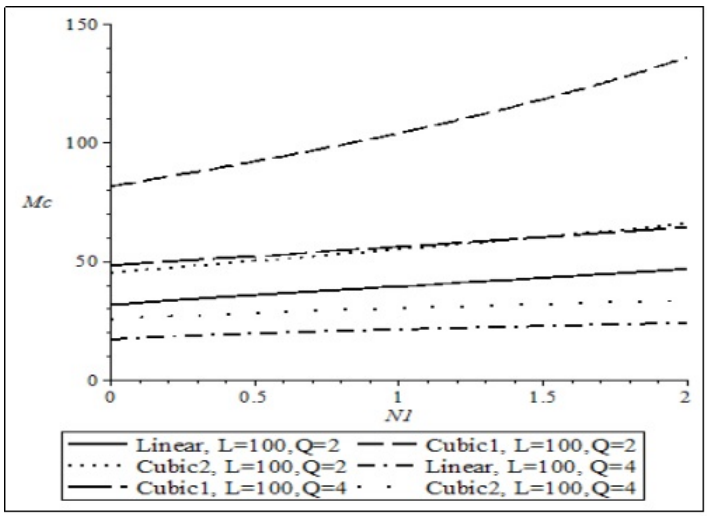

Figure 10.2: Plot of M_c versus N_1 for $Q = 2, 4$ with $N_3 = 2$, $N_5 = 1$ for $K = 2$ and $L = 100$.

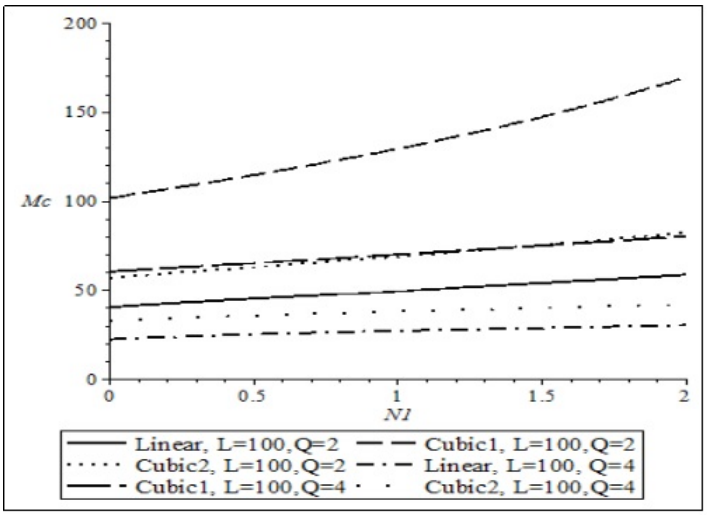

Figure 10.3: Plot of M_c versus N_1 for $Q = 2, 4$ with $N_3 = 2$, $N_5 = 1$ for $K = 4$ and $L = 100$.

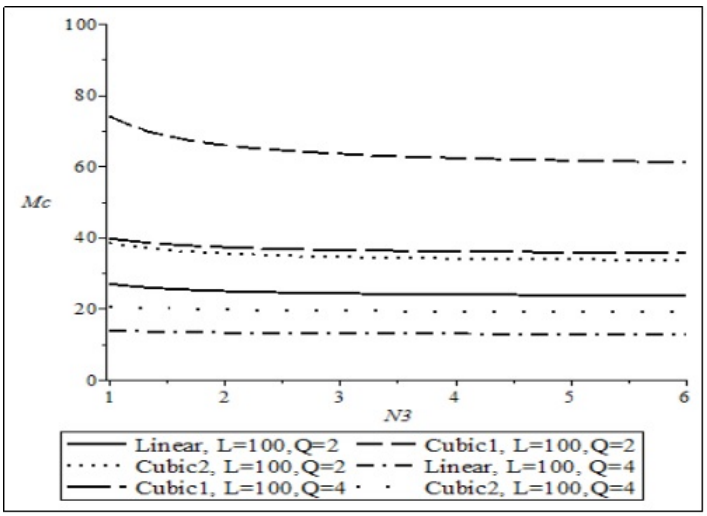

Figure 10.4: Plot of M_c versus N_3 for $Q = 2, 4$ with $N_1 = 0.5$, $N_5 = 1$ for $K = 0$ and $L = 100$.

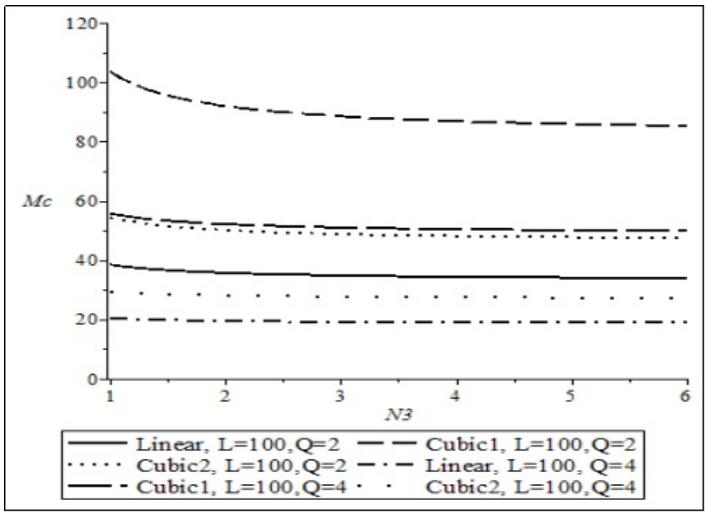

Figure 10.5: Plot of M_c versus N_3 for $Q = 2, 4$ with $N_1 = 0.5$, $N_5 = 1$ for $K = 2$ and $L = 100$.

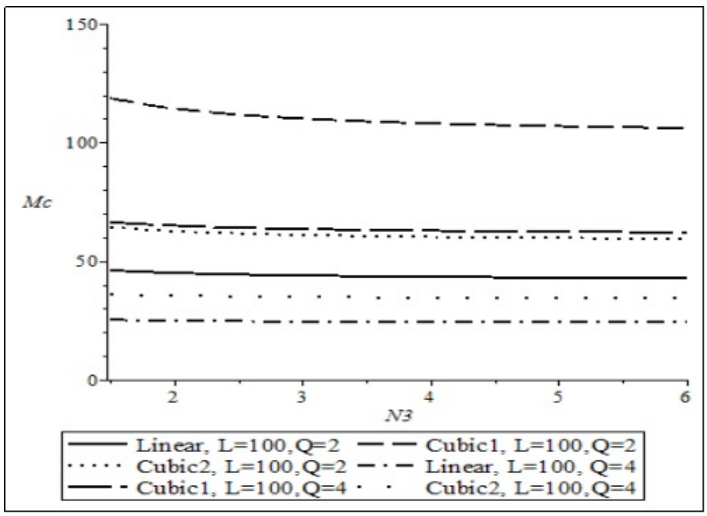

Figure 10.6: Plot of M_c versus N_3 for $Q = 2, 4$ with $N_1 = 0.5$, $N_5 = 1$ for $K = 4$ and $L = 100$.

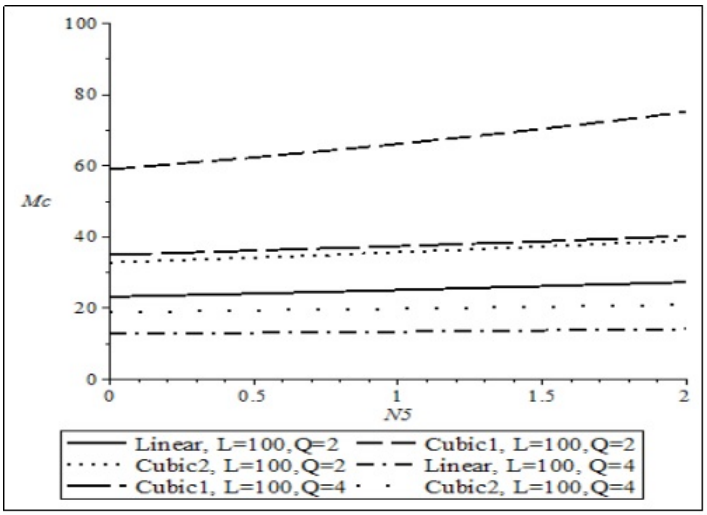

Figure 10.7: Plot of M_c versus N_5 for $Q = 2, 4$ with $N_1 = 0.5$, $N_3 = 2$ for $K = 0$ and $L = 100$.

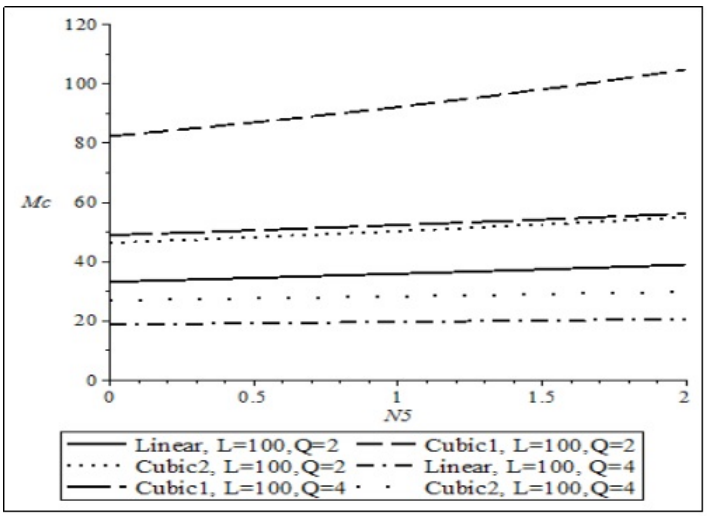

Figure 10.8: Plot of M_c versus N_5 for $Q = 2, 4$ with $N_1 = 0.5$, $N_3 = 2$ for $K = 2$ and $L = 100$.

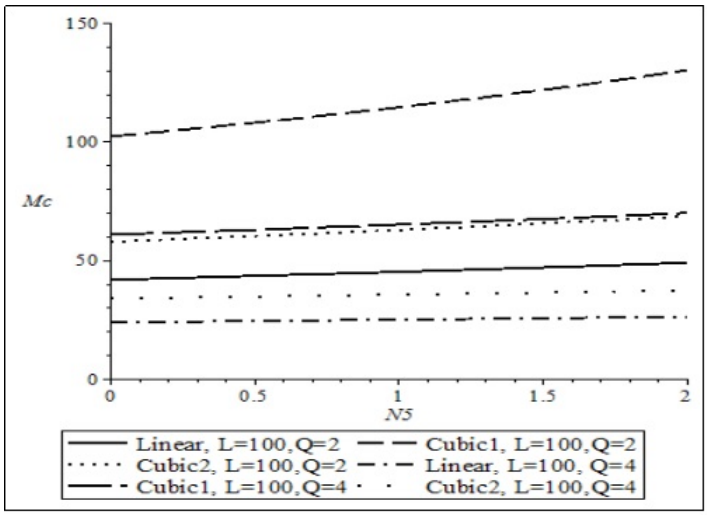

Figure 10.9: Plot of M_c versus N_5 for $Q = 2, 4$ with $N_1 = 0.5$, $N_3 = 2$ for $K = 4$ and $L = 100$.

10.4 Conclusion

The present study was designed to determine the classical linear stability analysis to analyse the effect of internal heat generation, and different type of temperature gradients profiles with the presence of feedback control on the onset of Marangoni convection in a dielectric micropolar fluid. Our findings prove that the presence of internal heat generation will helped in enhancing the onset of convection in dielectric micropolar fluid. The presence of feedback control will enhance the stability of the system. In addition, Electric number which plays the role as a destabilizing effect on the system will enhance the onset of thermal convection. Also, The basic temperature gradients used in the model are linear, Cubic 1 and Cubic 2. As a result, Cubic 1 is the most stable. Besides, the appropriate temperature gradient for experimental works in microgravity environment is Cubic 2. Therefore, we concluded that the internal heat generation with the presence of dielectric field mechanism has a destabilizing effect on the system.

Acknowledgement

The present research was partially supported by the Putra Grant with Project Number GP-IPM/2018/9596900.

Bibliography

[1] Pearson, J.R.A. (1958). *On Convection Cells Induced by Surface Tension*, Journal of Fluid Mechanics, Vol 4, 489–500.

[2] Smith, K. A. (1966). *On Convective Instability Induced by Surface Tension Gradient*, J. Fluid Mech, Vol 27, 646–654.

[3] Rudraiah, N., and Ramachandramurthy, V. (1985). *Effects of Magnetic Field and Non-Uniform Temperature Gradient on Marangoni Convection*, Int. J. Heat Mass Transfer, Vol 28, 1621–1624.

[4] Wilson, S. K. (1997). *The effects of uniform internal heat generation on the onset of steady Marangoni convection in a horizontal layer of fluid*, Acta Mechanica, Vol 124, 63–78.

[5] Hashim, I and Arifin, N. M (2003). *Oscillatory Marangoni convection in a conducting fluid layer with a deformable free surface in the deformable free surface in the presence of a vertical magnetic field*, Acta Mechanica, Vol 164(3–4), 199–215.

[6] Hashim, I and Arifin, N. M (2005). *The effect of a magnetic field on the linear growth rates of Bénard-Marangoni convection*, Microgravity Science and Technology, Vol 17(2), 5–8.

[7] Arifin, N.M and Hashim 1, (2004). *Growth rates of Bénard-Marangoni convection in a fluid layer in the presence of a magnetic field*, Microgravity Science and Technology Vol 15(1), 22–27.

[8] Vidal, A. and Acrivos, A. (1966). *Nature of the Neutral State in Surface Tension Driven Convection*, Phys. Fluids, 9, 615–616.

[9] Debler, W. R. and Wolf, L. F. (1970). *The Effect of Gravity and Surface Tension Gradients on Cellular Convection in Fluid Layers with Parabolic Temperature Profiles*, J. Heat Transfer, Vol 92, 351–358.

[10] Nield, D.A. (1975). *The onset of Transient Convective Instability*, J. Fluid Mech, Vol 71, 441–454.

[11] Friedrich, R. and Rudraiah, N. (1984). *Marangoni Convection in a Rotating Fluid Layer with Non-uniform Temperature Gradient*, Int. J. Heat Mass Transfer, Vol 3, 443–449.

[12] Idris, R., Othman, H., and Hashim, I. (2009). *Effect of Cubic Temperature Profile on Marangoni Convection in Micropolar Fluid*, Proc. Int. Conf. on Fluid Mechanics, Vol 6, 11–14.

[13] Isa, S. S. P. M., Arifin, N. M., and Saad, M. N. (2008). *Effect of Magnetic Field on the onset of Marangoni Convection in a Fluid Layer with Non-Uniform Basic Temperature*, Proc. Simposium Kebangsaan Sains Matematik, Vol 16, 280–287.

[14] Gupta, A. K. and Kalta S. K. (2016).]*Effect of Non-Uniform Temperature Gradient on Marangoni Convection in a Relatively Hotter or Cooler Layer of Liquid*, Math. J. of Interdisciplinary Sciences, Vol 4, 121–134.

[15] Shivakumara, I. S., Suma, S. P., and Gangadharaiah, Y. H. (2011). *Effect of Non-Uniform Basic Temperature Gradient on Marangoni Convection with a Boundary Slab of Finite Conductivity*, Int. J. of Eng. Sciences and Technology, Vol 3, 4151–4160.

[16] Mahmud, M.N., Idris, R., and Hashim, I. (2009). *Effects of Magnetic Field and Nonlinear Temperature Profile on Marangoni Convection in Micropolar Fluid*, Differential Equations and Nonlinear Mech. ID748794, 1–11.

[17] Azmi, H. M. and Idris, R. (2014). *Effects of Controller and Nonuniform Temperature Profile on the Onset of Rayleigh-Bénard-Marangoni Electroconvection in a Micropolar Fluid*,Journal of Applied Mathematics, ID 571437, 1–8.

[18] Mokhtar, N. F., Khalid, I. K., and Ariffin, N.M. (2013). *Efffect of Internal Heat Generation on Benard-Marangoni Convection in Micropolar Fluid with Feedback Control Effect*, Contemporary Mathematics, Mathematical Physics and Their Application. Vol 435, 1—5.

[19] Bau H. H. (1999). *Control of Marangoni-Benard convection*, International Journal of Heat and Mass Transfer. Vol 42(7), 1327–1341.

Chapter 11

Stability Analysis of Radiation Effect on MHD Thermosolutal Marangoni Convection in the Presence of Heat and Mass Generation or Consumption with Permeable Surface

Norfarahanim Mohd Ariffin[1], **Yong Faezah Rahim**[2,*], Norihan Md Arifin[1,3], Norfifah Bachok[1,3]

[1] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang Selangor, Malaysia.

*Corresponding author: yfaezah@upm.edu.my

Abstract

The characteristics of the fluid flow and heat transfer of magnetohydrodynamic (MHD) thermosolutal Marangoni convection in the presence of heat and mass generation or consumption with radiation through permeable surface is studied in this paper. The basic governing partial differential equations transformed into nonlinear ordinary differential equation using the similarity transformation and solved numerically. The analysis is done to analyse the effect of radiation and suction/injection on the flow of the fluid and the features of the problem are generalize in form of tables and figures. The result obtained are then compared with the previous work on which dual solutions exist, thus a stability analysis is performed in this present paper to determine the physical realizable solution of the problems.

Keywords: Radiation; Magnetohydrodynamic; Marangoni; Heat and mass generation; Stability analysis.

11.1 Introduction

A phenomenon that arise from the flow of the liquids from the area that having low surface tension to the higher surface tension area is known as Marangoni effect, a name given after an Italian physicist in nineteenth century, Carlo Marangoni, 1965. The Marangoni effect takes place when there is a gradient of surface tension

at the interface between two phases – in most situations, a liquid-gas interface. It is generally controlled by surface tension gradients on which the surface tension gradients that are responsible for the Marangoni convection can be due to gradients of temperature and/or concentration [1]. The very first work in Marangoni boundary layer was believed to be done by Napolitano [2] and the elementary mechanism of Marangoni convection can also be seen from Gelles [3] and Okano et al. [4]. The further development of theory of Marangoni flow was done by Napolitano [5] and focused on the study of the main features of the flow regimes. The applications of Marangoni are widely used in semiconductor processing and drying silicon wafers [6] and in many other aspects, see Kuroda [7]. Then Napolitano and Golia [8] provide a brief knowledge about behaviors, structures and properties of Marangoni boundary layers.

Numerous studied on Marangoni have been widely investigated with many different factors due to its useful contribution in industries. For such, Lichtenbelt et al. [9] studied the case of Marangoni convection and mass transfer from the liquid to the gas phase and performed experiment under micro-gravity conditions. Abergel and Dupaix [10] considered the existence and uniqueness of a stationary interface, in the neighbourhood of the capillary solution for Marangoni flow. Christopher and Wang [11] investigate the effect of Prandtl number on the flow and heat transfer characteristics of Marangoni convection over a flat surface. Arifin et al. [12] studied a case of non-isobaric Marangoni boundary layer flow for nanofluids in the present of Prandtl number, nanoparticle volume fraction and the exponent parameter. Following after, copious research related to Marangoni has been done by researchers such as Zhang and Zheng [13], Sastry [6], Aly and Ebaid [14], etc.

Radiation is a transmission of energy by electromagnetic waves. With the ability of no medium needed for the radiant interchange to occur between two locations makes the radiation as a significant mode of heat transfer. Due to this interest, a noticeable growth of research activity in various aspects related to radiation being investigated. Radiation has important applications in wide range of area such as in diagnosis and therapy, medical studies and research and agriculture and environment, Hurst and Turner [15]. Chamkha et al. [16] studied a problem of laminar free convection flow past a semi-infinite vertical plate in the presence of chemical species concentration and thermal radiation. Mat et al. [17] studied the effect of radiation on the Marangoni convection boundary layer flow together with suction/ injection effect. They stated that radiation descend the heat transfer rate at the surface. Yanhai et al. [18] examined the effect of radiation on the steady Marangoni convection flow driven by a power-law temperature gradient in non-Newtonian nanofluids containing different types of nanoparticles. Other Research related to radiation can be found in work done by Cess [19], Liu et al. [20], Saravanan and Sivaraj [21], etc.

Magnetohydrodynamic is the study of the feature of magnetic in the electrically conducting fluid such as liquid metals and plasmas. The beginning creation on the field of MHD about the basic properties and work related to it was proposed by Alfvén [22]. MHD can control the quality of the product demand in industrial applications due to its feature that it can control the rate of cooling. Thus, it has a main role basically in industrial and technologies applications. Furthermore, in general magnetic field can degrade the fluid velocity, heat transfer rate and surface concentration gradient. Maekawa and Tanasawa [23] studied theoretically about Marangoni convection in an electrically conducting liquid for the effect of magnetic field and Biot number on both the critical Marangoni number. Zhang and

Zheng [24] investigated the effects of uniform magnetic field, heat generation and first-order chemical reaction on the flow, heat and mass transfer of thermosolutal Marangoni convection. Mahdy and Ahmed [25] investigate the influence of magneto-hydrodynamic and Soret and Dufour effects on thermosolutal Marangoni convection and they found that as the number of magnetic parameter increase, the temperature and concentration species increase while the velocity features in decreases. More research about MHD can be seen from Katagiri [26], Andersson et al. [27], Mahapatra and Gupta [28], Aly and Ebaid (2015), etc.

Fluid heat generation or absorption effects are significant in those applications that involve heat removal from nuclear fuel debris, underground disposal of radioactive waste material and dissociating fluids in packed-bed reactors, Magyari and Chamkha [29]. It plays an important role in altering the heat transfer characteristics. The study of temperature-dependent heat generation or absorption on heat transfer in different geometries was done by Vajravelu and Hadjinicolaou [30]. Chamkha et al. [31] studied the mass and heat transfer characteristics of a boundary layer free convection of a non-Newtonian fluid on a vertical isothermal flat plate embedded in a fluid saturated porous medium in the presence of thermophoretic particle deposition and heat generation or absorption effects. They stated that in the result, as the heat generation or absorption coefficient increases the particle concentration level and the boundary layer thickness decreased. Zhang and Zheng [24] investigate the effect of heat generation on the temperature of the thermosolutal Marangoni convection and the result indicated that the temperature decrease with the increasing of heat generation. Chemical reaction in general depends on several factors. The first-order reaction is one of the simplest chemical reactions at which the rate of reaction is directly proportional to the species concentration. Anjali Devi and Kandasamy [32] investigated the influence of chemical reaction, heat and mass transfer on MHD laminar boundary layer flow with suction or injection effect. Reddy et al. [33] investigated the impact of magnetic field, radiation, rotation, chemical reaction and volume friction of the two type nanoparticles on the flow of the nanofluid past a flat permeable surface in porous medium. The chemical reaction as stated by them tends to decrease the concentration profile.

One of the applications of suction or injection is in the field of aerodynamic and space sciences. It can control the fluid flow on the surface of subsonic craft which can be benefit properties for the other important aspects such as fuel saving and operating costs, see Shojaefard et al. [34] and Braslow [35]. Research related to suction/injection has been done for example by Hamid et al. [36] on which they studied the effect of suction/injection on the case flow of thermosolutal Marangoni forced convection boundary layer and examine the existence of dual similarity solutions. They stated that the implication of suction/injection thus affect the flow, mass and heat transfer characteristics of the fluid where both of them shows an opposite effect to one another. While Aly and Ebaid [14] performed an exact analysis on the effect of suction/injection on the MHD Marangoni boundary layer in nanofluid with the presence of radiation. In general, suction tends to increase the skin friction and heat transfer coefficient while the injection shows an opposite result from suction [37]. Other research related to suction/injection can be seen from Black and Sarnecki [38], Pop and Watanabe [39], Attia [40], Ajibade et al. [41], etc.

The study of stability analysis is important particularly in fluid dynamics due to its significant way of finding which solution is stable whenever non-unique solutions exist in computation. This generally has attracted a new triggered in research

especially researchers who have locate multiple solutions in their computations. A solution that is not stable is when the eigenvalue of the solutions is negative as mentioned by Merkin [53]. Then Weidman et al. [38] rectified the stability by [53] and since then many researchers apply the Weidmen et al. [38] stability analysis to analyze the stability of their own research. One of the researches related to stability analysis can be seen from Mahapatra and Nandy [42] who inquire the conditions of existence and uniqueness of the similarity solution where dual solutions exist and linear stability analysis reveals that one solution is linearly stable while the other is linearly unstable. A stability analysis on the flow and heat transfer characteristics over a permeable shrinking sheet is done by Ishak [45] and the result obtained indicated that the first solution is physically realizable while the other one is not stable. Very recently, Hamid and Nazar [46] investigate the physical realizable solution of MHD thermosolutal Marangoni convection boundary layer flow and it is found that the first solution is stable and the second solution is not physically realizable. Generally it can be stated that, the first solution basically stable while the second one is not stable, thus not physically realizable. Other research related to the stability analysis can be seen from Mahapatra et al. [47], Noor [48], Rahman et al. [49], etc.

The present work considers the MHD thermosolutal Marangoni convective flow with the existence of heat generation or absorption effects. The analysis assumes that the surface is permeable and the work is done to analyse the effect of radiation on heat transfer characteristics of the fluid flow. By extending the previous work by Magyari and Chamkha [50], on which stated that dual solutions exist, a stability analysis is done in this paper to determine the stability of the solutions exists. The result obtained was then compared with the previous work by Mudhaf and Chamkha [51] and it is found to be in good agreement. Nonlinear ordinary differential equations are obtained by using similarity transformation from the general governing partial differential equations. The problems were then solved numerically by using Runge-Kutta-Fehlberg method (Maple 18) and shooting technique (Matlab R2014a).

11.2 Problem Formulation

The present work considers the steady laminar thermosolutal Marangoni flow of a viscous Newtonian fluid over a flat surface due to imposed temperature and concentration gradients. The surface tension varies linearly with temperature and concentration and the wall temperature and concentration variations are quadratic functions of the location is assumed in this analysis. The heat and mass generation or consumption and first order chemical are considered to exist within a uniform electrically conducting fluid in the direction normal to the surface through a permeable surface. By extending the previous work by Mudhaf and Chamkha [51], the effect of radiation under the influence of suction/injection cases on the heat transfer of the fluid is studied and a stability analysis is performed to analyse the stability of dual solutions exist stated on work done by Magyari and Chamkha [50]. Under these assumptions, the governing equations can be written in the following form based on the balance laws of mass, linear momentum, energy and concentration species,

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} = 0, \tag{11.1}$$

$$u\frac{\partial u}{\partial x}+v\frac{\partial u}{\partial y}=\nu\frac{\partial^2 u}{\partial y^2}-\frac{\Delta B_0^2}{\rho}u, \tag{11.2}$$

$$u\frac{\partial T}{\partial x}+v\frac{\partial T}{\partial y}=\alpha\frac{\partial^2 T}{\partial y^2}-\frac{1}{\rho C_p}\frac{\partial q_r}{\partial y}+\frac{Q_0}{\rho C_p}\left(T-T_\infty\right), \tag{11.3}$$

$$u\frac{\partial c}{\partial x}+v\frac{\partial c}{\partial y}=D\frac{\partial^2 c}{\partial y^2}-R\left(c-c_\infty\right), \tag{11.4}$$

with the boundary conditions,

$$\begin{aligned}&\mu\frac{\partial u}{\partial y}\bigg|_{y=0}=-\frac{\partial \sigma}{\partial x}\bigg|_{y=0}=\sigma_0\left(\gamma_T\frac{\partial T}{\partial x}\bigg|_{y=0}+\gamma_c\frac{\partial c}{\partial x}\bigg|_{y=0}\right),\\&v\left(x,0\right)=v_0,\ T\left(x,0\right)=T_\infty+T_0X^2,\ c\left(x,0\right)=c_\infty+c_0X^2,\ X=x/L,\\&u\left(x,\infty\right)=0,\ T\left(x,\infty\right)=0,\ c\left(x,\infty\right)=0.\end{aligned} \tag{11.5}$$

Here, u and v denoted as the the velocity components along the x and y axes. Where ν, B_0, ρ, T, α, C_p, q_r, Q_0, c, D and R are denoted as the kinematic viscosity, magnetic induction, density, thermal quantity, thermal diffusivity, specific heat at constant pressure, radiative heat flux, dimensional heat generation or absorption coefficients, concentration species, mass diffusivity and dimensional chemical reaction parameter, respectively. While, μ, σ, v_0 and L referred as dynamic viscosity, surface tension, dimensional suction or injection velocity and reference length.

The surface tension is assumed to depend on temperature and concentration linearly,

$$\sigma=\sigma_0\left[1-\gamma_T\left(T-T_\infty\right)-\gamma_c\left(c-c_\infty\right)\right], \tag{11.6}$$

where

$$\gamma_T=-\frac{1}{\sigma_0}\frac{\partial \sigma}{\partial T}\bigg|_c,\ \gamma_c=-\frac{1}{\sigma_0}\frac{\partial \sigma}{\partial c}\bigg|_T, \tag{11.7}$$

indicated as the temperature and concentration coefficients of the surface tension, respectively.

The stream function $\psi(x,y)$ by the usual definition is $u=\frac{\partial \psi}{\partial y}$ and $v=-\frac{\partial \psi}{\partial x}$ as well as the similarity transformations,

$$\begin{aligned}&\left(x,y\right)=\nu X f\left(\eta\right),\ \eta=y/L,\\&T\left(x,y\right)=T_\infty+T_0X^2\theta\left(\eta\right),\ c\left(x,y\right)=c_\infty+C_0X^2C\left(\eta\right).\end{aligned} \tag{11.8}$$

Using (11.8), the boundary value problem of Eqs. (11.1) to (11.7), reduces to the solution of the ordinary differential equations,

$$f'''+ff''-f'^2=0, \tag{11.9}$$

$$\frac{\theta''}{\mathrm{Pr}}+f\theta'+\left(\phi-2f'\right)\theta=0, \tag{11.10}$$

$$\frac{C''}{Sc}+fC'+\left(K+2f'\right)C=0, \tag{11.11}$$

along with the boundary conditions

$$\begin{aligned}&f\left(0\right)=f_0,\ f''(0)=-2\left(1+r\right),\theta\left(0\right)=1,\ C\left(0\right)=1,\\&f'\left(\infty\right)=0,\ \theta\left(\infty\right)=0,\ C\left(\infty\right)=0.\end{aligned} \tag{11.12}$$

The Prandtl and the Schmidt numbers denoted as $Pr = \frac{\nu}{\alpha}$ and $Sc = \frac{\nu}{D}$, respectively, where ϕ, K, f_0 and r are further dimensionless parameters defined as follows,

$$\phi = \frac{Q_0 L^2}{\rho v c_p},\ K = \frac{RL^2}{v},\ f_0 = f(0) = -\frac{v_0 L}{\nu},\ r = -\frac{C_0 \gamma_c}{T_0 \gamma_T}. \tag{11.13}$$

The reference length L has been chosen as,

$$L = -\frac{\mu\nu}{\sigma_0 T_0 \gamma_T}. \tag{11.14}$$

Having in view that with increasing temperature the surface tension σ in general decreases, its temperature gradient γ_T given by Eq. (11.7) is positive. Thus, the reference length chosen according to Eq. (11.14) is positive only if T_0 is negative. We also mention that the parameter r represents precisely the ratio of the solutal and thermal Marangoni numbers $Ma_c = \sigma_0 \gamma_c C_0 L/(\alpha\mu)$ and $Ma_T = \sigma_0 \gamma_T T_0 L/(\alpha\mu)$, respectively. Eqs. (11.9) to (11.12) show that the $f-$boundary value problem is decoupled from the temperature and concentration boundary value problems. Its solution $f = f(\eta)$ yields the dimensional velocity field in the form

$$u(x,y) = \frac{\nu}{L} X f'(\eta),\ v(x,y) = -\frac{\nu}{L} f(\eta), \tag{11.15}$$

The local mass flow in the boundary layer per unit span is given by:

$$\dot{m} = \int_0^\infty u\ dy = \rho\nu\left[f(\infty) - f_0\right] X \tag{11.16}$$

where $f(\infty)$ represents the similar entrainment velocity, $f(\infty) = -(L/\nu)\, v(x,\infty)$. In this way we obtain

$$\dot{m} = \rho x\left[v(x,0) - v(x,\infty)\right]. \tag{11.17}$$

The boundary value problem, Eqs. (11.9) to (11.12) has been investigated numerically for different values of the parameters involved by Mudhaf and Chamkha [51]. An approximate analytical solution has also been given in Mudhaf and Chamkha [51].

11.3 Stability Analysis

The stability analysis done in this paper is based on the stability analysis developed by Weidman et al. [38]. By referring to them, a variable τ has to be introduced. The unsteady form of Eqs (11.2) to (11.12) is considered as:

$$\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} = \nu\frac{\partial^2 u}{\partial y^2} - \frac{\Delta B_0^2}{\rho} u, \tag{11.18}$$

$$\frac{\partial T}{\partial t} + u\frac{\partial T}{\partial x} + v\frac{\partial T}{\partial y} = \alpha\frac{\partial^2 T}{\partial y^2} - \frac{1}{\rho C_p}\frac{\partial q_r}{\partial y} + \frac{Q_0}{\rho C_p}(T - T_\infty), \tag{11.19}$$

$$\frac{\partial c}{\partial t} + u\frac{\partial c}{\partial x} + v\frac{\partial c}{\partial y} = D\frac{\partial^2 c}{\partial y^2} - R(c - c_\infty), \tag{11.20}$$

with the new similarity transformations,

$$\begin{aligned} &u = \frac{v}{L^2} x\frac{\partial f(\eta,\tau)}{\partial \eta},\ v = -\frac{v}{L} f(\eta,\tau),\ \tau = \frac{v}{L^2} t,\ \eta = \frac{y}{L}, \\ &T(x,y) = T_\infty + T_0 X^2 \theta(\eta),\ c(x,y) = c_\infty + C_0 X^2 C(\eta). \end{aligned} \tag{11.21}$$

We substitute (11.21) into (11.22) to (11.24) and obtain the following equations:

$$\frac{\partial^3 f}{\partial \eta^3} + f\frac{\partial^2 f}{\partial \eta^2} - \left(\frac{\partial f}{\partial \eta}\right)^2 - M^2\frac{\partial f}{\partial \eta} - \frac{\partial^2 f}{\partial \eta \partial \tau} = 0, \tag{11.22}$$

$$\frac{1}{Pr}(1+Nr)\frac{\partial^2 \theta}{\partial \eta^2} + f\frac{\partial \theta}{\partial \eta} + \left(\phi - 2\frac{\partial f}{\partial \eta}\right)\theta - \frac{\partial \theta}{\partial \tau} = 0, \tag{11.23}$$

$$\frac{1}{Sc}\frac{\partial^2 C}{\partial \eta^2} + f\frac{\partial C}{\partial \eta} - \left(K - 2\frac{\partial f}{\partial \eta}\right)C - \frac{\partial C}{\partial \tau} = 0, \tag{11.24}$$

with the boundary conditions,

$$\begin{aligned} &f(0,\tau) = f_0,\ \frac{\partial^2 f}{\partial \eta^2}(0,\tau) = -2(1+r),\ \theta(0,\tau) = 1,\ C(0,\tau) = 1, \\ &\frac{\partial f}{\partial \eta}(\eta,\tau) = 0,\ \theta(\infty,\tau) = 0,\ C(\infty,\tau) = 0. \end{aligned} \tag{11.25}$$

To test the stability of the solution $f(\eta) = f_0(\eta)$, $(\eta) =_0 (\eta)$ and $C(\eta) = C_0(\eta)$ satisfying the boundary value problem (11.1) to (11.5), we write (see Weidman et al. [38]),

$$\begin{aligned} &f(\eta,\tau) = f_0(\eta) + e^{-\gamma\tau}F(\eta,\tau),\ \theta(\eta,\tau) = \theta_0(\eta) + e^{-\gamma\tau}G(\eta,\tau), \\ &C(\eta,\tau) = C_0(\eta) + e^{-\gamma\tau}H(\eta,\tau), \end{aligned} \tag{11.26}$$

where γ is an unknown eigenvalue parameter and $F(\eta,\tau)$, $G(\eta,\tau)$, and $H(\eta,\tau)$ are small relative to $f_0(\eta)$, ${}_0(\eta)$ and $C_0(\eta)$.

By substituting Eq. (11.26) into (11.22)-(11.24), we get the following:

$$\frac{\partial^3 F}{\partial \eta^3} + f_0\frac{\partial^2 F}{\partial \eta^2} + f_0''F - 2f_0'\frac{\partial F}{\partial \eta} - \frac{\partial^2 F}{\partial \eta \partial \tau} - M^2\frac{\partial F}{\partial \eta} + \gamma\frac{\partial F}{\partial \eta} = 0, \tag{11.27}$$

$$\frac{1}{Pr}(1+Nr)\frac{\partial^2 G}{\partial \eta^2} + f_0\frac{\partial G}{\partial \eta} + \theta_0'F + \phi G - 2f_0'G - 2\theta_0\frac{\partial F}{\partial \eta} + \gamma G = 0, \tag{11.28}$$

$$\frac{1}{Sc}\frac{\partial^2 H}{\partial \eta^2} + f_0\frac{\partial H}{\partial \eta} + C_0'F - KH + 2f_0'H + 2C_0\frac{\partial F}{\partial \eta} + \gamma H = 0, \tag{11.29}$$

with the boundary conditions,

$$\begin{aligned} &F(0,\tau) = 0,\ \frac{\partial^2 F(0,\tau)}{\partial \eta^2} = 0,\ G(0,\tau) = 0,\ H(0,\tau) = 0, \\ &\frac{\partial F(\eta,\tau)}{\partial \eta} \to 0,\ G(\eta,\tau) \to 0,\ H(\eta,\tau) \to 0 \text{ as } \eta \to \infty. \end{aligned} \tag{11.30}$$

We set $\tau = 0$, $F = F_0(\eta)$, $G = G_0(\eta)$ and $H = H_0(\eta)$. Thus we obtained the following equations:

$$F_0''' + f_0F_0'' + f_0''F_0 - 2f_0'F_0' - M^2F_0' + \gamma F_0' = 0, \tag{11.31}$$

$$\frac{1}{Pr}(1+Nr)G_0'' + f_0G_0' + \theta_0'F + \phi G - 2f_0'G - 2\theta_0F_0' + \gamma G = 0, \tag{11.32}$$

$$\frac{1}{Sc}H_0'' + f_0H_0' + C_0'F - KH + 2f_0'H + 2C_0F_0' + \gamma H = 0, \tag{11.33}$$

with the boundary conditions,

$$\begin{aligned} &F_0(0) = 0,\ F_0''(0) = 0,\ G_0(0) = 0,\ H_0(0) = 0, \\ &F_0'(\eta) \to 0,\ G_0(\eta) \to 0,\ H_0(\eta) \to 0 \text{ as } \eta \to \infty. \end{aligned} \tag{11.34}$$

Table 11.1: Values of $f'(0)$, $\theta'(0)$ and $-C'(0)$ for different value of Nr when $M = 0$, $Pr = 0.78$, $\phi = 0$, $Sc = 0.6$, $K = 0$ and $S = 0$.

Radiation Nr	[51] $g'(0)$	Present result $g'(0)$
0	1.442203	1.442067
2		0.684881
4		0.464511
6		0.357348
8		0.294281

The stability of the problem is determined by the smallest eigenvalue γ. The possible values of γ can be obtained by relaxing a boundary condition on $F_0'(\eta)$, $G_0(\eta)$ and $H_0(\eta)$, see Harris et al. [47]. In this problem, we relax the boundary condition $G_0(\infty) \to 0$ and solve the system using the bvp4c function with the new boundary condition $G_0'(0) = 1$.

11.4 Results and Discussion

In the presence of MHD and heat generation, the effect of radiation on the flow and heat transfer characteristics of Marangoni boundary layer past a flat surface through permeable surface has been studied in this paper along with the stability analysis. Runge-Kutta-Fehlberg (Maple 18) methods and bvp4c solver in Matlab (R2014a) software were used to solve the nonlinear ordinary differential equations (11.9) to (11.11) subjects to boundary conditions (11.12) numerically. The results of surface velocity $f'(\eta)$, heat flux $-\theta'(\eta)$ and concentration gradient at the surface $-C'(\eta)$ along with the value of temperature profiles $-\theta'(0)$ are obtained with various value of radiation, Nr and suction/injection, S. By extending the paper of Mudhaf and Chamkha [51] and referring to the paper of Magyari and Chamkha [50], we also run a stability analysis based on the dual result obtained by Magyari and Chamkha [50]. The stability analysis is computed using the bvp4c function in Matlab and performed to determine the physically realizable solution. Table 14.3 represents the result for the velocity, $f'(0)$ temperature, $-\theta'(0)$ and concentration, $-C'(0)$ profiles under the effect of radiation parameter with the fixed value of other parameters. The result obtained is compared with Mudhaf and Chamkha [51] and it is found to be in a good agreement. While, Table 11.2 shows the result obtained by stability analysis of the smallest eigen values γ at several values of thermo-solutal surface tension ratio, r with the fixed value of magnetic field, $M = 0$, Prandtl number, $Pr = 0.78$, dimensionless heat generation or absorption coefficient, $\phi = 0$, Schmidt number, $Sc = 0.6$, dimensionless chemical reaction parameter, $K = 0$ and suction/injection, $S = 3$. The outputs acquired indicate that the eigenvalues of the first solution are all positive while for the second solution are all negative. On which it resemble that, according to Merkin [53], a positive eigenvalue referred as stable while the negative one corresponded to not stable, and thus not physically realizable.

Fig. 17.1 shows the effect of radiation, Nr on the temperature profile, $\theta(\eta)$ of the fluid. It is worth to mention that the influence of radiation has no effect on the flow field and the concentration gradient of the fluid as can be seen from the Eqs. (11.9) and (11.11). From the figure obtained, one can see that the effect of radiation tends to decrease the dimensional temperature of the fluid. Radiation parameter

Table 11.2: Smallest eigenvalues γ at several values of r.

r	Upper branch	Lower branch
-3	1.40306	0.57784
-2.8	1.65496	0.39293
-2.6	1.76601	0.30235
-2.4	1.85907	0.20519
-2.2	1.90109	0.07216
-2.0	1.97854	-0.10890
-1.8	2.04916	-0.15798
$-1,6$	2.11452	-0.22760
-1.4	2.29291	-0.26182
-1.2	2.233395	-0.29329

is generally known as the measure of relative importance of the thermal radiation transfer to the conduction of heat. Due to this fact, as the radiation number increases then more heat being released into the system which helps to enhance the thermal boundary layer thickness and consequently increase the temperature profiles of the flow. Thus it can be concluded that temperature is an increasing function of radiation.

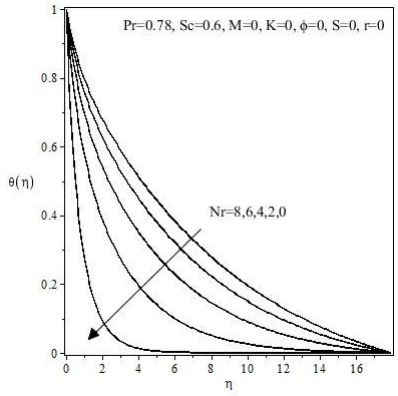

Figure 11.1: The effects of Nr on the $\theta(\eta)$ when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$, $S = 0$, $\phi = 0$ and $r = 0$.

Fig. 17.2 represents the variations of heat flux or temperature at the surface, $-\theta'(0)$ with radiation, Nr for different types of suction/injection, S parameter when Prandtl number, $Pr = 0.78$, Schmidt number, $Sc = 0.6$, magnetic field, $M = 0$, dimensionless chemical reaction parameter, $K = 0$ dimensionless heat generation or absorption coefficient, $\phi = 0$ and thermo-solutl surface tension ratio, $r = 0$. From the figure, it clearly shows that as the radiation parameter increase the temperature at the surface decreases. This is coinciding with the value shown in the Table 11.2 where as the number of radiation parameter increase, the value of heat flux decreases. Radiation reduces the energy transfer rate at the surface, thus it decreases the temperature of the fluid. Thereby decreases the heat transfer rate at the surface.

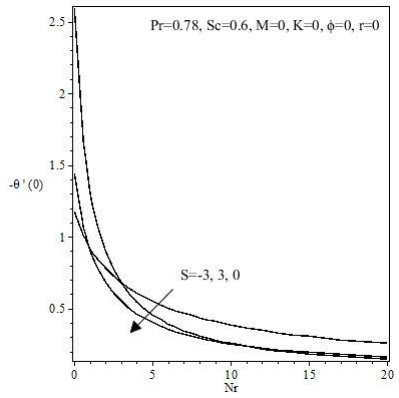

Figure 11.2: The variations of $-\theta'(0)$ with Nr for different types of S when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$, $\phi = 0$ and $r = 0$.

Figs. 17.3 to 17.5 shows the variations of interface velocity, $f'(0)$ heat flux, $-\theta'(0)$ and concentration gradients at the surface, $-C'(0)$ with suction/injection, S for different types of radiation, Nr. The influence of radiation has no impact on the interface velocity and surface concentration gradients under the effect of suction/injection parameter. As mention in work by Mudhaf and Chamkha [51], suction tends to decrease the interface velocity but increasing the surface temperature and concentration, while injection show an opposite effect. The result to point out here is that the temperature will get down under the suction and injection effect with the increasing of radiation influence compare to non-radiation uses. Thus radiation can be a helpful factor in reducing the heat within the effect of suction/injection.

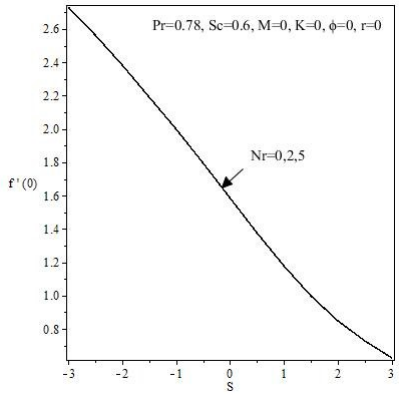

Figure 11.3: The variations of $f'(0)$ with S for different types of Nr when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$, $\phi = 0$ and $r = 0$.

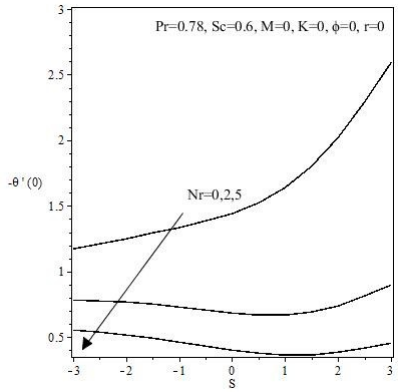

Figure 11.4: The variations of $-\theta'(0)$ with S for different types of Nr when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$, $\phi = 0$ and $r = 0$.

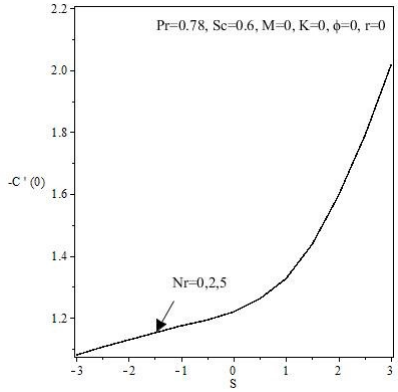

Figure 11.5: The variations of $-C'(0)$ with S for different types of Nr when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$, $\phi = 0$ and $r = 0$.

Fig. 17.6 portrayed the values of the surface velocity, $f'(0)$ when thermo-solutal surface tension ratio, r is varies with the effect of the suction. Two solutions were obtained for the same value of r for the range $-3 \leq r < -1$. Basically the first solution has higher value than the second solution. The figure obtained generally the same figure as Fig. 17.4 obtained by Mudhaf and Chamkha [51]. Hence, we can prove that our result are the same as Mudhaf and Chamkha [51] and can be concluding as in good agreement. Fig. 11.7 illustrated the velocity profiles, $f'()$ for different r on which to prove that the second solution exist.

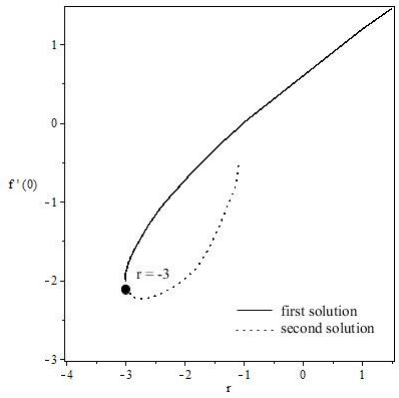

Figure 11.6: The variations of $f'(0)$ with r for $S = 3$ when $Pr = 0.78$, $Sc = 0.6$, $M = 0$, $K = 0$ and $\phi = 0$.

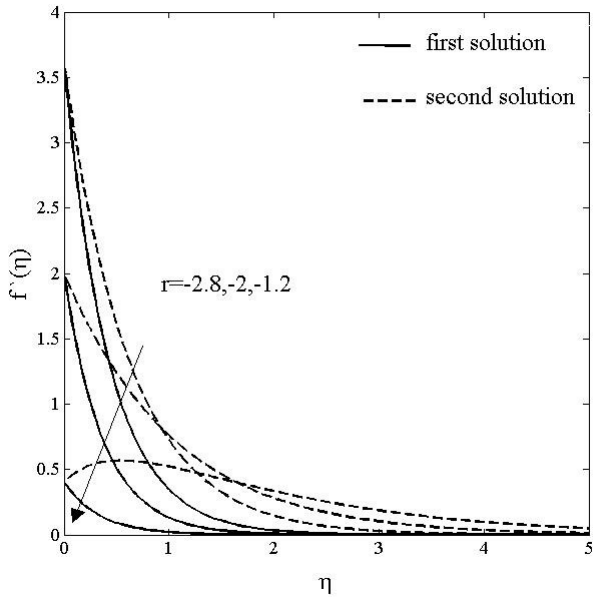

Figure 11.7: Velocity profiles $f'(\eta)$ for different r when $S = 3$.

11.5 Conclusion

The present paper considers the MHD thermosolutal Marangoni convection with the presence of heta and mass generation or consumption. The effect of radiation and suction/injection on the flow, mass and heat transfer characteristics of the viscous fluid is studied and discussed properly. The nonlinear ordinary differential equations obtained are solved numerically by using the Runge-Kutta-Fehlberg method and bvp4c solver in Matlab software. The radiation parameter tends to decreases the temperature at the surface. Stability analysis is also done in this paper based on the result achieved by Magyari and Chamkha [50] to determine which solution is linearly stable and physically realizable. The outputs acquired indicate that the first solution is stable the second solution are unstable and not physically realizable.

Bibliography

[1] Golia C, Viviani A (1986) Marangoni-Bouyant Boundary Layers. *L' Aerotecnica Missili e Spazio* **65(6)**, 29–35.

[2] Napolitano LG (1979) Marangoni Boundary Layers, *In Proc. 3rd European Symp. On Material Science in Space*, Grenoble, ESA SP-142.

[3] Gelles SH (1978) Microgravity Studies in the Liquid-Phase Immiscible System: Aluminium–Indium. *AIAA J.* **16(5)**, 431-–438.

[4] Okano Y, Itoh M, Hirata A (1989) Marangoni Convections in a Two-Dimensional Rectangular Open Boat. *J. Chem. Eng. Jpn* **22**, 275-–281.

[5] Napolitano LG (1986) Recent Development of Marangoni Flows Theory and Experimental Results. *Adv. Space Ret.* **6(5)**, 19–34.

[6] Sastry DRVSR (2015) MHD Thermosolutal Marangoni Convection Boundary Layer Nanofluid Flow Past a Flat Plate with Radiation and Chemical Reaction. *Indian Journal of Science and Technology* **8(13)**.

[7] Kuroda T (2000) The Marangoni Effect and Its Artistic Application. *Forma* **15(3)**, 203–204.

[8] Napolitano LG, Golia C (1981) Coupled Marangoni Boundary Layers. *Acta Astronautica* **8(5–6)**, 417–434.

[9] Lichtenbelt JH, Dijkstra HA, and Drinkenburg AAH (1986) Marangoni Convection and Mass Transfer from the Liquid to the Gasphase. *Adv. Space Res.* **6(5)**, 61–64.

[10] Abergel F, Dupaix C (1996) Existence of Smooth, Stationary Interfaces for Marangoni-Type Flow. *Nonlinear Analysis, Theory, Methods & Applications* **27(11)**, 1329–1350.

[11] Christopher DM, Wang B (2001) Prandlt Number Effects for Marangoni Convection over a Flat Surface. *Int. J. Therm. Sci.* **40**, 564–570.

[12] Arifin NM, Nazar R, Pop I (2011) Non-Isobaric Marangoni Boundary Layer Flow for Cu, Al2O3 and Tio2 Nanoparticles in a Water Based Fluid. *Meccanica* **46**, 833–843.

[13] Zhang Y, Zheng L, (2014) Similarity Solutions of Marangoni Convection Boundary Layer Flow With Gravity and External Pressure. *Chinese Journal of Chemical Engineering* **22(4)**, 365–369.

[14] Aly EH, Ebaid A (2016) Exact Analysis for the Effect of Heat Transfer on MHD and Radiation Marangoni Boundary Layer Nanofluid Flow Past a surface Embedded in a Porous Medium. *Journal of Molecular Liquids* **215**, 625–639.

[15] Hurst GS, Turner JE (1970) Elementary Radiation Physics, John Wiley & Sons, Inc.

[16] Chamkha AJ, Takhar HS, Soundalgekar VM (2001) Radiation Effects on Free Convection Flow Past a Semi-Infinite Vertical Plate with Mass Transfer. *Chemical Engineering Journal* **84**, 335–342.

[17] Mat NA, Arifin NM, Nazar R, Ismail F, Pop I (2013) Radiation Effects On Marangoni Convection Boundary Layer over a Permeable Surface. *Meccanica* **48**, 83-–89.

[18] Yanhai L, Zheng L, Zhang X (2014) Radiation Effects on Marangoni Convection Flow and Heat Transfer in Pseudo-Plastic non-Newtonian Nanofluids with Variable Thermal Conductivity. *International Journal of Heat and Mass Transfer* **77**, 708-–716.

[19] Cess RD (1961) The Effect of Radiation upon Forced-Convection Heat Transfer. *Appl. Sci. Res.* **10**, 430–438.

[20] Liu L, Tan H, He Z (2001) Inverse Radiation Problem of Source Term in Three-Dimensional Complicated Geometric Semitransparent Media. *Int. J. Therm. Sci* **40**, 528—538.

[21] Saravanan S, Sivaraj C (2014) Surface Radiation Effect on Convection in a Closed Enclosure Driven By a Discrete Heater. *International Communications in Heat and Mass Transfer*, **53** 34-–38.

[22] Alfvén H (1942) Existence of Electromagnetic-Hydrodynamic Waves. *Nature* **150**, 405–406.

[23] Maekawa T, Tanasawa I (1986) Onset of Marangoni Convection in an Infinite Layer of an Electrically Conducting Liquid Under Magnetic Field. *Adv. Space Res 6(5)*, 41–44.

[24] Zhang Y,Zheng L (2012) Analysis of MHD Thermosolutal Marangoni Convection with the Heat Generation and a First-Order Chemical Reaction. *Chemical Engineering Science* **69**, 449–455.

[25] Mahdy A, Ahmed SE (2015) Thermosolutal Marangoni Boundary Layer Magnetohydrodynamic Flow with the Soret and Dufour Effects Past a Vertical Flat Plate. *Engineering Science and Technology, an International Journal* **18**, 24–31

[26] Katagiri M (1969) Magnetohydrodynamic Flow with Suction or Injection at the Forward Stagnation Point. *Journal of the Physical Society of Japan* **27(6)**.

[27] Andersson HI, Bech KH, Dandapat BS (1992) Magnetohydrodynamic Flow of a Power-Law Fluid over a Stretching Sheet. *Int. J. Nonlinear Mechanics* **27(6)**, 929–935.

[28] Mahapatra TR, Gupta AS (2001) Magnetohydrodynamic Stagnation-Point Flow Towards a Stretching Sheet. *Acta Mechanica* **152**, 191-–196.

[29] Magyari E, Chamkha AJ (2010) Combined Effect of Heat Generation or Absorption and First-Order Chemical Reaction on Micropolar Fluid Flows over a Uniformly Stretched Permeable Surface: The Full Analytical Solution. *International Journal of Thermal Sciences* **49**, 1821–1828.

[30] Vajravelu K, Hadjinicolaou A (1993) Heat Transfer in a Viscous Fluid over a Stretching Sheet with Viscous Dissipation and Internal Heat Generation. *International Communications in Heat and Mass Transfer* **20**, 417–430.

[31] Chamkha AJ, Mudhaf AF, Pop I (2006) Effect of Heat Generation or Absorption on Thermophoretic Free Convection Boundary Layer from a Vertical Flat Plate Embedded in a Porous Medium, *International Communications in Heat and Mass Transfer* **33**, 1096–1102.

[32] Anjali Devi SP, Kandasamy R (2002) Effects of Chemical Reaction Heat and Mass Transfer on Non-Linear MHD Laminar Boundary-Layerflow over a Wedge with Suction or Injection. *International Communications in Heat and Mass Transfer* **29**, 707–716.

[33] Reddy JVR, Sugunamma V, Sandeep N, Sulochana C (2015) Influence of Chemical Reaction, Radiation and Rotation on MHD Nanofluid Flow past a Permebale Flat Plate in Porous Medium. *Journal of Nigerian Mathematical Society* 66165.

[34] Shojaefard MH, Noorpoor AR, Avanesians A, Ghaffapour M (2005) Numerical Investigation of Flow Control by Suction and Injection on a Subsonic Airfoil. *The American Journal of Applied Sciences* **20**, 1474–1480.

[35] Braslow A (1999) A History of Suction Type Laminar Flow Control with Emphasis on Flight Research, Washington, Wash, USA: American Institute of Aeronautics and Astronautics.

[36] Hamid RA, Arifin NM, Nazar R, Ali FM, Pop I (2011) Dual Solutions on Thermosolutal Marangoni Forced Convection Boundary Layer with Suction and Injection. *Mathematical Problems in Engineering.*

[37] Al-Sanea SA (2004) Mixed Convection Heat Transfer along a Continuously Moving Heated Vertical Plate with Suction or Injection. *Int. J. Heat Mass Transfer* **47**, 1445–1465.

[38] Black TJ, Sarnecki AJ (1965) The Turbulent Boundary Layer with Suction or Injection. *Aeronautical Research Council, Reports and Memoranda* 3387.

[39] Pop H, Watanabe W (1992) The Effects of Suction or Injection in Boundary Layer Flow and Heat Transfer on a Continuous Moving Surface. *Technische Mechanik* 13.

[40] Attia HA (2005) The Effect of Suction and Injection on the Unsteady Flow Between two Parallel Plates with Variable Properties. *Tamkang Journal of Science and Engineering* **8(1)**, 17–22.

[41] Ajibade AO, Jha BK, Omame A (2011) Entropy Generation Under the Effect of Suction/Injection. *Applied Mathematical Modelling* **35**, 4630–4646.

[42] Merkin JH (1985) Free Convection Above a Uniformly Heated Horizontal Circular Disk. *J. Eng. Math.* **20**, 171–179.

[43] Weidman PD, Kubitschek DG, Davis AMJ (2006) The Effect of Transpiration on Self-Similar Boundary Layer Flow over Moving Surfaces. *Int. J. Eng. Sci.* **44**, 730–737.

[44] Mahapatra TR, Nandy SK (2011) Stability Analysis of Dual Solutions in Stagnation-point Flow and Heat Transfer over a Power-law Shrinking Surface. *International Journal of Nonlinear Science* **12(1)**, 86–94.

[45] Ishak A (2014) Flow and Heat Transfer over a Shrinking Sheet: A Stability Analysis. *International Journal of Mechanical, Aerospace, Industrial and Mechatronics Engineering* **8(5)**.

[46] Hamid RA, Nazar R (2016) Stability Analysis of MHD Thermosolutal Marangoni Convection Boundary Layer Flow. *AIP Conference Proceedings* **1750**.

[47] Mahapatra TR, Nandy SK, Gupta AS (2014) Dual Solution of MHD Stagnation-Point Flow towards a Stretching Surface. *Engineering* **2(4)**, 299–305.

[48] Noor A, Nazar R, Jafar K (2014) Stability Analysis of Stagnation-Point Flow past a Shrinking Sheet in a Nanofluid. *Journal of Quality Measurement and Analysis* **10(2)**, 51–63.

[49] Rahman MM, Roşca AV, Pop I (2014), Boundary Layer Flow of a Nanofluid Past a Permeable Exponentially Shrinking/Stretching Surface with Second Order Slip Using Buongiorno's Model. *Int. J. Heat Mass Transf.* **77**, 1133–1143.

[50] Magyari E, Chamkha AJ (2007) Exact Analytical Solutions for Thermosolutal Marangoni Convection in the Presence of Heat and Mass Generation or Consumption. *Heat and Mass Transfer* **43**, 965–974.

[51] Mudhaf A, Chamkha AJ (2005) Similarity Solutions for MHD Thermosolutal Marangoni Convection over a Flat Surface in the Presence of Heat Generation or Absorption Effects. *Heat and Mass Transfer* **42**, 112–121.

[52] Harris SD, Ingham DB, Pop I (2009) Mixed Convection Boundary-Layer Flow Near the Stagnation Point on a Vertical Surface in a Porous Medium: Brinkman Model With Slip. *Transport Porous Media* **77**, 267–285.

[53] Merkin JH (1985) Free Convection Above a Uniformly Heated Horizontal Circular Disk. *J. Eng. Math.* **20**, 171–179.

[54] Postelnicu A, Pop I (2011) Falkner-Skan Boundary Layer Flow of a Power-Law Fluid past a Stretching Wedge. *Appl. Math. Comput.* **217** 4359–4368.

[55] Roşca AV, Pop I (2013) Flow and Heat Transfer over a Vertical Permeable Stretching/ Shrinking Sheet with a Second Order Slip. *Int. J. Heat Mass Transfer* **60** 355–364.

[56] Ismail NS, Arifin NM, Bachok N, Mahiddin N (2016) Flow and Heat Transfer on a Moving Flat Plate in a Parallel Stream with Constant Surface Heat Flux: A Stability Analysis, *Indian Journal of Science and Technology* **9(31)**.

Chapter 12

Approximate Integrals Based on Linear Legendre-Multi Wavelets

Mohammad Hasan Abdul Sathar[1,*], Ahmad Fadly Nurullah Rasedee[2], Nor Fadzillah Mohd Mokhtar[1]

[1] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, 78100 Nilai, Negeri Sembilan, Malaysia.

*Corresponding author: mohdhasan@upm.edu.my

Abstract

The solution for single, double and triple integrals with variable limits based on linear Legendre multi-wavelets are proposed. An algorithm with the properties of linear Legendre multi-wavelets are constructed to find the numerical approximation for the integrals. The generalized algorithms for solving the integrals are simple and easy applicable. Some numerical examples for single, double and triple integrals are given to show the efficiency of the method. Approximation of the integrals by using linear Legendre multi-wavelets are compared with the existing methods in order to validate the error estimation.

Keywords: numerical integration , linear Legendre multi-wavelets, Holder class.

12.1 Introduction

Numerical integration has several applications in science and engineering. There are many engineering problems require the evaluation of the integral such as skin friction coefficient for the governing boundary layer equations in fluid dynamic. To determined the probability of electron in a region of space by solving the Schrodinger equation in quantum mechanics and several other problems. A lot of research have been done to solve numerical integration problems in terms of quadrature rule such as Newton-Cotes formulas and Gauss quadrature [1–7]. Regardless of the simplicity of quadrature rule, there exists a few disadvantages. For example, the Newton-Cotes formulas cause erratic behavior with high degree polynomial interpolation when the equally spaced nodes are large. The Gaussian quadrature rule is derived by method of undetermined coefficients but the resulting equations for the nodes and weights are nonlinear. This procedure is complicated to find the nodes and

weights. Other than that, there is limitation with Gaussian quadrature rule method where the limits of integration need to convert into -1 to 1 ([7]). To overcome the disadvantages, a new method based on wavelets approximation is propose to find the numerical solutions of integrals. There are several types of wavelets have been used in numerical approximations, for examples, Daubechies' [8], Chebyshev wavelets [9] and Haar wavelets [10–13].

According to [11], Haar wavelets are used to solve for single, double and triple integrals with variable limits. Algorithm based on Haar wavelets have been obtained to approximate the integrals for single, double and triple integrals. Linear Legendre multi wavelets display similar properties to the Haar wavelets. Due to this similarities, the linear Legendre multi-wavelets should also be able to solve the multi-dimensional integral easily [14]. There are numerous research have been done to solve problems such as integral equations by using linear Legendre multi-wavelets [15,16].

In this work, we deduce generalized solution based on linear Legendre multi-wavelets. The organization of this paper is as follows. We introduce about linear Legendre multi-wavelets in section 2, and in section 3 numerical system by linear Legendre multi-wavelets are shown for single, double and triple integrals with variable limits. Error analysis are describe in section 4 to show the convergence of the method and numerical results are reported in section 5. Finally further discussion and conclusion are drawn in section 6 and 7.

12.2 Linear Legendre multi-wavelets (LLMW)

In this paper, we used LLMW to handle with the problems of single, double and triple integrals with variable limits. Generally, wavelets have been used in various fields of engineering and science. It consists of two functions which are scaling function and mother wavelet. To construct the linear Legendre mother wavelets, we first introduce the scaling functions. There are two scaling functions for linear Legendre multi-wavelets which are as follows:

$$\phi_0(x) = 1, \quad \phi_1(x) = \sqrt{3}(2x-1), \quad a \le x < b.$$

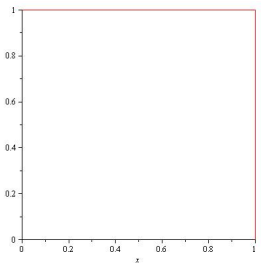

Figure 12.1: LLMW scaling $\phi_0(x)$

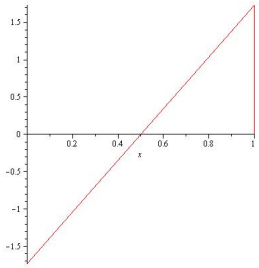

Figure 12.2: LLMW scaling $\phi_1(x)$

Figure 1-2 describe the scaling functions. Now let $\psi^0(x)$ and $\psi^1(x)$ as the corresponding mother wavelets, then by multiresolution of analysis (MRA) we have

$$\psi^0(x) = a_0\phi_0(2x) + a_1\phi_1(2x) + a_2\phi_0(2x-1) + a_3\phi_1(2x-1),$$
$$\psi^1(x) = b_0\phi_0(2x) + b_1\phi_1(2x) + b_2\phi_0(2x-1) + b_3\phi_1(2x-1)$$

and there are suitable conditions that applied on $\psi^0(x)$ and $\psi^1(x)$. As a result, the formulas for linear Legendre mother wavelets are obtained as

$$\psi^0(x) = \begin{cases} -\sqrt{3}(4x-1), & \left[a, \dfrac{a+b}{2}\right) \\ \sqrt{3}(4x-3), & \left[\dfrac{a+b}{2}, b\right) \end{cases}, \qquad \psi^1(x) = \begin{cases} 6x-1, & \left[a, \dfrac{a+b}{2}\right) \\ 6x-5, & \left[\dfrac{a+b}{2}, b\right) \end{cases},$$

and the diagram are given in Figure 3-4

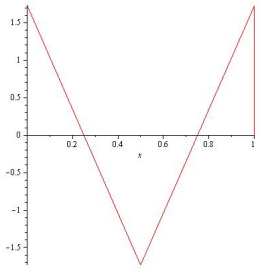

Figure 12.3: LLMW wavelet $\psi_{00}^0(x)$

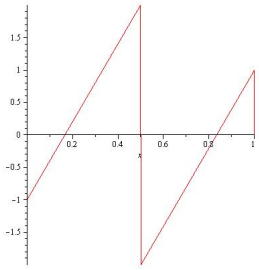

Figure 12.4: LLMW wavelet $\psi_{00}^1(x)$

By translating and dilating the mother wavelets, the linear Legendre multi-wavelets is constructed as

$$\psi_{kn}^j(x) = \begin{cases} 2^{\frac{k}{2}}\psi^j\left(2^k\dfrac{x-a}{b-a} - n\right), & a + n\dfrac{(b-a)}{2^k} \leq x < a + (n+1)\dfrac{(b-a)}{2^k}, \\ 0, & otherwise, \end{cases}$$

here $k, \in \mathbb{Z},\ n = 0, 1, ..., 2^k - 1$, and $j = 0, 1$ are defined on the interval $[a, b)$. The next four functions are drawn in Figure 5-8 to show how luckily the wavelets function behave after translation and dilation from the mother wavelets.

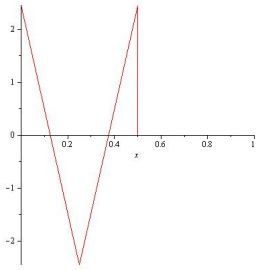

Figure 12.5: LLMW wavelet $\psi_{10}^0(x)$

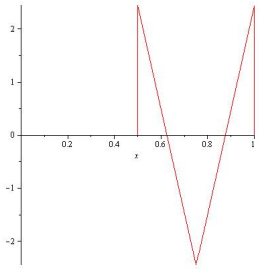

Figure 12.6: LLMW wavelet $\psi_{11}^0(x)$

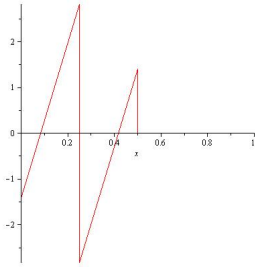

Figure 12.7: LLMW wavelet $\psi_{10}^1(x)$

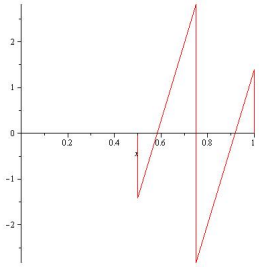

Figure 12.8: LLMW wavelet $\psi_{11}^1(x)$

Any function $f(x)$ in the interval $[a, b)$ can be written as

$$f(x) \approx c_0\phi_0(x) + c_1\phi_1(x) + \sum_{k=0}^{M}\sum_{j=0}^{1}\sum_{n=0}^{2^k-1} c_{kn}^{j}\psi_{kn}^{j}(x) = C^T\Psi(x), \tag{12.1}$$

where C and $\Psi(x)$ are

$$C = [c_0, c_1, c_{00}^0, c_{00}^1, ..., c_{M0}^0, c_{M1}^0, ..., c_{M(2^M-1)}^0, c_{M0}^1, c_{M1}^1 ..., c_{M(2^M-1)}^1]^T,$$

and

$$\Psi = [\phi_0, \phi_1, \psi_{00}^0, \psi_{00}^1, ..., \psi_{M0}^0, \psi_{M1}^0, ..., \psi_{M(2^M-1)}^0, \psi_{M0}^1, \psi_{M1}^1 ..., \psi_{M(2^M-1)}^1]^T.$$

12.3 Approximation of integrals based on LLMW

In this section, the LLMW functions are consider for solving the double and triple integrals with variable limits according to [14].

12.3.1 Numerical formula for single integral by LLMW

In [14], numerical integration formula by using LLMW were derived for single, double and triple integrals with definite limits. In this work, we apply LLMW for double and triple integrals with variable limits using the similar formula derived for single integral with definite limits. The following equation is the numerical formula derived in [14] for single integral with definite limits

$$\int_a^b f(x)\,dx \approx \frac{(b-a)}{K}\sum_{i=0}^{K-1} f\left(a + \frac{(b-a)(i+0.5)}{K}\right). \tag{12.2}$$

where $K = 2^{k_1+2}$ and k_1 is the level of resolution of the LLMW.

12.3.2 Numerical formula for double integral with variable limits

Consider the double integral with variable limits as follows:

$$\int_c^d \int_{a(y)}^{b(y)} F(x, y)\ dxdy.$$

We apply Eq. (14.2) to the integral

$$\int_{a(y)}^{b(y)} F(x, y)\,dx.$$

while variable y is constant. Then, we obtain the following approximations.

$$\int_{a(y)}^{b(y)} F(x, y)\,dx \tag{12.3}$$

$$= \frac{(b(y)-a(y))}{K}\sum_{i=0}^{K-1} F\left(a(y)+\frac{(b(y)-a(y))(i+0.5)}{K}, y\right) \tag{12.4}$$

$$\approx G(y). \tag{12.5}$$

Repeat the same process as above by substituting Eq. (14.2) into Eq () to get the numerical formula for double integral with variable limits

$$\int_c^d \int_{a(y)}^{b(y)} F(x,y)\,dx \approx \int_c^d G(y)\,dy \tag{12.6}$$

$$\approx \frac{(d-c)}{L}\sum_{j=0}^{L-1} F\left(c+\frac{(d-c))(j+0.5)}{L}\right). \tag{12.7}$$

where $L = 2^{k_2+2}$ and k_2 is the level of resolution of the LLMW.

12.3.3 Numerical formula for triple integral with variable limits

By using the same way as previous numerical systems, we obtained the numerical integration formula for triple integrals with variable limits as below

$$\int_e^f \int_{c(z)}^{d(z)} \int_{a(y,z)}^{b(y,z)} F(x,y,z)\ \ dxdydz \approx \frac{(f-e)}{P}\sum_{l=0}^{P-1} H\left(f+\frac{(f-e))(l+0.5)}{P}\right). \tag{12.8}$$

where $H(z)$ and $G(y,z)$ are

$$H(z) = \frac{(d(z)-c(z))}{L}\sum_{j=0}^{L-1} G\left(c(z)+\frac{(d(z)-c(z)))(j+0.5)}{L}, z\right).$$

$$G(y,z) = \frac{(b(y,z)-a(y,z))}{K}\sum_{i=0}^{K-1} F\left(a(y,z)+\frac{(b(y,z)-a(y,z))(i+0.5)}{K}, y, z\right).$$

In the Eq. (14.7), $P = 2^{k_3+2}$ where k_3 is the level of resolution of the LLMW.

12.4 Error Analysis

We continued with the definition of the Holder classes of order $H^s[0,1]$, $0 < s < 1$. The set of all continuous functions on $[0,1]$, which satisfies the inequality :

$$|f(x)-f(y)| \le L\,|x-y|^s\,,\ L > 0, \forall x, y \in [0,1].$$

Holder classes are medium spaces between $C[0,1]$ and $C^1[0,1]$ such that:

$$C^1[0,1] \subset H^s[0,1] \subset C[0,1].$$

Consider $f(x) \in H^s[0,1]\,,\ 0 < s < 1$, then

$$\|f - f_M\|_{L_2[0,1]} \le \frac{L^2}{4^{Ms}(4^s-1)}\left(\frac{3}{16}+\frac{4^s}{9}\left[\frac{8\left(\frac{2}{3}\right)^s - 3 + 3s}{(s+2)(s+1)}\right]^2\right).$$

where

$$f_M(x) = c_0\phi_0(x) + c_1\phi_1(x) + \sum_{k=0}^{M-1}\sum_{j=0}^{1}\sum_{n=0}^{2^k-1} c_{kn}^j \psi_{kn}^j(x), \;\; M \in \mathbb{Z}^+,$$

refer to [17]. The error bound are inversely proportion to the level of resolution M of the LLMW and will establish better approximation if increase the value of M.

12.5 Numerical Examples

In this section, we applied LLMW for solving numerical integration problems for double and triple integrals. The results will show the efficiency of LLMW by comparing it with reported in [11]. In [11] Haar wavelets have been applied to approximate double and triple integrals with variable limits of integration. We solved all of the examples in [11] using LLMW numerically and compare the numerical results with Haar wavelets at the same level dilation (J_i is the dilation for Haar and value of k_i is the dilation for LLMW, $i = 1, 2, 3$) to validate the error estimation.

12.5.1 Test Problems

Table 12.1: Please write your table caption here

Example	Problem	Exact Solution
1.	$\int_0^1 \int_0^y e^{\lvert x+y-1\rvert}\, dxdy$	$-2+e$
2.	$\int_0^{\frac{\pi}{4}} \int_0^{\sin y} \frac{1}{\sqrt{1-x^2}}\, dxdy$	$\frac{\pi^2}{32}$
3.	$\int\int_R (x+y)^{-\frac{1}{2}}\, dxdy$	$\frac{2}{3}(2-7\sqrt{3}-15\sqrt{5}+20\sqrt{6})$
	$= \int_1^2 \int_{(5-3y)}^{\frac{1}{2}(y+3)} (x+y)^{-\frac{1}{2}} dxdy$	
	$+ \int_2^3 \int_{(y-3)}^{\frac{1}{2}(y+3)} (x+y)^{-\frac{1}{2}} dxdy$	
	$+ \int_3^4 \int_{(y-3)}^{(9-2y)} (x+y)^{-\frac{1}{2}}\, dxdy$	
4.	$\int_0^{\pi} \int_0^{z} \int_0^{zy} \frac{1}{y}\sin(\frac{x}{y})\, dxdydz$	$\frac{1}{2}(4+\pi^2)$

12.5.2 Numerical Results

Table 12.2: Absolute errors of Example 1

LLMW	Absolute Errors	Haar	Absolute Errors
$k_1, k_2 = 3$	1.1857E-04	$J_1, J_2 = 3$	4.7400E-04
$k_1, k_2 = 4$	2.7875E-05	$J_1, J_2 = 4$	9.7811E-05
$k_1, k_2 = 5$	6.7701E-06	$J_1, J_2 = 5$	2.7875E-05
$k_1, k_2 = 6$	1.7065E-06	$J_1, J_2 = 6$	6.7700E-06

Table 12.3: Absolute errors of Example 2

LLMW	Absolute Errors	Haar	Absolute Errors
$k_1, k_2 = 3$	6.2347E-06	$J_1, J_2 = 3$	2.4839E-05
$k_1, k_2 = 4$	1.5604E-06	$J_1, J_2 = 4$	6.2348E-06
$k_1, k_2 = 5$	3.9030E-07	$J_1, J_2 = 5$	1.5601E-06
$k_1, k_2 = 6$	9.7300E-08	$J_1, J_2 = 6$	3.9030E-07

Table 12.4: Absolute errors of Example 3

LLMW	Absolute Errors	Haar	Absolute Errors
$k_1, k_2 = 3$	1.8930E-04	$J_1, J_2 = 3$	7.5503E-04
$k_1, k_2 = 4$	4.7363E-05	$J_1, J_2 = 4$	1.8930E-04
$k_1, k_2 = 5$	1.1852E-05	$J_1, J_2 = 5$	4.7365E-05
$k_1, k_2 = 6$	3.0528E-06	$J_1, J_2 = 6$	1.1855E-05

Table 12.5: Absolute errors of Example 4

LLMW	Absolute Errors	Haar	Absolute Errors
$k_1, k_2, k_3 = 3$	9.0291E-04	$J_1, J_2, J_3 = 3$	3.5959E-03
$k_1, k_2, k_3 = 4$	2.2597E-04	$J_1, J_2, J_3 = 4$	9.0291E-04
$k_1, k_2, k_3 = 5$	5.6516E-05	$J_1, J_2, J_3 = 5$	2.2598E-04
$k_1, k_2, k_3 = 6$	1.4127E-05	$J_1, J_2, J_3 = 6$	5.6507E-05

12.6 Discussion

All the test problems in this work are from [11]. [11] approximate the double and triple integrals by using Haar wavelets $h_i(x)$ where $i = 1, 2...., 2M$. They denote $M = 2^J$ and $J = 0, 1, 2, ...$ is the is the maximum level of resolution of Haar wavelets see [11] equation 1. Regarding table 1 and 3 for absolute errors in [11] suggest letting $M = 3, 5$ or 6, where else this research favours taking the value of M as an order of 2. Therefore Haar wavelets functions of order 2 ($M = 8, 16, ...,$) are consider to approximate the double and triple integrals. Concerning table 4, the problem are related to three dimensional case and the absolute errors are equivalent to the previous work. Moreover the absolute error between this two methods for Haar wavelets and LLMW functions are compared using the same order of dilation in all the test problems.

12.7 Conclusion

In this work, numerical integration based on LLMW has been applied to approximate the numerical examples for double and triple integrals with variable limits of integration. Generalized solution for LLMW are obtained to approximate the integrals. By analyzing the numerical results in terms of absolute errors between LLMW and Haar wavelets from [11], LLMW performs a better results in approximating the examples as shown in the tables 1-4. From the tables, it is clearly observed that the error estimation by linear Legendre multi-wavelets gives less error for the approximation. Therefore, it has been proved that the present method is more efficient and accurate than the Haar wavelets method.

Acknowledgements

This paper has been supported by University Putra Malaysia (UPM) under its short term grant Putra Muda (GP-IPM/9589600) scheme .

Bibliography

[1] Rokhlin V 1990 *Computers & Mathematics with Applications* **20** 51–62

[2] Ma J, Rokhlin V and Wandzura S 1996 *SIAM Journal on Numerical Analysis* **33** 971–996

[3] Alpert B K 1999 *SIAM Journal on Scientific Computing* **20** 1551–1584

[4] Place J and Stach J 1999 *Simulation* **73** 232–237

[5] Sermutlu E 2005 *Applied Mathematics and Computation* **171** 1048–1057

[6] Islam M S and Hossain M A 2009 *Applied Mathematics and Computation* **210** 515–524

[7] Rathod H, Nagaraja K and Venkatesudu B 2007 *Applied mathematics and computation* **188** 865–876

[8] Daubechies I *et al.* 1992 *Ten lectures on wavelets* vol 61 (SIAM)

[9] Babolian E and Fattahzadeh F 2007 *Applied Mathematics and Computation* **188** 417–426

[10] Siraj-ul-Islam, Imran Aziz and Fazal Haq 2010 *Computers & Mathematics with Applications* **59** 2026–2036

[11] Siraj-ul-Islam Aziz I, Khan W *et al.* 2011 *Computers & Mathematics with Applications* **61** 2770–2781

[12] Ahmedov A A and bin Abd Sathar M H 2013 Numerical integration of the integrals based on haar wavelets *Journal of Physics: Conference Series* vol 435 (IOP Publishing) p 012042

[13] Ahmedov A A, Sathar M H A, Rasedee A F N and Mokhtar N F B 2017 Approximating of functions from holder classes hα [0, 1] by haar wavelets *Journal of Physics: Conference Series* vol 890 (IOP Publishing) p 012073

[14] Mohammad Hasan Abd Sathar, Ahmad Fadly Nurullah Rasedee, Anvarjon A Ahmedov and Muhammad Asyraf Asbullah 2018 Numerical integration based on linear legendre multi wavelets *Journal of Physics: Conference Series* (IOP Publishing)

[15] Shang X and Han D 2007 *Applied Mathematics and Computation* **191** 440–444

[16] Saberi Najafi H, Aminikhah H and Edalatpanah S A 2016 *Math. Reports* **18(68)** 41–50

[17] Mohammad Hasan Abd Sathar, Ahmad Fadly Nurullah Rasedee and Anvarjon A Ahmedov 2019 *Journal of Engineering and Applied Science* **14** 6255–6259

Chapter 13

Security Threats on the GGH Lattice-Based Cryptosystem

Arif Mandangan[1,2], Hailiza Kamarulhaili[1], **Muhammad Asyraf Asbullah**[3,4,*]

[1] School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Penang, Gelugor, Pulau Pinang, Malaysia.
[2] Mathematics, Real Time Graphics and Visualization Laboratory, Faculty of Sciences and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia.
[3] Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Sciences, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[4] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Serdang, Selangor, Malaysia.

*Corresponding author: ma_asyraf@ums.edu.my

Abstract

Since the modern era of cryptography, the construction of most cryptographic schemes such as the Rivest-Shamir-Adleman (RSA), ElGamal and Elliptic Curves cryptosystems are based on number theory. Lately, these cryptosystems are conjectured to be broken once the Shor's algorithm could be executed in fully functioning quantum computers. To face this global crisis, cryptography society is currently moving towards a new era that is referred to as the post-quantum cryptography where lattice-based cryptography emerges as one of the most promising schemes. The construction of the lattice-based cryptographic schemes relies on linear algebra with simpler and cheaper mathematical operations involving vectors and matrices. In this paper, we revisit the construction of the first lattice-based encryption scheme that was considered practical known as the Goldreich-Goldwasser-Halevi (GGH) cryptosystem. Despite offering better efficiency and practicality compared to number-theoretical schemes, the GGH cryptosystem is considered broken due to the Nguyen's and Lee-Hahn's attacks. Moreover, we described these attacks in detail for allowing us to investigate the weakness points of the GGH cryptosystem that being exploited by the attacks. Finally, we also proposed some potential strategy to strengthen the GGH cryptosystem for making it survive.

Keywords: Post-quantum cryptography, lattice-based cryptography, GGH cryptosystem, closest-vector problem, shortest-vector problem, lattices.

13.1 Introduction

The first lattice-based cryptosystem that was considered practical is proposed by Goldreich, Goldwasser and Halevi [2], widely known as the Goldreich-Goldwasser-Halevi (GGH) cryptosystem. The GGH cryptosystem surpasses the well-established schemes such as the RSA [3] and ElGamal [4] cryptosystems in terms of the efficiency of its encryption and decryption algorithms. Without involvement of any high-cost integer exponentiation operations, the encryption and decryption algorithms of the GGH cryptosystem executed using some lower computational-cost algebraic operations on vectors and matrices. The security of the GGH cryptosystem is relying on the conjectured-hardness of a Closest-Vector Problem (CVP) instance that arose from its trapdoor function. The instance is referred to as the GGH-CVP instance. After various experiments and thorough security analyses, the GGH cryptosystem was conjectured to be intractable once it is implemented in a lattice with dimension beyond 200.

The conjecture became more reliable when all initial attempts for decrypting the GGH Internet Challenges [5] that was published on the Internet, only managed to decypt the challenge in the lowest lattice dimension of 200 and failed to reach the other challenges in the lattice dimensions of 250 up to 400. Nguyen [6] realized that the underlying GGH-CVP instance is hard to solve in its original form. Although it is reduceable to its corresponding Shortest-Vector Problem (SVP) instance, the derived SVP instance also hard to solve in the lattice dimension beyond 200. Later, Nguyen [6] discovered a novel strategy for breaking the GGH Cryptosystem. Consequently, the Nguyen's attack completely decrypted the GGH Internet Challenges in the lattice dimension of 200 up to 350, where the GGH cryptosystem was conjectured intractable in these dimensions. However, the attack only managed to partially decrypt the challenge in the lattice dimension of 400. Only about 10 years later, Lee and Hahn [7] completely decrypted the whole ciphertext of the challenge in a lattice dimension of 400.

In this paper, we revisit the construction of the GGH cryptosystem as well as the security threats on it. From that, we investigate the weakness points of the GGH cryptosystem that was exploited by those attacks. By considering these weakness points, we propose some potential remedies to strengthen the security of the GGH cryptosystem for making it survive against those security threats. This paper is organized in the following flow. In Section 2, we provide some mathematical background related to our discussion. Then, we provide a light introduction to the GGH cryptosystem in Section 3 and then followed by the security threats on it in Section 4. The investigation of the weakness points of the GGH cryptosystem is presented in Section 5 and the proposed potential strategies for strengthening the GGH cryptosystem is given in Section 6. Finally, this paper is concluded in Section 7.

13.2 Mathematical Background

All vectors are considered as column vectors. For $m \in \mathbb{N}$, then $\vec{u}_1 \in \mathbb{R}^m$ is a column vector with entries $u_{i,1} \in \mathbb{R}$ for all $i = 1, \ldots, m$. The vector $\vec{u}_1$ and its entries can be

represented as follows, $\vec{u}_1 = \begin{bmatrix} u_{1,1} \\ u_{2,1} \\ \vdots \\ u_{m,1} \end{bmatrix} \in \mathbb{R}^m$. Any vector $\vec{u}_1 \in \mathbb{R}^m$ can be converted into an integer vector $\lfloor \vec{u}_1 \rceil \in \mathbb{Z}^m$ by rounding each entry $u_{i,1} \in \mathbb{R}$ to its nearest integer $\lfloor u_{i,1} \rceil \in \mathbb{Z}$ such that $|u_{i,1} - \lfloor u_{i,1} \rceil| < 1/2$ for all $i = 1, \ldots, m$.

Definition 13.2.1. [8] Let $m \in \mathbb{N}$. The set of vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in \mathbb{R}^m$ is said to be linearly independent if the only way to obtain the following linear combination,

$$\alpha_1 \vec{u}_1 + \alpha_2 \vec{u}_2 + \cdots + \alpha_n \vec{u}_n = \vec{0} \tag{13.1}$$

is when the scalars $\alpha_i = 0$ for all $i = 1, \ldots, n$. Otherwise, the set is called linearly dependent.

The lattice $\mathcal{L}$ that is spanned by the set of linearly independent vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in \mathbb{R}^m$ is defined as the following,

Definition 13.2.2. [8] For $m, n \in \mathbb{N}$ with $m \leq n$, let $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in \mathbb{R}^m$ be the set of linearly independent vectors. The lattice $\mathcal{L}$ generated by the vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$ is defined as the set of all linear combinations of the vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$ with integer scalars, i.e.,

$$\mathcal{L} = \{a_1 \vec{u}_1 + a_2 \vec{u}_2 + \cdots + a_n \vec{u}_n : a_i \in \mathbb{Z}, \forall i = 1, \ldots, n\} \tag{13.2}$$

The set $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in \mathbb{R}^m$ that span the lattice $\mathcal{L}$ is called the basis for the lattice $\mathcal{L}$. The vectors in the lattice basis are referred to as basis vectors. The number of these basis vectors is representing the dimension of the lattice $\mathcal{L}$, i.e., $dim(\mathcal{L}) = n$ and the number of entries in the basis vector $\vec{u}_i \in \mathbb{R}^m$ is representing the rank of the lattice $\mathcal{L}$, i.e., $rank(\mathcal{L}) = m$. When $m = n$, then the lattice $\mathcal{L}$ is called a full-rank lattice. From here, we only deal with this kind of the lattice in the rest of this paper.

Suppose that $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ be a basis for the full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$. The basis $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n$ could be represented in a matrix form as the following,

$$G = \begin{pmatrix} \vec{g}_1 & \vec{g}_2 & \cdots & \vec{g}_n \end{pmatrix} = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1} & g_{n,2} & \cdots & g_{n,n} \end{pmatrix}. \tag{13.3}$$

where the basis vectors $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n$ become the columns of the matrix $G \in \mathbb{R}^{n \times n}$.

Theorem 13.2.3. A square matrix is invertible if and only if its columns are linearly independent [9].

Thus, the basis G for the full-rank lattice $\mathcal{L}$ is a non-singular matrix with $\det(G) \neq 0$. For any non-singular integer matrix, the inverse of this matrix does not guaranteed to be an integer matrix. However, there is a non-singular integer matrix that has special property where the inverse of this matrix is guaranteed to be an integer matrix as well. This kind of matrix is called unimodular matrix.

Definition 13.2.4. [10] Let $n \in \mathbb{N}$. A unimodular matrix $U \in \mathbb{Z}^{n \times n}$ is a square matrix with integer entries and $\det(U) = \pm 1$.

The lattice $\mathcal{L}$ can be spanned by more than one basis. Two different bases for the same lattice $\mathcal{L}$ are mathematically related by a unimodular matrix.

Proposition 13.2.5. [11] For $n \in \mathbb{N}$, let $G, B \in \mathbb{R}^{n\times n}$ be two non-singular matrices. The matrices G and B generate the same lattice $\mathcal{L} \subset \mathbb{R}^n$, denoted as $L(G) = L(B) = \mathcal{L}$, if and only if these matrices are related by a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ such that $G = BU$.

When $n \geq 2$, there are infinitely many unimodular matrices. Therefore, a lattice $\mathcal{L} \subset \mathbb{R}^n$ with dimension $n \geq 2$ has infinitely many bases. These bases have different quality in terms of the length and orthogonality of basis vectors. A lattice basis with short and slightly non-orthogonal basis vectors is referred to as a 'good basis' while a lattice basis with long and highly non-orthogonal basis vectors is referred to as a 'bad basis'. The length of a basis vector can be measured as an Euclidean norm while the distance between two vectors can be measured as an Euclidean distance.

Definition 13.2.6. [12] For $n \in \mathbb{N}$, let $\vec{u}_1, \vec{u}_2 \in \mathbb{R}^n$. The Euclidean norm of the vector $\vec{u}_1$ is computed as follows,

$$\|\vec{u}_1\| = \sum_{i=1}^{n} (u_{i,1})^2 \tag{13.4}$$

and the Euclidean distance between the vectors $\vec{u}_1$ and $\vec{u}_2$ is computed as follows,

$$\|\vec{u}_1 - \vec{u}_2\| = \sum_{i=1}^{n} (u_{i,1} - u_{i,2})^2 \tag{13.5}$$

The orthogonality of vectors can be determined by using a quantity that is called dot product. The dot product of two vectors in $\mathbb{R}^n$ is defined as follows:

Definition 13.2.7. For $n \in \mathbb{N}$, let $\vec{u}_1, \vec{u}_2 \in \mathbb{R}^n$. The dot product of $\vec{u}_1$ and $\vec{u}_2$ is computed as follows,

$$\vec{u}_1 \cdot \vec{u}_2 = \sum_{i=1}^{n} (u_{i,1} u_{i,2}) \in \mathbb{R} \tag{13.6}$$

If $\vec{u}_1 \cdot \vec{u}_2 = 0$, then $\vec{u}_1$ and $\vec{u}_2$ are said to be orthogonal. Otherwise, these vectors are said to be non-orthogonal. The degree of non-orthogonality of basis vectors $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ can be measured by computing the dual-orthogonal defect of the basis G as follows:

Definition 13.2.8. [2] For $n \in \mathbb{N}$, let $G \in \mathbb{R}^{n\times n}$ with columns $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ be a basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$. The dual-orthogonal defect of the basis G is computed as follow,

$$dual_{OD}(G) = \frac{\prod_{i=1}^{n} \|\vec{g}_i'\|}{|\det G^{-1}|} \tag{13.7}$$

where $\|\vec{g}_i'\|$ is the Euclidean norm of the i-th row vector in G^{-1}.

The smaller the dual-orthogonal defect is, then the more orthogonal basis vectors in the basis G. On the contrary, the larger the dual-orthogonal defect indicates that the more non-orthogonal basis vectors in the basis G. Thus, the basis G is required to have small dual-orthogonal defect in order to be classified as a good basis while to be a bad basis, the basis G is required to have large dual-orthogonal defect.

Most of the lattice problems are related to vectors' norm and distance minimizations. Before we provide the definition of some well-established lattice problems, consider the following definition regarding the shortest non-zero vector in the lattice $\mathcal{L} \subset \mathbb{R}^n$.

Definition 13.2.9. [7] For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. The i-th minimum of the lattice $\mathcal{L}$, denoted as $\lambda_i(\mathcal{L})$, is defined by the radius of the smallest sphere centered in the origin containing i linearly independent lattice vectors.

Basically, the first minimum of the lattice $\mathcal{L}$ is $\lambda_1(\mathcal{L}) = \|\vec{v}_1\|$, where $\vec{v}_1 \in \mathcal{L}$ is shortest non-zero vector in the lattice $\mathcal{L}$ and the second minimum of the lattice is $\mathcal{L}$ is $\lambda_2(\mathcal{L}) = \|\vec{v}_2\|$, where $\vec{v}_2 \in \mathcal{L}$ is the second shortest non-zero vector in the lattice $\mathcal{L}$ such that $\|\vec{v}_1\| < \|\vec{v}_2\|$. From the successive minima of the lattice $\mathcal{L}$, the lattice gap for the lattice $\mathcal{L}$ can be measured as follows,

Definition 13.2.10. [6] For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice with successive minima $\lambda_1, \lambda_2 \in \mathbb{R}$. The lattice gap for the lattice $\mathcal{L}$ is the ratio between the second minimum and the length of the shortest non-zero vector in the lattice $\mathcal{L}$, i.e.,

$$lattice_{gap}(\mathcal{L}) = \frac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})} \in \mathbb{R}$$

The orthogonality of any lattice basis could be enhanced by performing lattice reduction operation on it by using lattice-reduction algorithm such as the *LLL*-algorithm [13] and its variants. For instance, let B be a basis for the lattice $\mathcal{L}$ that consisting long and highly non-orthogonal basis vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$. By reducing the basis B using the *LLL*-algorithm, the reduced form of the basis B, denoted as B_{LLL} has shorter and more orthogonal basis vectors $\vec{\beta}_1, \vec{\beta}_2, \ldots, \vec{\beta}_n$ where the first vector $\vec{\beta}_1 \in B_{LLL}$ is the approximated shortest non-zero vector in the lattice $L(B) = \mathcal{L}$. Although the *LLL*-algorithm is a polynomial-time algorithm, it only manages to approximate a shortest non-zero vector in the lattice $\mathcal{L}$ to an exponential approximation factor in the lattice dimension n. The lattice gap plays significant role in lattice reduction operation. It is experimentally shown that the larger the lattice gap is, the easier lattice reduction operation becomes [6]. That means, lattice-reduction algorithm could perform better when the lattice gap is large.

The security of lattice-based cryptosystems are relying on some well-established hard lattice problems such as the Shortest-Vector Problem (SVP), Closest-Vector Problem (CVP) and the variants of these problems.

Definition 13.2.11. [11] For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. Given a basis for the lattice $\mathcal{L}$, the Shortest-Vector Problem (SVP) is to find a non-zero vector $\vec{v} \in \mathcal{L}$ such that the Euclidean norm $\|\vec{v}\|$ is minimal, i.e., $\|\vec{v}\| = \lambda_1(\mathcal{L})$.

Definition 13.2.12. [8] For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. Given a basis of the lattice $\mathcal{L}$ and a target vector $\vec{t} \in \mathbb{R}^n$, the Closest-Vector Problem (CVP) is to find a non-zero vector $\vec{v} \in \mathcal{L}$ such that the Euclidean norm $\|\vec{t} - \vec{v}\|$ is minimum .

The CVP is an NP-hard problem while the SVP is an NP-hard under randomize reduction [8]. Although both problems are considered hard, the CVP is proven to be a little bit harder than the SVP [14]. Using embedding technique, the CVP in n-dimensional lattice can be reduced into an SVP instance in an $(n+1)$-dimensional lattice. Solving the derived SVP instance could immediately solve the corresponding CVP instance.

The solution of the SVP can be approximated using lattice-reduction algorithm while the solution of the CVP can be approximated by using Babai's round-off method.

Theorem 13.2.13. [8] For $n \in \mathbb{N}$, let $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ be the basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\vec{t} \in \mathbb{R}^n$ be a target vector. If the basis vectors $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ are sufficiently orthogonal to one another, the following algorithm of the Babai's round-off method solves the CVP:

Table 13.1: Algorithm of the Babai's Round-off Method

Input	The basis vectors $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ and the target vector $\vec{t} \in \mathbb{R}^n$.
Steps	Write the vector $\vec{t}$ in a linear combination form as follows, $\vec{t} = \alpha_1\vec{g}_1 + \alpha_2\vec{g}_2 + \cdots + \alpha_n\vec{g}_n = G\vec{\alpha}$ where $G \in \mathbb{R}^{n\times n}$ is a matrix with columns $\vec{g}_i$ and $\vec{\alpha} \in \mathbb{R}^n$ is an unknown vector of scalars. Compute the unknown vector $\vec{\alpha}$ as $\vec{\alpha} = B^{-1}\vec{t}$. Round each entry $\alpha_i \in \vec{\alpha}$ to the nearest integer $\lfloor \alpha_i \rceil \in \mathbb{Z}$ such that $\lvert \alpha_i - \lfloor \alpha_i \rceil \rvert < \frac{1}{2}$ for all $i = 1, \ldots, n$.
Output	Compute a lattice vector $\vec{v} \in \mathcal{L}$ as, $\vec{v} = \lfloor \alpha_1 \rceil \vec{g}_1 + \lfloor \alpha_2 \rceil \vec{g}_2 + \cdots + \lfloor \alpha_n \rceil \vec{g}_n$.

In general, if the basis vectors are reasonably orthogonal to one another, then the algorithm solves some version of approximation CVP. But if the basis vectors are highly non-orthogonal, then the lattice vector returned by the algorithm is generally far from the target vector $\vec{t}$.

13.3 GGH Encryption Scheme

Goldreich *et. al* [2] proposed a trapdoor one-way function inspired by two scenario in lattice. The function is referred to as the GGH trapdoor one-way function. Firstly, the one-way function is developed based on the scenario in lattice where using a given lattice vector $\vec{v} \in \mathcal{L} \subset \mathbb{R}^n$ and an small error vector $\vec{e} \in \mathbb{R}^n$, to compute a non-lattice vector $\vec{t} \in \mathbb{R}^n$ such that $\vec{t} = \vec{v} + \vec{e}$ is an easy task. On the contrary, the task to recover the lattice vector $\vec{v}$ from the given target vector $\vec{t}$ without knowing the error vector $\vec{e}$ is hard to be done especially when the dimension n is large. This scenario could be considered as a CVP instance. We address the CVP instance that arose from the GGH one-way function as the GGH-CVP instance. The task for solving the GGH-CVP instance can be made easier is by introducing a trapdoor information.

Thus, the idea to create the trapdoor information is inspired from the scenario in lattice where every basis of the same lattice offers different ability in assisting the Babai's round-off method for solving the GGH-CVP instance. By executing the method using a 'good' basis, the returned lattice vector is located closest to the target vector. However, the method performs badly when it is executed using a 'bad' basis. Therefore, the 'good' basis could be considered as the trapdoor information for the GGH trapdoor one-way function. From the proposed GGH trapdoor one-way function, Goldreich *et. al* [2] developed an encryption scheme that we called as the

GGH cryptosystem and a digital signature scheme. This paper is only discussing the former one.

To describe the GGH cryptosystem, consider the following communication scenario. Suppose that Alice and Bob want to communicate and they decide to use GGH cryptosystem. As a message recipient, Alice performs the keys generation process. Firstly, she decides her security parameter $n \in \mathbb{N}$ which is representing the dimension of the lattice to be implemented by the GGH cryptosystem. Next, Alice generates her private key which is a 'good basis' $G \in \mathbb{R}^{n\times n}$ for the lattice $\mathcal{L} \subset \mathbb{R}^n$ with low dual-orthogonal defect. From the generated G, Alice determines the threshold parameter $\sigma \in \mathbb{R}$ based on the following condition,

Theorem 13.3.1. For $n \in \mathbb{N}$, let $G \in \mathbb{R}^{n\times n}$ be the private basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\rho \in \mathbb{R}$ denotes the maximum l_1-norm of the rows of G^{-1}. As long as the threshold parameter $\sigma \in \mathbb{R}$ satisfies

$$\sigma < \frac{1}{2\rho}, \tag{13.8}$$

then no decryption error can occur [2].

Next, Alice generates a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ and followed by the generation of her public key which is a 'bad basis' $B \in \mathbb{R}^{n\times n}$ for the lattice $\mathcal{L}$ such that $B = GU^{-1}$. Basically, Alice's private and public keys are two different bases G and B that span the same lattice $\mathcal{L} \subset \mathbb{R}^n$, i.e., $L(G) = L(B) = \mathcal{L}$. Alice sends the parameters (n, σ) and her public basis B to Bob and keeps the unimodular matrix U and her private basis G secretly.

Upon receiving the information from Alice, Bob generates two vectors prior the encryption process namely an integer vector $\vec{m} \in \mathbb{Z}^n$ that contains the encoded secret message and a small error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$. Although the parameter σ is a public information, the actual arrangement of the entries $-\sigma$ and $+\sigma$ in the error vector $\vec{e}$ is known by Bob alone. Even Alice has no idea about the exact arrangement of these entries in the Bob's error vector $\vec{e}$. The secret vector $\vec{m}$ is encrypted as follows,

$$\vec{c} = B\vec{m} + \vec{e} \tag{13.9}$$

where $\vec{c} \in \mathbb{R}^n$ is a ciphertext vector and $B\vec{m}$ is a lattice vector, denoted as $\vec{v} = B\vec{m} \in L(B)$ since B is a lattice basis and $\vec{m} \in \mathbb{Z}^n$. Bob sends the ciphertext $\vec{c}$ to Alice.

Upon receiving the ciphertext $\vec{c}$ from Bob, Alice uses her private 'good basis' G to execute the Babai's round-off method. Firstly, Alice represents the ciphertext $\vec{c}$ in a linear combination form as follows,

$$\vec{c} = \alpha_1\vec{g}_1 + \alpha_2\vec{g}_2 + \cdots + \alpha_n\vec{g}_n \tag{13.10}$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \alpha_1 \begin{bmatrix} g_{1,1} \\ g_{2,1} \\ \vdots \\ g_{n,1} \end{bmatrix} + \alpha_2 \begin{bmatrix} g_{1,2} \\ g_{2,2} \\ \vdots \\ g_{n,2} \end{bmatrix} + \cdots + \alpha_n \begin{bmatrix} g_{1,n} \\ g_{2,n} \\ \vdots \\ g_{n,n} \end{bmatrix} \tag{13.11}$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1} & g_{n,2} & \cdots & g_{n,n} \end{pmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \tag{13.12}$$

$$\vec{c} \;=\; G\vec{\alpha} \tag{13.13}$$

where $\vec{\alpha} \in \mathbb{R}^n$ is in unknown vector. Next, Alice computes the unknown $\vec{\alpha}$ as $\vec{\alpha} = G^{-1}\vec{c}$ and round each entry $\alpha_i \in \mathbb{R}$ to the nearest integer $\lfloor \alpha_i \rceil \in \mathbb{Z}$ such that $|\alpha_i - \lfloor \alpha_i \rceil| < \frac{1}{2}$ for all $i = 1, \ldots, n$ and form an integer vector $\lfloor \vec{\alpha} \rceil \in \mathbb{Z}^n$. Finally, Alice performs the decryption as follows,

$$\begin{aligned}
U\lfloor \vec{\alpha} \rceil &= U\lfloor G^{-1}\vec{c} \rceil, \textit{since } \vec{\alpha} = G^{-1}\vec{c} \\
&= U\lfloor G^{-1}(B\vec{m} + \vec{e}) \rceil, \textit{since } \vec{c} = B\vec{m} + \vec{e} \\
&= U\lfloor G^{-1}B\vec{m} + G^{-1}\vec{e} \rceil \\
&= \lfloor UG^{-1}B\vec{m} \rceil + U\lfloor G^{-1}\vec{e} \rceil \\
&= \lfloor B^{-1}GG^{-1}B\vec{m} \rceil + U\lfloor G^{-1}\vec{e} \rceil, \textit{since } U = B^{-1}G \\
&= \lfloor \vec{m} \rceil + U\lfloor G^{-1}\vec{e} \rceil \\
&= \vec{m} + U\lfloor G^{-1}\vec{e} \rceil, \textit{since } \vec{m} \in \mathbb{Z}^n
\end{aligned}$$

If $\lfloor G^{-1}\vec{e} \rceil = \vec{0}$, then

$$\begin{aligned}
U\lfloor \vec{\alpha} \rceil &= \vec{m} + U\lfloor \vec{0} \rceil \\
&= \vec{m}
\end{aligned}$$

where $\vec{m}$ contains the secret message from Bob. Obviously, decryption error could be avoided if and only if $\lfloor G^{-1}\vec{e} \rceil = \vec{0}$ and this could be met if the chosen threshold parameter σ fulfills the condition as stated in Theorem 13.3.1.

The security of the GGH cryptosystem is relying on the GGH-CVP instance that arose from the GGH trapdoor one-way function. Mandangan *et. al* [18] explicitly defined the GGH-CVP instance as the following:

Definition 13.3.2. Let $n \in \mathbb{N}$. Given a basis B for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, a perturbation parameter $\sigma \in \mathbb{R}$ and a ciphertext $\vec{c} \in \mathbb{R}^n$ such that $\vec{c} = \vec{v} + \vec{e}$, where $\vec{v} \in \mathcal{L}$ is an unknown error vector and $\vec{e} \in \{-\sigma, +\sigma\}^n$ is an unknown small vector. The GGH-CVP instance is a problem to find a lattice vector $\vec{v}$ that is closest to ciphertext $\vec{c}$ which minimizes the Euclidean distance $\|\vec{c} - \vec{v}\|$.

By solving the GGH-CVP instance, Eve as an attacker could obtain a lattice vector $\vec{w} \in \mathcal{L}$ that is closest to the ciphertext $\vec{c}$. If $\vec{w} = \vec{v}$, then Eve could recover the encrypted secret vector $\vec{m}$ since $\vec{v} = B\vec{m}$. As stated in [6], the Euclidean distance between the given target vector and the desired lattice vector is $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$. We provide the proof as the following:

Proposition 13.3.3. For $n \in \mathbb{N}$, let $B \in \mathbb{R}^{n \times n}$ a public basis, $\vec{m} \in \mathbb{Z}^n$ be a vector with encoded secret message, $\vec{c} \in \mathbb{R}^n$ be a ciphertext vector and $\vec{e} \in \{-\sigma, +\sigma\}^n$ be an error vector such that $\vec{c} = B\vec{m} + \vec{e}$. Then, $\|\vec{c} - B\vec{m}\| = \sigma\sqrt{n}$.

Proof. Given that $\vec{c} = B\vec{m} + \vec{e}$ and $\vec{e} \in \{-\sigma, +\sigma\}^n$. Thus,

$$\begin{aligned}
\vec{c} - B\vec{m} &= \vec{e} \\
\|\vec{c} - B\vec{m}\| &= \|\vec{e}\| \\
&= \sqrt{\sum_{i=1}^{n} (e_i)^2}
\end{aligned}$$

$$
\begin{aligned}
&= \sqrt{\sum_{i=1}^{n} (\pm\sigma)_i^2} \\
&= \sqrt{n\sigma^2} \\
&= \sigma\sqrt{n}
\end{aligned}
$$

□

With distance $\|\vec{c} - B\vec{m}\| = \sigma\sqrt{n}$, the underlying GGH-CVP instance has been experimentally tested, analysed and conjectured by its inventors to be invulnerable to some possible attacks once the implemented lattice dimension is larger than 150 [2]. The tested attacks and the experiment results are summarized in Table 13.2.

Table 13.2: Security analyses on the GGH Cryptosystem

Attacks	**Experimental Results**
Round-off attack	Fails once the lattice dimension $n > 90$.
Nearest-plane attack	Fails once the lattice dimension $n > 140$.
Embedding attack	Fails once the lattice dimension $n > 120$.

To establish the GGH cryptosystem, its inventors published five challenges on the Internet, known as the GGH Internet Challenges [5]. In these challenges, ciphertext produced by the GGH cryptosystem in the lattice dimensions of 200, 250, 300, 350 and 400 are published together with the corresponding public bases that used to produce each ciphertext. The challenge is to decrypt the published ciphertext based on the given information. In the beginning, it was look promising when all earlier attempts for solving the challenges failed to decrypt the published ciphertext. One of the ways to solve the challenge is by solving the underlying GGH-CVP instance. Using embedding technique, the GGH-CVP instance in the lattice $\mathcal{L} \subset \mathbb{R}^n$ is reduceable to an SVP instance in an embedded lattice $\mathcal{L}' \subset \mathbb{R}^{n+1}$. Then, lattice-reduction algorithms can be used to solve the derived SVP instance. The solution of the derived SVP instance could immediately solve the corresponding GGH-CVP instance. We address this approach as embedding attack.

Using the embedding attack, Schnorr *et. al* [15] successfully break the GGH cryptosystem but only in a lattice dimension up of 150. The GGH Internet Challenges attracted the attention of Nguyen [6], who is one of the prolific cryptanalysts in lattice-based cryptography. In his earlier attempt, he tried to solve the underlying GGH-CVP instance by executing the improved algorithm of Schnorr and Hörner [16] using Shoup's NTL package [17]. After a few days of execution processes, the only solvable challenge is the one in the lowest lattice dimension of 200. In higher lattice dimensions, the challenges were unsolvable which makes the GGH Cryptosystem being potentially considered as a secure and practical lattice-based encryption scheme. The underlying GGH-CVP instance seems to be unsolvable in the lattice dimensions beyond 200.

Realizing that the GGH-CVP instance is hard solve in its original form, Nguyen [6] discovered a novel strategy for simplifying the GGH-CVP instance which eventually made it solvable and consequently made the GGH cryptosystem broken. The Nguyen's attack completely decrypted the GGH Internet Challenges in the lattice dimensions of 200 up to 350. By extending the Nguyen's attack, another attack by Lee and Hahn [7] finally decrypted the whole ciphertext of the final challenge in the

lattice dimension of 400. Similarly, the embedding attack is used in the final stage of both attacks. Therefore, we consider that the embedding attack, Nguyen's attack and Lee-Hahn's attack as the fatal security threats on the GGH cryptosystem.

13.4 Security Threats on the GGH Cryptosystem

In this section, we revisit the fatal security threats on the GGH cryptosystem with focus more into the mathematical aspect of these attacks for allowing us to investigate the weakness points of the GGH cryptosystem that was exploited by those attacks.

13.4.1 Embedding Attack

The embedding attack is a combination of embedding technique and lattice-reduction algorithm. The embedding technique is used to reduce the CVP instance into an SVP instance while the lattice-reduction algorithm is used to solve the derived SVP instance. The performance of this attack depends on two factors. Firstly is the lattice gap in the embedded lattice $\mathcal{L}' \subset \mathbb{R}^{n+1}$. As mentioned by Nguyen [6], the larger the lattice gap is then the easier reduction can be done by lattice-reduction algorithm. The second factor is the lattice dimension n. In small dimension n, lattice-reduction algorithm could perform well for solving the SVP. However, the performance degrades exponentially as the lattice dimension n grows. That is why the embedding attack was failed to break the GGH cryptosystem in the lattice dimension beyond 120 as tested in [2].

To describe the embedding attack on the GGH-CVP instance, consider a lattice $\mathcal{L} \subset \mathbb{R}^n$ with basis $B \in \mathbb{R}^{n \times n}$ and a target vector $\vec{c} \in \mathbb{R}^n$. The aim of this attack is to obtain a lattice vector $\vec{v} \in L(B) = \mathcal{L}$ that is located closest to the target vector $\vec{c}$. To launch the embedding attack, firstly the embedding technique is used where the target vector $\vec{c}$ is embedded into the basis B to form a new basis $X \in \mathbb{R}^{(n+1)\times(n+1)}$ for a new lattice $\mathcal{L}' \subset \mathbb{R}^{(n+1)}$. The new basis X has the following form,

$$X = \begin{pmatrix} \vec{c} & \vec{b_1} & \cdots & \vec{b_n} \\ 1 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} c_1 & b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ c_2 & b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \\ c_n & b_{n,1} & b_{n,2} & \cdots & b_{n,n} \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{13.14}$$

where $c_i \in \vec{c}$ and $b_{i,j} \in \vec{b_j}$ for all $i, j = 1, \ldots, n$. Suppose that the desired lattice vector $\vec{v} \in L(B)$ in the GGH-CVP instance is represented in the following linear combination form,

$$\vec{v} = \alpha_1 \vec{b}_1 + \alpha_2 \vec{b}_2 + \cdots + \alpha_n \vec{b}_n \tag{13.15}$$

where $\alpha_i \in \mathbb{Z}$ for all $i = 1, \ldots, n$. Then, consider a non-zero vector $\vec{\delta}_1$ in the embedded lattice $L'(X) = \mathcal{L}'$ that is represented in the following form,

$$\begin{aligned} \vec{\delta}_1 &= \alpha' \begin{bmatrix} \vec{c} \\ 1 \end{bmatrix} - \alpha_1 \begin{bmatrix} \vec{b_1} \\ 0 \end{bmatrix} - \alpha_2 \begin{bmatrix} \vec{b_2} \\ 0 \end{bmatrix} - \cdots - \alpha_n \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix} \\ &= \alpha' \begin{bmatrix} \vec{c} \\ 1 \end{bmatrix} - \left(\alpha_1 \begin{bmatrix} \vec{b_1} \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} \vec{b_2} \\ 0 \end{bmatrix} + \cdots + \alpha_n \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix} \right). \end{aligned} \tag{13.16}$$

By letting $\alpha' = 1$ and considering equation (13.15), we have

$$\vec{\delta}_1 \quad = \quad \begin{bmatrix} \vec{c} \\ 1 \end{bmatrix} - \begin{bmatrix} \vec{v} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{c} - \vec{v} \\ 1 \end{bmatrix} \tag{13.17}$$

In the GGH-CVP instance, we have $\vec{c} = \vec{v} + \vec{e}$ which implies that $\vec{c} - \vec{v} = \vec{e}$. Hence, we have

$$\vec{\delta}_1 = \begin{bmatrix} \vec{e} \\ 1 \end{bmatrix} \in L'(X). \tag{13.18}$$

where $\vec{e} \in \{-\sigma, +\sigma\}^n$. Since $\vec{e}$ is a small vector for ensuring that the vectors $\vec{c}$ and $\vec{v}$ are located closest to each other, then the embedding attack is expecting that vector $\vec{\delta}_1$ as the shortest non-zero vector in the embedded lattice $L'(X)$.

Finding for the shortest vector $\vec{\delta}_1$ in the embedded lattice $L'(X)$ is an SVP instance. That means, the embedding technique has reduced the underlying GGH-CVP instance into an SVP instance. We address the instance as the GGH-SVP instance. To solve the derived GGH-SVP instance, the embedding attack uses the lattice reduction algorithm for reducing the embedded basis X. Suppose that the used algorithm is the LLL-algorithm. Then, we denote the LLL-reduced form of the basis X as $X_{LLL} = \{\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_{n+1}\}$ where the first reduced basis vector $\vec{x}_1$ is the shortest vector in the reduced-basis X_{LLL}. Therefore, the lattice-reduction algorithm returns the shortest vector $\vec{x}_1 = \vec{\delta}_1$ as the solution of the GGH-SVP instance. From the obtained solution $\vec{x}_1$, then we can easily solve the equation (13.17) for the unknown vector $\begin{bmatrix} \vec{v} \\ 0 \end{bmatrix}$ since the ciphertext $\vec{c}$ is known. To obtain the vector $\vec{v}$, simply compute

$$\begin{bmatrix} \vec{v} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{c} \\ 1 \end{bmatrix} - \vec{x}_1. \tag{13.19}$$

Obviously, the obtained vector $\begin{bmatrix} \vec{v} \\ 0 \end{bmatrix}$ contains the desired lattice vector $\vec{v} \in \mathcal{L}$ which immediately solves the GGH-CVP instance.

The most challenging part in the embedding attack is the execution of the lattice-reduction operations on the embedded basis X. This is because, the public basis B is a bad basis consisting of long and highly non-orthogonal basis vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$. Consequently, the execution time could be too long and the obtained vector $\vec{x}_1$ could be not the shortest vector in the lattice $L'(X)$. That is why, the attempt by Schnorr *et. al* [15] for breaking the GGH cryptosystem using the embedding attack by implementing the LLL-algorithm to perform the lattice-reduction operation only managed to break the cryptosystem in a lattice dimension up to 150. Similarly, the initial embedding attack by Nguyen [6] using the pruning enumeration-algorithm to perform the lattice-reduction operation also failed to break the GGH Internet Challanges in the lattice dimension beyond 200. Since that, the inventors of the GGH cryptosystem conjectured that the underlying GGH-CVP instance as invulnerable in the lattice dimensions 300 and beyond.

13.4.2 Nguyen's Attack

Instead of directly implementing the embedding attack on the GGH-CVP instance in its original form, the Nguyen's attack [6] is implementing the embedding attack on the simplified version of the GGH-CVP instance. Basically, the Nguyen's attack is consisting of a sequence of three stages. The first stage is an elimination stage which

aims to eliminate the error vector $\vec{e}$ from the encryption equation. To accomplish that aim, an integer vector $\vec{s} = \{+\sigma\}^n$ is inserted into the encryption equation (13.9) as follows,

$$\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} = \frac{\vec{e} + \vec{s}}{2\sigma}. \tag{13.20}$$

Since $\vec{s} = \{+\sigma\}^n$ and $\vec{e} \in \{-\sigma, +\sigma\}^n$, then $\vec{e} + \vec{s} \in \{0, 2\sigma\}^n$. Hence,

$$\frac{\vec{e} + \vec{s}}{2\sigma} \in \{0, 1\}^n \in \mathbb{Z}^n.$$

By considering equation (13.20), we have

$$\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} \in \mathbb{Z}^n$$

as well and this implies that

$$\vec{c} + \vec{s} \equiv B\vec{m} \pmod{2\sigma}. \tag{13.21}$$

Observe that, the error vector $\vec{e}$ has been completely eliminated from the encryption equation.

That means, the attack has completed the elimination stage and now it can proceed to the second stage which is the simplification stage. This stage aims to simplify the underlying GGH-CVP instance. Observe that, the only unknown value in the congruence (13.21) is the secret vector $\vec{m} \in \mathbb{Z}^n$. Solving the congruence (13.21) for the vector $\vec{m}$ yields,

$$\vec{m} \equiv B^{-1}(\vec{c} + \vec{s}) \pmod{2\sigma}. \tag{13.22}$$

For simplicity, denote $B^{-1}(\vec{c} + \vec{s}) = \vec{m}_{2\sigma}$. Then we have

$$\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}. \tag{13.23}$$

Although $\vec{m}_{2\sigma} \neq \vec{m}$, the vector $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}$ provides partial information from the secret vector $\vec{m}$ which allows the simplification of the GGH-CVP instance becomes possible. To perform the simplification process, the partial information $\vec{m}_{2\sigma}$ is multiplied by the basis B and then inserted into both sides of the encryption equation (13.9) as follows,

$$\begin{aligned} \vec{c} - B\vec{m}_{2\sigma} &= B\vec{m} - B\vec{m}_{2\sigma} + \vec{e} \\ &= B(\vec{m} - \vec{m}_{2\sigma}) + \vec{e}. \end{aligned} \tag{13.24}$$

The congruence (13.23) implies that, there exist $\vec{k} \in \mathbb{Z}^n$ such that

$$\vec{m} - \vec{m}_{2\sigma} = 2\sigma\vec{k}. \tag{13.25}$$

Thus, the equation (13.24) can be rewritten as the following,

$$\begin{aligned} \vec{c} - B\vec{m}_{2\sigma} &= B(2\sigma\vec{k}) + \vec{e} \\ \frac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} &= B\vec{k} + \frac{\vec{e}}{2\sigma} \end{aligned} \tag{13.26}$$

For simplicity, denote

$$\frac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} = \vec{s} \in \mathbb{R}^n.$$

Since the ciphertext $\vec{c}$, public basis B, partial information $\vec{m}_{2\sigma}$ and threshold parameter σ are known, then the vector $\vec{s}$ is a known vector. Then, denote $B\vec{k} = \vec{t}$. Note that, B is a basis for the lattice $\mathcal{L}$ and $\vec{k} \in \mathbb{Z}^n$ is an unknown integer vector. Hence, $\vec{t} \in L(B) = \mathcal{L}$ in an unknown lattice vector. Since $\vec{e} \in \{-\sigma, +\sigma\}^n$, then

$$\frac{\vec{e}}{2\sigma} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n.$$

We denote the new error vector as $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. Although the exact arrangement of the entries $\left(-\frac{1}{2}\right)$ and $\left(+\frac{1}{2}\right)$ in the new error vector $\vec{\epsilon}$ is unknown, the entries of this error vector is much smaller than the original error vector $\vec{e} \in \{\sigma, +\sigma\}^n$. Now, the equation (13.26) can be rewritten as follows,

$$\vec{s} = \vec{t} + \vec{\epsilon}. \tag{13.27}$$

A new and simpler GGH-CVP instance can be derived from the equation (13.27). We address the new instance as the Nguyen$_{GGH}$-CVP instance and it can be explicitly defined as follows [18],

Definition 13.4.1. Let $n \in \mathbb{N}$ and $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Given a basis $B \in \mathbb{R}^{n \times n}$ for the lattice $\mathcal{L}$ and a target vector $\vec{s} \in \mathbb{R}^n$ such that

$$\vec{s} = \vec{t} + \vec{\epsilon}$$

where $\vec{t} \in L(B) = \mathcal{L}$ is an unknown lattice vector and $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$ is an unknown error vector. The Nguyen$_{GGH}$-CVP instance is a problem to find a lattice vector $\vec{t}$ that is closest to $\vec{s}$ which minimizes the Euclidean distance $\|\vec{s} - \vec{t}\|$.

Once the simplification stage is accomplished, the Nguyen's attack moves to it's final stages that we address as the solution stage which aims to solve the Nguyen$_{GGH}$-CVP instance. For that purpose, the Nguyen's attack executing the embedding attack on the Nguyen$_{GGH}$-CVP instance. To launch the embedding attack, firstly the embedding technique is used to embed the target vector $\vec{s}$ into the basis B to form a new basis $Y \in \mathbb{R}^{(n+1)\times(n+1)}$ for a new lattice $\mathcal{L}' \subset \mathbb{R}^{(n+1)}$. The new basis Y has the following form,

$$Y = \begin{pmatrix} \vec{s} & \vec{b_1} & \cdots & \vec{b_n} \\ 1 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} s_1 & b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ s_2 & b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \\ s_n & b_{n,1} & b_{n,2} & \cdots & b_{n,n} \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{13.28}$$

where for all $i, j = 1, \ldots, n$, then $s_i \in \vec{s}$ and $b_{i,j} \in \vec{b_j}$ are the columns of the public basis B. Suppose that the desired lattice vector $\vec{t} \in L(B)$ in the Nguyen$_{GGH}$-CVP instance is represented in the following linear combination form,

$$\vec{t} = \beta_1\vec{b_1} + \beta_2\vec{b_2} + \cdots + \beta_n\vec{b_n} \tag{13.29}$$

where $\beta_i \in \mathbb{Z}$ for all $i = 1, \ldots, n$. Then, consider a non-zero vector $\vec{\delta_2}$ in the embedded lattice $L'(Y)$ that is represented in the following form,

$$\vec{\delta_2} = \beta' \begin{bmatrix} \vec{s} \\ 1 \end{bmatrix} - \beta_1 \begin{bmatrix} \vec{b_1} \\ 0 \end{bmatrix} - \beta_2 \begin{bmatrix} \vec{b_2} \\ 0 \end{bmatrix} - \cdots - \beta_n \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix}$$

$$= \beta' \begin{bmatrix} \vec{s} \\ 1 \end{bmatrix} - \left(\beta_1 \begin{bmatrix} \vec{b_1} \\ 0 \end{bmatrix} + \beta_2 \begin{bmatrix} \vec{b_2} \\ 0 \end{bmatrix} + \cdots + \beta_n \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix} \right). \tag{13.30}$$

By letting $\beta' = 1$ and considering equation (13.29), we have

$$\vec{\delta_2} = \begin{bmatrix} \vec{s} \\ 1 \end{bmatrix} - \begin{bmatrix} \vec{t} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{s} - \vec{t} \\ 1 \end{bmatrix} \tag{13.31}$$

In the Nguyen$_{GGH}$-CVP instance, we have $\vec{s} = \vec{t} + \vec{\epsilon}$ which implies that $\vec{s} - \vec{t} = \vec{\epsilon}$. Hence, we have

$$\vec{\delta_2} = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix} \in L'(Y). \tag{13.32}$$

where $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. Since $\vec{\epsilon}$ is a small vector for ensuring that the vectors $\vec{s}$ and $\vec{t}$ are located closest to each other, then the embedding attack is expecting that vector $\vec{\delta_2}$ as the shortest non-zero vector in the embedded lattice $L'(Y)$. Finding for the shortest vector $\vec{\delta_2}$ in the embedded lattice $L'(Y)$ is an SVP instance. That means, the embedding technique has reduced the Nguyen$_{GGH}$-CVP instance into an SVP instance. We address the instance as the Nguyen$_{GGH}$-SVP.

To solve the derived Nguyen$_{GGH}$-SVP instance, the embedding attack uses the lattice reduction algorithm for reducing the embedded basis Y. Suppose that the LLL-algorithm is used. We denote the LLL-reduced form of the basis Y as $Y_{LLL} = \{\vec{y}_1, \vec{y}_2, \ldots, \vec{y}_{n+1}\}$ where the first reduced basis vector $\vec{y}_1$ is the shortest vector in the reduced-basis Y_{LLL}. Therefore, the LLL-algorithm returns the shortest vector $\vec{y}_1 = \vec{\delta_2}$ as the solution of the Nguyen$_{GGH}$-SVP instance.

From the obtained solution $\vec{y}_1$, then we can easily solve the equation (13.31) for the unknown vector $\begin{bmatrix} \vec{t} \\ 0 \end{bmatrix}$ since the target vector $\vec{s}$ is known. To obtain the vector $\vec{t}$, simply compute

$$\begin{bmatrix} \vec{t} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{s} \\ 1 \end{bmatrix} - \vec{y}_1. \tag{13.33}$$

Obviously, the obtained vector $\begin{bmatrix} \vec{t} \\ 0 \end{bmatrix}$ contains the desired lattice vector $\vec{t} \in \mathcal{L}$ which immediately solves the Nguyen$_{GGH}$-CVP instance.

Pereviously, the embedding attack only managed to solve the GGH-CVP instance in the lattice dimension 200 and below. But this time, the embedding attack is managed to solve the Nguyen$_{GGH}$-CVP instance in the lattice dimension beyond 200 up to 350. This indicates that, the Nguyen$_{GGH}$-CVP instance is much easier than the original GGH-CVP instance. Due to a certain reason, the final challenge in the lattice dimension of 400 could only be partially decrypted by the Nguyen's attack. The reason behind this occurence will be discussed in the other section of this paper.

13.4.3 Lee-Hahn's Attack

By using the partially decrypted ciphertext, $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^{400}$ that is published by Nguyen in [6], Lee and Hahn [7] extended the Nguyen's attack to further simplify the underlying GGH-CVP instance which later allowing the Lee-Hahn's attack to completely decrypt the whole ciphertext for the final GGH Internet Challenge in the lattice dimension of 400. Basically, the Lee-Hahn's attack also consisting a sequence of three stages namely the guessing stage, simplification stage and the solution stage.

In order to accomplish its simplification stage, some actual plaintext values are required. For that purpose, the Lee-Hahn's attack initiates it's guessing stage which aims to obtain the actual value of some plantext from the whole plaintext $\vec{m} \in \mathbb{Z}^{400}$ of the final GGH challenge. In the challenge, the plaintext vector $\vec{m}$ has integer entries $m_i \in [-128, 127]$ and the used threshold parameter is $\sigma = 3$. From the elimination stage of the Nguyen's attack, the congruence $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$ holds. Thus,

$$m_i \equiv m_{2\sigma,i} \pmod 6 \tag{13.34}$$

where $m_i \in \vec{m}$ and $m_{2\sigma,i} \in \vec{m}_{2\sigma}$ for all $i = 1, \ldots, 400$ and $2\sigma = 2(3) = 6$. Referring to the published $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^{400}$, the first entry is $m_{2\sigma,1} = 5$. Thus,

$$m_1 \equiv 5 \pmod 6. \tag{13.35}$$

Since $m_1 \in [-128, 127]$, there are 43 possible integers in that interval that could satisfies the congruence (13.35).That means, it is possible to guess the actual value of the first entry m_1. By continuing the same steps, the Lee-Hahn's attack revealed some other entries of the plaintext $\vec{m} \in \mathbb{Z}^{400}$.

Now, the attack could proceed to it's simplification stage which aims to further simplify the GGH-CVP instance. Suppose that the Lee-Hahn's attack has obtained the first $k \in \mathbb{N}$ with $k < 400$, entries out of 400 entries of the plaintext $\vec{m} \in \mathbb{Z}^{400}$. Now, the plaintext $\vec{m} \in \mathbb{Z}^{400}$ can be divided into two blocks as $\vec{m}^1 \in \mathbb{Z}^k$ that contains the known k entries of $\vec{m}$ and $\vec{m}^2 \in \mathbb{Z}^{400-k}$ that contains the remaining $(400 - k)$ unknown entries of $\vec{m}$. Thus, the vector $\vec{m}$ can be represented as follows,

$$\vec{m} = \begin{pmatrix} \vec{m}^1 \\ \vec{m}^2 \end{pmatrix} \in \mathbb{Z}^{400} \tag{13.36}$$

where $m_1, \ldots, m_k \in \vec{m}^1$ and $m_{k+1}, \ldots, m_{400} \in \vec{m}^2$. Similarly, the public basis $B \in \mathbb{R}^{400\times 400}$ also has the following new representation as follows

$$B = \begin{pmatrix} B_1 & B_2 \end{pmatrix} \tag{13.37}$$

where $\vec{b}_1, \ldots, \vec{b}_k \in B_1 \in \mathbb{R}^{400\times k}$ and $\vec{b}_{k+1}, \ldots, \vec{b}_{400} \in B_2 \in \mathbb{R}^{n\times(400-k)}$. Now, the encryption equation (13.9) has a new representation as follows,

$$\begin{aligned} \vec{c} &= \begin{pmatrix} B_1 & B_2 \end{pmatrix} \begin{pmatrix} \vec{m}^1 \\ \vec{m}^2 \end{pmatrix} + \vec{e} \\ \vec{c} &= B_1\vec{m}^1 + B_2\vec{m}^2 + \vec{e} \\ \vec{c} - B_1\vec{m}^1 &= B_2\vec{m}^2 + \vec{e}. \end{aligned} \tag{13.38}$$

Similarly, the published $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^{400}$ also can be represented in two blocks as $\vec{m}_{2\sigma}^1 \in \mathbb{Z}^k$ that contains the first k entries of $\vec{m}_{2\sigma}$ and $\vec{m}_{2\sigma}^2 \in \mathbb{Z}^{400-k}$ that contains the remaining $(400 - k)$ entries of $\vec{m}_{2\sigma}$. Thus, the vector $\vec{m}_{2\sigma}$ be represented as follows,

$$\vec{m}_{2\sigma} = \begin{pmatrix} \vec{m}_{2\sigma}^1 \\ \vec{m}_{2\sigma}^2 \end{pmatrix} \in \mathbb{Z}^{400}. \tag{13.39}$$

From the following multiplication,

$$B\vec{m}_{2\sigma} = \begin{pmatrix} B_1 & B_2 \end{pmatrix} \begin{pmatrix} \vec{m}_{2\sigma}^1 \\ \vec{m}_{2\sigma}^2 \end{pmatrix} = B_1\vec{m}_{2\sigma}^1 + B_2\vec{m}_{2\sigma}^2$$

the vector $B_2\vec{m}_{2\sigma}^2$ can be inserted into the equation (13.38) and yields the following equations,

$$\vec{c} - B_1\vec{m}^1 - B_2\vec{m}_{2\sigma}^2 = B_2\vec{m}^2 - B_2\vec{m}_{2\sigma}^2 + \vec{e}$$

$$\vec{c} - B_1\vec{m}^1 - B_2\vec{m}_{2\sigma}^2 = B_2(\vec{m}^2 - \vec{m}_{2\sigma}^2) + \vec{e}. \tag{13.40}$$

Since $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$, then $\vec{m}^2 \equiv \vec{m}_{2\sigma}^2 \pmod{2\sigma}$. This implies that,

$$\vec{m}^2 - \vec{m}_{2\sigma}^2 = 2\sigma\vec{l} \tag{13.41}$$

where $\vec{l} \in \mathbb{Z}^{400-k}$. Substituting the equation (13.41) into the equation (13.40) yields

$$\vec{c} - B_1\vec{m}^1 - B_2\vec{m}_{2\sigma}^2 = B_2(2\sigma\vec{l}) + \vec{e}$$

$$\frac{\vec{c} - B_1\vec{m}^1 - B_2\vec{m}_{2\sigma}^2}{2\sigma} = B_2\vec{l} + \frac{\vec{e}}{2\sigma}. \tag{13.42}$$

For simplicity, denote the left side of the equation (13.42) as $\vec{p} \in \mathbb{R}^{400}$. Since $\vec{c}, B_1, \vec{m}^1, B_2$ and $\vec{m}_{2\sigma}^2$ are known, then $\vec{p}$ is a known vector. Then, denote $B_2\vec{l} = \vec{q} \in \mathbb{R}^{400}$. Note that, $B_2 \in \mathbb{R}^{400\times(400-k)}$ is a basis for the sub-lattice $L(B_2)$ and $\vec{l} \in \mathbb{Z}^{400-k}$ is an unknown integer vector. Thus, $\vec{q} \in L(B_2)$ is an unknown lattice vector. Note that, the new error vector is similar with the error vector in the Nguyen$_{GGH}$-CVP instance. Thus, we denote the new error vector as $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$ as well. Now, the equation (13.42) can be rewritten as follows,

$$\vec{p} = \vec{q} + \vec{\epsilon}. \tag{13.43}$$

Again, the underlying GGH-CVP instance has been simplified by the Lee-Hahn's attack. A new and simpler GGH-CVP instance can be explicitly defined from the equation (13.43). We refer this instance as LeeHahn$_{GGH}$-CVP instance and it can be explicitly defined as the following [18]:

Definition 13.4.2. Let $k, n \in \mathbb{N}$ where $k < n$ and $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$, be a basis for the full-rank lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$. Suppose that, the basis B is representable as follows,

$$B = \begin{pmatrix} B_1 & B_2 \end{pmatrix}$$

where $\vec{b}_1, \ldots, \vec{b}_k \in B_1 \in \mathbb{R}^{n\times k}$ and $\vec{b}_{k+1}, \ldots, \vec{b}_n \in B_2 \in \mathbb{R}^{n\times(n-k)}$. Given a target vector $\vec{p} \in \mathbb{R}^n$ and the sub-basis B_2 for the sub-latice $L(B_2) \subset \mathbb{R}^n$ such that

$$\vec{p} = \vec{q} + \vec{\epsilon}$$

where $\vec{q} \in \mathcal{L}$ is an unknown lattice vector and $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$ is an unknown error vector. The LeeHahn$_{GGH}$-CVP instance is a problem to find a lattice vector $\vec{q}$ that is closest to $\vec{p}$ which minimizes the Euclidean distance $\|\vec{p} - \vec{q}\|$.

To solve LeeHahn$_{GGH}$-CVP instance, the Lee-Hahn's attack proceeds to its final stage that we address as the solution stage. Similarly as the Nguyen's attack, the Lee-Hahn's attack also executed the embedding attack in its solution stage. To launch the embedding attack, firstly the embedding technique is used to embed the

target vector $\vec{p}$ into the sub-basis B_2 to form a new basis $Z \in \mathbb{R}^{(n+1)\times(n-k+1)}$ for a new lattice $\mathcal{L}^* \subset \mathbb{R}^{(n+1)}$. The new basis Z has the following form,

$$Z = \begin{pmatrix} \vec{p} & \vec{b}_{k+1} & \cdots & \vec{b}_n \\ 1 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} p_1 & b_{1,k+1} & \cdots & b_{1,n} \\ p_2 & b_{2,k+1} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_n & b_{n,k+1} & \cdots & b_{n,n} \\ 1 & 0 & \cdots & 0 \end{pmatrix} \tag{13.44}$$

where $p_i \in \vec{p}$ and $b_{i,j} \in \vec{b_j}$ are the columns of the sub-basis B_2 for all $i = 1, \ldots, n$ and $j = k+1, \ldots, n$. Suppose that the desired lattice vector $\vec{q} \in L(B_2)$ in the LeeHahn$_{GGH}$-CVP instance is represented in the following linear combination form,

$$\vec{q} = \gamma_1 \vec{b}_{k+1} + \gamma_2 \vec{b}_{k+2} + \cdots + \gamma_{(n-k+1)} \vec{b}_n \tag{13.45}$$

where $\gamma_i \in \mathbb{Z}$ for all $i = 1, \ldots, (n-k+1)$. Then, consider a non-zero vector $\vec{\delta}_3$ in the embedded lattice $L(Z)$ that is represented in the following form,

$$\begin{aligned} \vec{\delta}_3 &= \gamma' \begin{bmatrix} \vec{p} \\ 1 \end{bmatrix} - \gamma_1 \begin{bmatrix} \vec{b}_{k+1} \\ 0 \end{bmatrix} - \gamma_2 \begin{bmatrix} \vec{b}_{k+2} \\ 0 \end{bmatrix} - \cdots - \gamma_{(n-k+1)} \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix} \\ &= \gamma' \begin{bmatrix} \vec{p} \\ 1 \end{bmatrix} - \left(\gamma_1 \begin{bmatrix} \vec{b}_{k+1} \\ 0 \end{bmatrix} + \gamma_2 \begin{bmatrix} \vec{b}_{k+2} \\ 0 \end{bmatrix} + \cdots + \gamma_{(n-k+1)} \begin{bmatrix} \vec{b_n} \\ 0 \end{bmatrix} \right). \end{aligned} \tag{13.46}$$

By letting $\gamma' = 1$ and considering equation (13.45), we have

$$\vec{\delta}_3 = \begin{bmatrix} \vec{p} \\ 1 \end{bmatrix} - \begin{bmatrix} \vec{q} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{p} - \vec{q} \\ 1 \end{bmatrix}. \tag{13.47}$$

In the LeeHahn$_{GGH}$-CVP instance, we have $\vec{p} = \vec{q} + \vec{\epsilon}$ which implies that $\vec{p} - \vec{q} = \vec{\epsilon}$. Hence, we have

$$\vec{\delta}_3 = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix} \in L(Z) \tag{13.48}$$

where $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. Since $\vec{\epsilon}$ is a small vector for ensuring that the vectors $\vec{p}$ and $\vec{q}$ are located closest to each other, then the embedding attack is expecting that vector $\vec{\delta}_3$ as the shortest non-zero vector in the embedded lattice $L(Z)$. Finding for the shortest vector $\vec{\delta}_3$ in the embedded lattice $L(Z)$ is an SVP instance. That means, the embedding technique has reduced the LeeHahn$_{GGH}$-CVP instance into an SVP instance. We address the instance as the LeeHahn$_{GGH}$-SVP instance.

To solve the derived LeeHahn$_{GGH}$-SVP instance, the embedding attack uses the lattice reduction algorithm for reducing the embedded sub-basis Z. Suppose that the LLL-algorithm is used. We denote the LLL-reduced form of the basis Z as $Z_{LLL} = \{\vec{z}_1, \vec{z}_2, \ldots, \vec{z}_{n-k+1}\}$ where the first reduced basis vector $\vec{z}_1$ is the shortest vector in the reduced-basis Z_{LLL}. Therefore, the LLL-algorithm returns the shortest vector $\vec{z}_1 = \vec{\delta}_3$ as the solution of the LeeHahn$_{GGH}$-SVP instance. From the obtained solution $\vec{z}_1$, then we can easily solve the equation (13.47) for the unknown vector $\begin{bmatrix} \vec{q} \\ 0 \end{bmatrix}$ since the target vector $\vec{p}$ is known. To obtain the vector $\vec{q}$, simply compute

$$\begin{bmatrix} \vec{q} \\ 0 \end{bmatrix} = \begin{bmatrix} \vec{p} \\ 1 \end{bmatrix} - \vec{z}_1. \tag{13.49}$$

Obviously, the obtained vector $\begin{bmatrix}\vec{q}\\0\end{bmatrix}$ contains the desired lattice vector $\vec{q} \in L(B_2)$ which immediately solves the Nguyen$_{GGH}$-CVP instance. Consequently, the Lee-Hahn's attack completely decrypted the final GGH Internet Challenge in the lattice dimension of 400 which was previously failed to be reached by the Nguyen's attack.

13.4.4 Discussion

Observe that, there are several similarities between the Nguyen's and Lee-Hahn's attacks. Firstly, the entries of the new error vector in both simplified instances are randomly selected from the same set, $\left\{-\frac{1}{2}, +\frac{1}{2}\right\}$. That means, the Euclidean distance between the target vector and the desired lattice vector in both the $Nguyen_{GGH}$-CVP and LeeHahn$_{GGH}$-CVP instances are similar. As stated in [6], the Euclidean distance is now shorthened becomes $\sqrt{n}/2$ compared to its original distance $\sigma\sqrt{n}$ in the GGH-CVP instance. We provide the proof as follows,

Proposition 13.4.3. For $n \in \mathbb{N}$, let $\vec{s} \in \mathbb{R}^n$ be a target vector and $\vec{t} \in \mathcal{L} \subset \mathbb{R}^n$ be a lattice vector such that

$$\vec{s} = \vec{t} + \vec{\epsilon}$$

where $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. Then, $\|\vec{s} - \vec{t}\| = \frac{\sqrt{n}}{2}$.

Proof. Given that $\vec{s} = \vec{t} + \vec{\epsilon}$. Thus, $\vec{s} - \vec{t} = \vec{\epsilon}$. Since $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$, therefore

$$\begin{aligned}
\|\vec{s} - \vec{t}\| &= \|\epsilon\| \\
&= \sqrt{\sum_{i=1}^{n} \left(\pm\frac{1}{2}\right)_i^2} \\
&= \sqrt{\sum_{i=1}^{n} \left(\frac{1}{4}\right)_i} \\
&= \sqrt{n\left(\frac{1}{4}\right)} \\
&= \frac{\sqrt{n}}{2}.
\end{aligned}$$

□

Clearly, the Euclidean distance is shorter compared to the Euclidean distance $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$ in the GGH-CVP instance. With this shorter distance, the Nguyen$_{GGH}$-CVP and LeeHahn$_{GGH}$-CVP instances are considered simpler than the GGH-CVP instance.

Secondly, both attacks use the same strategy for breaking the security of the GGH cryptosystem. Instead of direcly solving the GGH-CVP instance in its original form, these attacks are managed to solve the simplified versions of the instance. To solve the simplified instances, both attacks also use the same strategy by executing the embedding attack. Previously, the execution of the embedding attack on the original GGH-CVP instance only managed to break the GGH cryptosystem in lattice dimensions below 150. But through the Nguyen's and Lee-Hahn's attacks, the execution of the embedding attack could break the GGH cryptosystem in the lattice dimensions up to 400.

Why does the GGH-CVP instance could be simplified? How does the Nguyen's attack as well as the Lee-Hahn's attack could improve the ability of the embedding attack for breaking the GGH cryptosystem? Why does the Lee-Hahn's attack succeeds for completely decrypting the final GGH Internet Challenge in the lattice dimension of 400 while the Nguyen's attack previously failed to do so? We address these questions in the next section.

13.5 Weaknesses of the GGH Cryptosystem

From our discussion in the Section 13.4, it can be observed that most hazardous security threat on the GGH cryptosystem is the embedding attack. Most of the earlier attempts for breaking the GGH cryptosystem as well as the GGH Internet Challenges prior the Nguyen's attack used the embedding attack. However, these attacks only managed to solve the underlying GGH-CVP instance in the lattice dimensions not more than 200. Similarly, the Nguyen's and the Lee-Hahn's attacks also executed the embedding attack in their solution stage.

But this time, the implementation of the embedding attack in the solution stages of the Nguyen's and Lee-Hahn's attacks works effectively even in the lattice dimensions beyond 200 up to 400. This is because the embedding attack is used to solve the simplified versions of the GGH-CVP instance, instead of the original GGH-CVP instance. The simplification of the GGH-CVP instance into the Nguyen$_{GGH}$-CVP and LeeHahn$_{GGH}$-CVP instances allowed the embedding attack to perform better than before. In this section, we justify the reason behind this occurence.

For that purpose, we compare the embedding attack on the GGH-CVP instance and the Nguyen$_{GGH}$-CVP instance since the embedded bases $X, Y \in \mathbb{R}^{(n+1)\times(n+1)}$, in both instances have the same dimensions. Recall that the embedded basis $X \in \mathbb{R}^{(n+1)\times(n+1)}$ in the GGH-CVP instance has the following representation,

$$X = \begin{pmatrix} \vec{c} & \vec{b_1} & \cdots & \vec{b_n} \\ 1 & 0 & \cdots & 0 \end{pmatrix} \tag{13.50}$$

where $\vec{c} \in \mathbb{R}^n$ is the ciphertext vector and $\vec{b_i} \in B$ for all $i = 1, \ldots, n$. Similarly, recall that the embedded basis $Y \in \mathbb{R}^{(n+1)\times(n+1)}$ in the Nguyen$_{GGH}$-CVP instance has the following representation,

$$Y = \begin{pmatrix} \vec{s} & \vec{b_1} & \cdots & \vec{b_n} \\ 1 & 0 & \cdots & 0 \end{pmatrix} \tag{13.51}$$

where $\vec{s} \in \mathbb{R}^n$ is the target vector and $\vec{b_i} \in B$ for all $i = 1, \ldots, n$. In the GGH-CVP instance, the expected shortest vector in the embedded lattice $L'(X)$ is the vector $\vec{\delta_1} = \begin{bmatrix} \vec{e} \\ 1 \end{bmatrix} \in L'(X)$ where $\vec{e} \in \{-\sigma, +\sigma\}^n$ while the expected shortest vector in the embedded lattice $L'(Y)$ is the vector $\vec{\delta_2} = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix} \in L'(Y)$ where $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. These vectors could be obtained by reducing the embedded bases X and Y using the LLL-algorithm and yields the LLL-reduced bases X_{LLL} and Y_{LLL} respectively. The first vectors in these LLL-reduced bases are expected to be the shortest vector in the embedded lattices $L'(X)$ and $L'(Y)$ respectively. Therefore, we have $\vec{x}_1 = \vec{\delta_1}$ and $\vec{y}_1 = \vec{\delta_2}$, where $\vec{x}_1 \in X_{LLL}$ and $\vec{y}_1 \in Y_{LLL}$.

Notice that other than their first columns, both the embedded bases X and Y are consisting the same columns $\begin{bmatrix}\vec{b}_1\\0\end{bmatrix}, \begin{bmatrix}\vec{b}_2\\0\end{bmatrix}, \cdots, \begin{bmatrix}\vec{b}_n\\0\end{bmatrix} \in \mathbb{R}^{n+1}$. This implies that, the second shortest vector in the reduced embedded bases X_{LLL} and Y_{LLL} are the same vector $\vec{x}_2 = \vec{y}_2 = \begin{bmatrix}\vec{b}_1^*\\0\end{bmatrix} = \vec{b}_1^*$, which is the shortest vector in the LLL-reduced form of the basis B. Now, we can determine the lattice gap between the embedded lattice $L'(X)$ and $L'(Y)$ as follows,

$$lattice_{gap}(L'(X)) = \frac{\lambda_2\left(L'(X)\right)}{\lambda_1\left(L'(X)\right)} = \frac{\|\vec{b}_1^*\|}{\|\vec{\delta}_1\|} \tag{13.52}$$

and

$$lattice_{gap}(L'(Y)) = \frac{\lambda_2\left(L'(Y)\right)}{\lambda_1\left(L'(Y)\right)} = \frac{\|\vec{b}_1^*\|}{\|\vec{\delta}_2\|}. \tag{13.53}$$

Since $\vec{\delta}_1 = \begin{bmatrix}\vec{e}\\1\end{bmatrix} \in L'(X)$ where $\vec{e} \in \{-\sigma, +\sigma\}^n$, then

$$\|\vec{\delta}_1\| \quad = \quad \|\vec{e}\| + \|1\|. \tag{13.54}$$

Based on Proposition 13.3.3, we have $\|\vec{e}\| = \sigma\sqrt{n}$. Thus,

$$\|\vec{\delta}_1\| \quad = \quad \sigma\sqrt{n} + 1.$$

On the other hand, we have $\vec{\delta}_2 = \begin{bmatrix}\vec{\epsilon}\\1\end{bmatrix} \in L'(Y)$ where $\vec{\epsilon} \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$, then

$$\|\vec{\delta}_2\| \quad = \quad \|\vec{\epsilon}\| + \|1\|. \tag{13.55}$$

Based on Proposition 13.4.3, we have $\|\vec{\epsilon}\| = \frac{\sqrt{n}}{2}$. Thus,

$$\|\vec{\delta}_2\| \quad = \quad \frac{\sqrt{n}}{2} + 1 = \frac{\sqrt{n}+2}{2}.$$

By considering $n \in \mathbb{N}$ and $\sigma \in \mathbb{R}$ with $\sigma \geq 1$, then we have

$$\|\vec{\delta}_2\| < \|\vec{\delta}_1\|.$$

Consequently,

$$\frac{\|\vec{b}_1^*\|}{\|\vec{\delta}_2\|} > \frac{\|\vec{b}_1^*\|}{\|\vec{\delta}_1\|}$$

$$lattice_{gap}(L'(Y)) > lattice_{gap}(L'(X)).$$

Therefore, we showed that the lattice gap in the embedded lattice $L'(Y)$ that is derived from the Nguyen$_{GGH}$-CVP instance is larger than the lattice gap in the embedded lattice $L'(X)$ that is derived from the GGH-CVP instance. That is why the lattice reduction that performed by the embedding attack on the Nguyen$_{GGH}$-CVP instance becomes easier compared to the lattice reduction that performed by the embedding attack on the GGH-CVP instance. Consequently, the embedding

attack successfully solved the Nguyen$_{GGH}$-CVP instance in the lattice dimensions of 200 up to 350 and allowing the Nguyen's attack to completely decrypt the GGH Internet Challenges in those dimensions.

Other than the lattice gap, the performance of the lattice reduction also influenced by the lattice dimension n. Recall that, the embedded lattice $L'(Y)$ that is derived in the Nguyen$_{GGH}$-SVP instance is spanned by the embedded basis $Y \in \mathbb{R}^{(n+1)\times(n+1)}$. On the other hand, the embedded lattice $L'(Z)$ that is derived in the LeeHahn$_{GGH}$-SVP instance is spanned by the embedded basis $Z \in \mathbb{R}^{(n+1)\times(n-k+1)}$. Observe that, the dimension of the embedded lattice $L'(Y)$ is $(n+1)$ while the dimension of the embedded lattice $L'(Z)$ is $(n-k+1)$. Since $n, k \in \mathbb{N}$ with $k < n$, therefore,

$$dim\left(L'(Z)\right) < dim\left(L'(Y)\right).$$

Due to this smaller lattice dimension and the simplification of the GGH-CVP instance to LeeHahn$_{GGH}$-CVP instance, then the lattice reduction algorithm for solving the LeeHahn$_{GGH}$-SVP instance could perform better than the lattice reduction algorithm for solving the Nguyen$_{GGH}$-SVP instance. That is why the Lee-Hahn's attack successfully recovered the whole plainetext $\vec{m} \in \mathbb{Z}^{400}$ of the final GGH Internet Challenge while the Nguyen's attack failed to do so.

After all, the main reason why does the Nguyen's attack as well as the Lee-Hahn's attack succeeded for breaking the GGH cryptosystem in the lattice dimensions beyond 200 while the earlier embedding attacks failed to do so is due to the simplification of the GGH-CVP instance. The simplification makes the Euclidean distance between the target vector and the desired lattice vector in the Nguyen$_{GGH}$-CVP instance as well as the LeeHahn$_{GGH}$-CVP instance shortened from $\sigma\sqrt{n}$ in the GGH-CVP instance become $\frac{\sqrt{n}}{2}$ in its simplified forms.

Consequently, the lattice gaps in the embedded lattices $L'(Y)$ and $L'(Z)$ that are derived in the Nguyen$_{GGH}$-SVP instance as well as the LeeHahn$_{GGH}$-SVP instance respectively become larger than the lattice gap in the embedded lattice $L'(X)$ that is derived in the GGH-SVP instance. The simplification becomes possible once the partial information $\vec{m}_{2\sigma}$ successfully obtained in the elimination stage of the Nguyen's attack and elimination stage becomes possible due to the simple structure of the error vector $\vec{e}$.

Reconsider the following equation as obtained in elimination stage of the Nguyen's attack,

$$\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} = \frac{\vec{e}+\vec{s}}{2\sigma}$$

where $\vec{s} = \{+\sigma\}^n$. Since the entries of the error vector $\vec{e}$ are randomly selected from the small set $\{-\sigma, +\sigma\}$, then the following fractions

$$\frac{\vec{e}+\vec{s}}{2\sigma} \in \mathbb{Z}^n$$

and

$$\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} \in \mathbb{Z}^n$$

hold and consequently make that congruence (13.21) below,

$$\vec{c}+\vec{s} \equiv B\vec{m} \pmod{2\sigma}$$

holds. Solving the congruence (13.21) for the secret vector $\vec{m}$ yields $\vec{m}_{2\sigma} = B^{-1}(\vec{c}+\vec{s})$ where $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$. The obtained vector $\vec{m}_{2\sigma}$ is the partial information that

is demanded for allowing the simplification of the GGH-CVP instance becomes possible.

Clearly, the simple structure of the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$ is the major flaw that being exploited for allowing the simplification process being happened. That means, the simple structure of the error vector $\vec{e}$ must be modified in order to prevent the vector $\vec{e}$ from being eliminated. However, this modification must be done in a proper way. By simply changing this structure, the Euclidean distance between the ciphertext $\vec{c}$ and the lattice vector $\vec{v} = B\vec{m}$ could be affected and this occurence might induces security and practicality failures. This matter will be discussed further in the next section.

13.6 Strategy to Rescue the GGH Cryptosystem

Although the Lee-Hahn's attack seems to be more powerful than the Nguyen's attack, this attack depends heavily on the Nguyen's attack. In order to perform the simplification stage in the Lee-Hahn's attack, some of the actual values from the plaintext $\vec{m} \in \mathbb{Z}^{400}$ in the final GGH Internet Challenge are required. For that purpose, the Lee-Hahn's attack uses the partially decrypted plaintext $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^{400}$ that is obtained by the Nguyen's attack. Without the partially decrypted plaintext $\vec{m}_{2\sigma}$, it is hard for the Lee-Hahn's attack to guess some of actual plaintext values and the attack could not proceed to its simplification stage. Moreover, the simplification stage of the Lee-Hahn's attack also requires the partial information $\vec{m}_{2\sigma}$ to simplify the GGH-CVP instance to the LeeHahn$_{GGH}$-CVP instance. After all, we consider the Nguyen's attack as more hazardous security threats on the GGH cryptosystem compared to the Lee-Hahn's attack. We expect that, strengthening the GGH cryptosystem against the Nguyen's attack should be sufficient for making the GGH cryptosystem surviving.

To rescue the GGH cryptosystem against the Nguyen's attack, the simplification of the GGH-CVP instance must be avoided to ensure that the instance remains in its original form. Clearly, Nguyen's attack could not proceed to its simplification stage if the elimination stage could be prevented from being happened. The obvious way to avoid the elimination stage is by replacing the set $\{-\sigma, +\sigma\}$ from which the entries of the error vector $\vec{e}$ are being selected with other set that could make the following fraction vector

$$\frac{\vec{e} + \vec{s}}{2\sigma} \notin \mathbb{Z}^n$$

holds so that the following fraction vector could be true

$$\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} \notin \mathbb{Z}^n$$

as well. This implies that,

$$\vec{c} + \vec{s} \not\equiv B\vec{m} \pmod{2\sigma}.$$

This indicates that, the partial information $\vec{m}_{2\sigma}$ could not be obtained and consequently the simplification stage could not be done. For that purpose, the set $\{-\sigma, +\sigma\}$ can be replaced by the set $\{\pm\sigma, \pm(\sigma - 1)\}$ as proposed by Nguyen [6]. However, he rejected this idea since the Euclidean distance of the target vector and the desired lattice vector in the GGH-CVP instance becomes shorter than $\sigma\sqrt{n}$. As described before, shorter distance could make lattice gap in the embedded lattice

larger and consequently makes the GGH cryptosystem insecure again. We suggest that, this strategy could be implemented only if the distance $\sigma\sqrt{n}$ could be maintained. To maintain this distance, the distribution of the entries $\pm\sigma$ and $\pm(\sigma-1)$ in the vector $\vec{e}$ should be controlled and fixed to certain numbers. The positions could be random but the numbers of $\pm\sigma$ and $\pm(\sigma-1)$ entries should be controlled so that the $\|\vec{e}\|$ is about $\sigma\sqrt{n}$.

13.7 Conclusion

In this paper, we revisited the GGH cryptosystem that we believe as one of the most promising cryptographic schemes in the post-quantum cryptography era. Bear in mind that, the original design of the GGH Cryptosystem was experimentally shown and analysed to be invulnerable to various attacks when it is implemented in a lattice dimension beyond 200. All efforts for solving the GGH Internet Challenge also failed to reach a lattice dimension beyond 200. These invulnerabilities are possible since all attacks prior the Nguyen's attack failed to solve the underlying GGH-CVP instance. Only by simplifying the instance made the Nguyen's attack succeeded for breaking the security of the GGH Cryptosystem. We are optimistic that, it is better to upgrade the security of the GGH Cryptosystem by defeating the Nguyen's attack and at the same time maintaining the security reliance of the upgraded GGH Cryptosystem on the GGH-CVP instance. If such improvement could be done, then all security features of the GGH Cryptosystem prior the Nguyen's attack could be restored. As a conclusion, there is hope, potential and opportunity for the GGH Cryptosystem to survive and return into the mainstream discussion in lattice-based cryptography. With its upgraded security, efficiency and practicality, the GGH Cryptosystem could emerges as one of the most preferable and competitive cryptographic schemes in the post-quantum cryptography era.

Acknowledgements

The present research is partially supported by the Putra-Grant–GP/2017/9552200. The corresponding author also want to acknowledge the Malaysian Ministry of Education and Universiti Malaysia Sabah for financial support.

Bibliography

[1] Shor, P. W. (1997) , *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing, 26(5), 1484–1509.

[2] Goldreich, O., Goldwasser, S. and Halevi, S. (1997), *Public-key cryptosystems from lattice reduction problems*, Kaliski Jr B. S.(Ed): Advances in Cryptology—CRYPTO'97, LNCS 1294, 112–131.

[3] Rivest, R. L., Shamir, A. and Adleman, L. (1978), *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, 21(2):120–126.

[4] ElGamal, T. (1985), *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inform. Theory, 31(4):469–472.

[5] Goldreich, O., Goldwasser, S. and Halevi, S. *Challenges for the GGH Cryptosystem*. Available at http://groups.csail.mit.edu/cis/lattice/challenge.html

[6] Nguyen P. (1999), *Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97*, Wiener M.(Ed): Advances in Cryptology— CRYPTO'99, LNCS 1666, 288-304.

[7] Lee, M. S., Hahn, S.G. (2010), *Cryptanalysis of the GGH Cryptosystem*, Math.Comput.Sci. 3, 201-208.

[8] Hoffstein, J., Pipher, J., and Silverman, J. H. (2008), *Lattices and Cryptography*, In Axler, S. and Ribet, K. A. (Eds.), An Introduction to Mathematical Cryptography. Spring Street, New York: Springer Science+Business Media, LLC, 349-422.

[9] Goodaire, E. G. (2015), *Euclidean n-Space*, In Linear Algebra: Pure and Applied. Toh Tuck Link, Singapore: World Scientific Publishing Co. Pte. Ltd., 1-83.

[10] Galbraith, S. D. (2012), *Background Mathematics*, In Mathematics of Public Key Cryptography. New York USA: Cambridge University Press, 564-578.

[11] Galbraith, S. D. (2012), *Lattices*, In Mathematics of Public Key Cryptography. New York: Cambridge University Press, 337-345.

[12] Serre, D. (2010), *Norms*, In Axler, S. and Ribet, K. A. (Eds.), Matrices: Theory and Applications 2nd ed., Heidelberg London: Springer Science+Business Media, LLC, 127-137.

[13] Lenstra, A.K., Lenstra, Jr., H.W., and Lovász, L. (1982), *Factoring polynomials with rational coefficients*, Math. Ann., 261(4), 515–534.

[14] Goldreich, O., Micciancio, D., Safra, S. and Seifert, J.-P. (1999), *Approximating shortest lattice vectors is not harder than approximating closet lattice vectors*, Inf. Process. Lett., 71(2), 55-61.

[15] Schnorr, C-P., Fischlin, M., Koy, H. and May, A. (1997), *Lattice attacks on GGH Cryptosystem. Rump session of Crypto '97.*

[16] Schnorr C.P. and Hörner, H.H. (1995), *Attacking the Chor-Rivest cryptosystem by improved lattice reduction*, Proc. of Eurocrypt'95, LNCS 921, 1-12.

[17] Shoup, V. *Number Theory C++ Library (NTL) version 3.6*, can be obtained at http://www.shoup.net/ntl/.

[18] Mandangan A, Kamarulhaili H and Asbullah MA. (2018), *On the Underlying Hard Lattice Problems of GGH Encryption Scheme*, In Proceedings of the Cryptology and Information Security Conference (CRYPTOLOGY2018), 42-50.

[19] Hoffstein, J., Pipher, J., and Silverman, J.H. (1998), *NTRU: a ring based public key cryptosystem*, Proc. of ANTS-III, LNCS 1423, 267– 288.

[20] Regev, O. (2005), *On lattices, learning with errors, random linear codes, and cryptography*, Proc. 37th ACM Symp. on Theory of Computing (STOC), 84–93.

[21] Lyubashevsky, V., Peikert, C. and Regev, O. (2013), *On ideal lattices and learning with errors over rings*,Journal of the ACM (JACM), 60(6):43

[22] Babai, L. (1986), *On Lovász' lattice reduction and the nearest lattice point problem*, Combinatorica, 6(1), 1-13.

[23] Micciancio, D. (2001), *Improving lattice-based cryptosystems using the hermite normal form*, In Silverman ,J. (Ed), Cryptography and Lattices Conference — CaLC 2001, LNCS 2146, 126–145.

[24] Micciancio, D. and Regev, O. (2009), *Lattice-based cryptography*, In Bernstein, D. J., Buchmann, J., and Dahmen, E. (Eds), Post-Quantum Cryptography, Springer Berlin Heidelberg, 147–191.

Chapter 14

Variable Order Step Size Algorithm for Solving Second Order ODEs

Ahmad Fadly Nurullah Rasedee[1,*], Mohamad Hassan Abdul Sathar[2], Wong Tze Jin[3], Koo Lee Feng[3]

[1] Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, 78100 Nilai, Negeri Sembilan, Malaysia.
[2] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Department of Basic Sciences and Engineering, Faculty of Agriculture and Food Science, Universiti Putra Malaysia, Bintulu Campus, 97008 Bintulu, Sarawak, Malaysia.

*Corresponding author: fadlynurullah@usim.edu.my

Abstract

Previous multi step method using a divided difference formulation for solving higher order ordinary differential equations (ODEs) requires calculating the integration coefficients at every step. In the current research, a multi step method in backwards difference form is established. The backward difference formulation offers a solution to the tedious calculation of integration coefficients. Rather than calculating integration coefficients at every step change, a backward difference formulation requires calculating integration coefficients only once in the beginning and if required once more at the end. The proposed method will also be equipped with a variable order step size algorithm to reduce computational cost (calculation time). Both linear and nonlinear second order ODEs will used to validate the accuracy and efficiency of the proposed method.

Keywords: ODE, backward difference, multistep method.

14.1 Introduction

Various of science and engineering problems are found in the form of higher order Ordinary Differential Equations (ODEs). A few examples where these problems can be found are, in the motion of projectiles, the bending of a thin clamped beam and growth population. Previously, it was common practice to solve these higher order ODEs by reducing them to a system of first order equations. These methods worked, so that methods for solving higher order ODEs were disregarded as robust

codes. In this research, an efficient algorithm for solving higher order, or in the current case second order ODEs with Initial Value Conditions (IVCs) directly using variable order step size method in backward difference formulation is developed. The advantages of solving second order systems directly compared to reducing it to first order systems will be apparent.

The approach for solving ODEs using multistep methods was made popular by authors such as [1–4]. Beginning from reduction to first order method to the current method of solving higher order ODEs directly. Suleiman in [4] initially proposed solving higher order ODEs using a divided difference multistep method. This lead to the current interest of using multistep methods for solving higher ODEs directly. Suleiman [4] designed a multistep code for solving stiff and nonstiff higher order ODEs directly without the need for reducing the problems to first order. This method was regarded as the Direct Integration (DI) method. The drawback of the proposed DI method was the tedious calculations of the divided differences in computing integration coefficients at every step change. Current research influenced by the works of [4] includes research by authors such as [5], [6, 7], [8–10], [11, 12] and [13–16].

In the current research, a multistep method based on backward difference formulation in predictor-corrector mode is established with variable order step size capability. The derivation of the proposed method begins as follow.

14.2 Derivation of The Predictor-Corrector Formulation

First consider the second order ordinary differential equation (ODE) in the general form

$$y'' = f(x, y, y'), \tag{14.1}$$

with $\widetilde{Y}(\alpha) = \widetilde{\eta}$ as the initial solution in the interval $\alpha \leq x \leq \beta$, and the initial value conditions are given by

$$\widetilde{Y}(x) = (x, y, y'), \qquad \widetilde{\eta} = (\eta, \eta'). \tag{14.2}$$

In order to obtain the predictor, the explicit integration coefficients need to be established.

14.2.1 Explicit Coefficients

For the evaluation of the explicit integration coefficients, y_{n+1} consider the second order ODE in (14.1). The derivation begins by integrating equation (14.1), once as follows

$$\int_{x_n}^{x_{n+1}} y''(x_{n+1})dx = \int_{x_n}^{x_{n+1}} f(x, y, y')dx. \tag{14.3}$$

This yields

$$y'(x_{n+1}) = y'(x_n) + \int_{x_n}^{x_{n+1}} f(x, y, y')dx. \tag{14.4}$$

Next, $f(y, y')$ is interpolated by the Newton-Gregory backward difference polynomial, $P_n(x)$

$$P_n(x) = \sum_{i=0}^{k-1} (-1)^i \begin{pmatrix} -s \\ i \end{pmatrix} \nabla^i f_n, \qquad s = \frac{x - x_n}{h}. \tag{14.5}$$

and substituting $dx = hds$ changes the limit of integration, thus giving

$$y'(x_{n+1}) = y'(x_n) + \int_0^1 \sum_{i=0}^{k-1} (-1)^i \begin{pmatrix} -s \\ i \end{pmatrix} \nabla^i f_n \, hds. \tag{14.6}$$

By denoting, $\gamma_{1,i}$ by

$$\gamma_{1,i} = (-1)^i \int_0^1 \begin{pmatrix} -s \\ i \end{pmatrix} ds.$$

and substituting $\gamma_{1,i}$ into equation (14.6) yields

$$y'(x_{n+1}) = y'(x_n) + h \sum_{i=0}^{k-1} \gamma_{1,i} \nabla^i f_n \, ds, \tag{14.7}$$

This is followed by defining the generating function, $G_1(t)$ of the coefficients $\gamma_{1,i}$ as

$$G_1(t) = \sum_{i=0}^{\infty} \gamma_{1,i} t^i. \tag{14.8}$$

Then by substituting $\gamma_{1,i}$ in the generating function as defined in (14.8) and solving the integral gives

$$G_1(t) = -\left[\frac{(1-t)^{-1}}{\log(1-t)} - \frac{1}{\log(1-t)} \right]. \tag{14.9}$$

The 2^{nd} order generating function, $G_2(t)$ is obtained by integrating equation (14.1) twice, followed by repeating steps from equation (14.3) to (14.8), hence

$$G_2(t) = \left[\frac{1}{\log(1-t)} - \frac{-1}{\log(1-t)} \left[\frac{(1-t)^{-1}}{\log(1-t)} - \frac{1}{\log(1-t)} \right] \right]. \tag{14.10}$$

The generating function, $G_2(t)$ then can be rewritten in terms of $G_1(t)$

$$G_2(t) = \left[\frac{1}{\log(1-t)} - \frac{G_1(t)}{\log(1-t)} \right].$$

14.2.2 Implicit Coefficients

The implicit integration coefficients can be obtained in a similar manner as the explicit coefficients with some subtle differences. As the prior, the derivation of the implicit coefficients also begins with equation (14.3). Again, using the Newton-Gregory backward difference polynomial to interpolate, $f(y, y')$ with the difference of substituting

$$s = \frac{x - x_{n+1}}{h},$$

thus, resulting in

$$y'(x_{n+1}) = y'(x_n) + \int_{-1}^{0} \sum_{i=0}^{k-1} (-1)^i \begin{pmatrix} -s \\ i \end{pmatrix} \nabla^i f_n \, h ds. \tag{14.11}$$

Now, denote $\gamma^*_{1,i}$ by

$$\gamma^*_{1,i} = (-1)^i \int_{-1}^{0} \begin{pmatrix} -s \\ i \end{pmatrix} ds$$

which gives

$$y'(x_{n+1}) = y'(x_n) + h \sum_{i=0}^{k-1} \gamma^*_{1,i} \nabla^i f_n \, ds, \tag{14.12}$$

The implicit generating function, $G^*_1(t)$ can be mathematically deduced as the following formulation

$$G^*_1(t) = -\left[\frac{1-(1-t)}{\log(1-t)}\right] \tag{14.13}$$

which can be generalized as

$$G^*_{(d)}(t) = \frac{(1-t)}{(d-1)!}\left[\frac{1}{\log(1-t)} - \frac{(d-1)! G^*_{(d-1)}(t)}{\log(1-t)}\right] \qquad d = 1, 2. \tag{14.14}$$

Calculation of the explicit and implicit coefficients directly involving large numbers of integration can be tedious and time consuming. To overcome this drawback, a recurrence relationship between integration coefficients is provided. This enables for a more efficient code when programming the algorithm. The recurrence relationship can expressed as follows

$$G^*_{(d)}(t) = (1-t) G_{(d)}(t), \qquad d = 1, 2. \tag{14.15}$$

From the generating function, its corresponding integration coefficients is represented as

$$\sum_{i=0}^{k} \gamma^*_{(d),i} = \gamma_{(d),k} \tag{14.16}$$

14.3 Order and step size criteria

The order and step size selection of a variable order step size algorithm is based on its acceptance criteria. This acceptance criteria will determine whether to increase the order and step size. When handling a variable order step size algorithm, determining the success of an integration step is crucial. The threshold for each integration step is predetermined by setting an acceptable tolerance level (TOL). The success of an integration step depends on whether the estimated error, $|E_k^{(d-p)}|$ satisfies the following local accuracy requirements

$$\text{TOL} > \frac{|E_k^{(d-p)}|}{A + B + P_n} \tag{14.17}$$

where A and B determines the type of error test used. Hence, every estimated error that satisfies the local accuracy condition also fulfills the acceptance criteria.

The variable order in a multistep method relies on the back values stored. The order may be increased if back values from the previous step are retained and may be decreased simply by relinquishing the appropriate amount of back values. The order strategies adopted here are similar to strategies proposed in [2].

When implementing a variable step size algorithm, Shampine and Gordon suggests restrictions on ratio of successive step size due to convergence and stability issues of variable step size techniques to ensure stability. Because the proposed method is based on the Adams-Bashforth formulation as predictor and Adams-Moulton formulation as corrector (PECE mode), we adopt the doubling or halving the step size algorithm from [1] which is implements a step size changing technique from [17].

14.4 Numerical Results

The tables and figures below show the numerical results for Problems 1 to 3 which were solved using Direct Integration and Backwards Difference method directly. Numerical result for methods that reduces second order ODES to first order systems are also included as a benchmark. In this section, numerical result includes the evaluation of maximum and average values of the error in the computed solution y. The efficiency of the 1PBD will be validated by comparing results of obtain by Suleiman's DI method.

Following are abbreviation used in this section
TOL: Tolerance level
MTHD: Method
TS: Total steps
FS: Fail steps
MAX: Maximum error (exponent of 10)
AVE: Average error (exponent of 10)
TIME: Execution time in micro seconds
D1: Reduction to first order divided difference method
D1: Reduction to first order backward difference method
DI: Direct Integration method
1PBD: 1 Point Backward Difference method
TTS: Truncated Taylor Series
RTA: Rational Approximation

Problem 1:(source: Suleiman [18])

$$y_1''(x) = -\frac{y_1}{r^3}, \quad , y_2''(x) = -\frac{y_2}{r^3}, \quad r = \left(y_1^2 + y_2^2\right)^{\frac{1}{2}} \quad 0 \le x \le 16\pi.$$

Initial condition

$$y_1(0) = 1 \quad y_1'(0) = 0, \quad y_2(0) = 0, \quad y_2'(0) = 1.$$

Exact Solution

$$y_1(x) = \cos x, \quad y_2(x) = \sin x.$$

Problem 2:(source: Rasedee [19])

$$y''(t) = 2y^3(t) + ty(t) + \mu, \quad 0 \leq x \leq 5$$

Initial condition

$$y\,(0) = 1, \quad y'\,(0) = 0.$$

Exact Solution

$$unknown$$

Problem 3:(source: Rasedee [20])

$$y''(x) + y(x) + y'(x) + y^2(x)y'(x) = 2\cos x - \cos^3 x, \quad 0 \leq x \leq 100$$

Initial condition

$$y(0) = 0, \quad y'(0) = 1,$$

Exact Solution

$$y(x) = \sin x$$

Table 1 and 3 displays numerical results for problem 1 and 3. The results displayed compares steps taken, accuracy and computational cost between the D1, B1, DI and 1PBD method. The D1 and B1 method are the traditional reduction to first order method, where as the DI and 1PBD method are direct solution methods. Reduction to first order methods are used as benchmarks to validate the viability of the direct method. Table 2 on the other hand, provide approximation of a problem without any known solution. In this table, the accuracy of the 1PBD method is test against more established methods.

Numerical result shown in Table 1 are results for nonlinear second order ODE with periodic solution (two body problem). Result shows the superiority of the 1PBD method in terms of accuracy and computational cost and its competitiveness in steps taken, especially at tolerance 10^{-10} where the difference in steps required is more than 100 compared to its nearest rival.

Table 14.1: Numerical results of D1, B1, DI and 1PBD method for problem 1.

TOL	MTHD	TS	FS	MAX	AVE	TIME
10^{-2}	D1	113	5	8.80309(-2)	1.19400(-1)	2078
	B1	89	3	2.07488(-1)	6.87734(-2)	1628
	DI	76	1	8.78700(-2)	2.56159(-2)	969
	1PBD	71	0	1.17774(-1)	1.70700(-2)	969
10^{-4}	D1	151	2	4.30130(-3)	5.45887(-3)	3024
	B1	170	1	5.37539(-4)	1.06165(-4)	3169
	DI	94	1	4.25614(-3)	1.53472(-3)	1284
	1PBD	149	0	5.05592(-6)	1.21782(-3)	1951
10^{-6}	D1	275	3	1.80685(-6)	1.81711(-6)	5227
	B1	121	0	1.38184(-5)	2.65555(-6)	4077
	DI	179	1	3.15166(-4)	1.29162(-4)	2294
	1PBD	176	0	5.88468(-6)	2.26518(-6)	2272
10^{-8}	D1	348	2	3.49871(-8)	2.75009(-8)	6310
	B1	424	2	4.59227(-7)	1.19307(-7)	5367
	DI	205	0	6.69118(-5)	2.76364(-5)	8665
	1PBD	209	0	6.96499(-8)	2.35911(-8)	2664
10^{-10}	D1	526	9	3.45300(-9)	2.61398(-9)	9866
	B1	475	10	7.88269(-9)	1.39352(-9)	8822
	DI	370	0	1.44822(-7)	5.81042(-8)	4639
	1PBD	248	0	4.13390(-9)	8.63144(-10)	3109

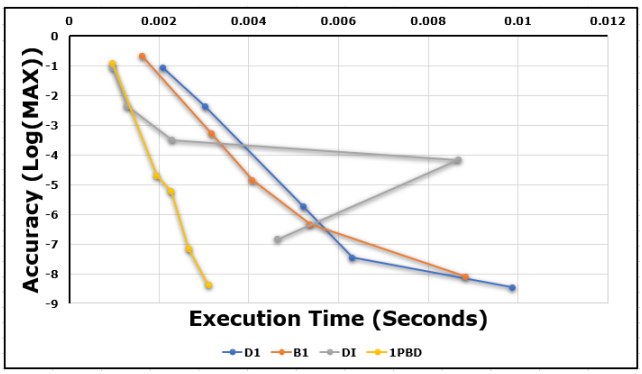

Figure 14.1: Efficiency of D1, B1, DI and 1PBD method for problem 1.

Table 2 contains results for a Riccatti type second order ODE without any exact solution. This problem was selected because of its level of difficulty. The 1PBD method is then compared against TTS ([21]) and RTA ([22]) methods which accuracy has been established for solving second order ODEs. Results in the current table reflects the accuracy of the proposed 1PBD method. The accuracy of the 1PBD increases when using smaller tolerances, to the point of matching accuracy provided by the TTS and RTA methods.

Table 3 provide results of approximated solution for Problem 3. Problem 3 is a Duffing type second order ODE and was selected for this research to test real life application problems. The selected problem has similar features with oscillatory problems with damping force. Numerical results provided in Table 3 shows the advantage of the 1PBD method in terms of accuracy and total step size over its counterpart, the DI method. The 1PBD out performs the DI method in least number of steps required at every tolerance. In terms of accuracy, the 1PBD method shows to be superior at almost every tolerance level with the exception of TOL= 10^{-2}.

Table 14.2: Comparison of accuracy for problem 2.

t	1PBD			TTS	RTA
	TOL$= 1 \times 10^{-2}$	TOL$= 1 \times 10^{-5}$	TOL$= 1 \times 10^{-10}$		
0.0	1.00000(0)	1.00000(0)	1.00000(0)	1.00000(0)	1.00000(0)
0.2	1.07160(0)	1.06262(0)	1.06261(0)	1.06260(0)	1.06260(0)
0.4	1.27252(0)	1.27417(0)	1.27415(0)	1.27420(0)	1.27420(0)
0.6	1.72688(0)	1.72542(0)	1.72538(0)	1.72540(0)	1.72540(0)
0.8	2.80714(0)	2.73708(0)	2.73694(0)	2.73690(0)	2.73690(0)
1.0	6.89972(0)	6.31186(0)	6.31100(0)	6.31100(0)	6.31040(0)

Table 14.3: Comparison of total steps and accuracy for problem 3.

TOL	MTD	STEPS	MAXE	AVER
10^{-2}	DI	254	8.49079(-2)	2.04794(-2)
	1PBD	217	1.07600(-1)	3.03894(-2)
10^{-4}	DI	332	1.54704(-3)	4.72630(-4)
	1PBD	284	1.24649(-3)	1.92899(-4)
10^{-6}	DI	382	4.24089(-5)	1.56849(-5)
	1PBD	330	1.28039(-5)	3.26641(-6)
10^{-8}	DI	651	7.93605(-7)	1.55130(-7)
	1PBD	499	7.27324(-7)	1.46368(-7)
10^{-10}	DI	772	7.83863(-9)	2.03721(-9)
	1PBD	702	9.05773(-9)	1.01381(-9)

Figure 1 illustrates the efficiency of the D1, B1, DI and 1PBD method where as, Figure 2 provides a clear comparison of efficiency between the DI and 1PBD method. Efficiency of the methods is adopted from definition in [16], where the efficiency is illustrated by undermost curve of the provided graphs. The efficiency of the proposed method is clearly presented in both figures where the 1PBD method is the under most curve of all four methods.

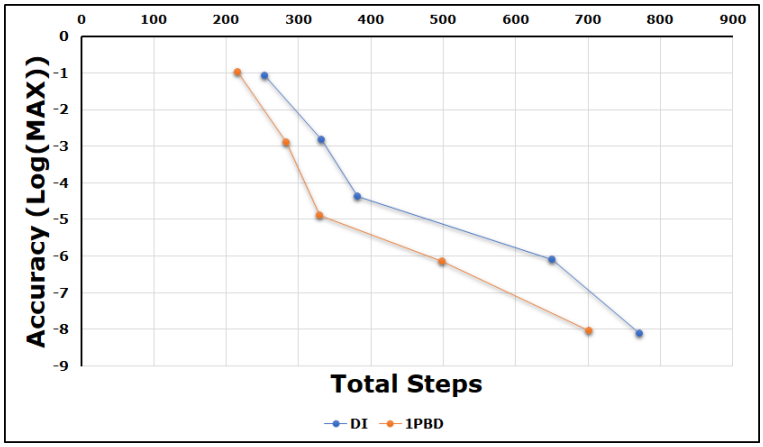

Figure 14.2: Efficiency of DI and 1PBD method for problem 3.

14.5 Conclusion

By justifications above, the 1PBD method proves to be a viable option for solving second order ODEs.

Acknowledgment

The research conducted in this article has been supported by Ministry of Education (MoE) and Universiti Sains Islam Malaysia (USIM) under the Fundamental Research Grant Scheme (FRGS), project number USIM/FRGS/FEM/055002/51517 and Universiti Putra Malaysia under Grant Putra (GP), project number GP-IPM/2017/9589600.

Bibliography

[1] Krogh, F. T. (1973), *Algorithms for changing the step size*, SIAM Journal on Numerical Analysis, Vol 10(5), 949–965.

[2] Shampine, L. F. and Gordon M. K. (1975), *Local error and variable order Adams codes*, Applied Mathematics and Computation, Vol 1(1), 47–66.

[3] Hall, G. and Suleiman, M. (1981), *Stability of Adams-Type Formulae for Second-Order Ordinary Differential Equations*, IMA Journal of Numerical Analysis, Vol 1(4), 427–438.

[4] Suleiman, M. B. (1989), *Solving nonstiff higher order ODEs directly by the direct integration method*, Applied Mathematics and Computation, Vol 33(3) 197–219.

[5] Majid, Z. A. and Suleiman, M. (2007), *Two point fully implicit block direct integration variable step method for solving higher order system of ordinary differential equations*, World Congress on Engineering, 812–815.

[6] Mohd Ijam, H., Suleiman, M., Rasedee, A. F. N., Senu, N., Ahmadian, A. and Salahshour, S. (2014), *Solving nonstiff higher-order ordinary differential equations using 2-point block method directly*, Abstract and Applied Analysis, Vol 2014, Article ID 867095, 13 pages.

[7] Mohd Ijam, H., Ibrahim, Z. B., Senu, N., Suleiman, M. and Rasedee, A. F. N. (2018), *Order and stability of 2-point block backward difference method*, AIP Conference Proceedings, Vol 1974(1), 020054.

[8] Waeleh, N., Abdul Majid, Z., Ismail, F. and Suleiman, M. (2012), *Numerical Solution of Higher Order Ordinary Differential Equations by Direct Block Code*, Journal of Mathematics and Statistics, Vol 8(1), 77-81.

[9] Waeleh, N. and Abdul Majid, Z. (2016), *A 4-Point Block Method for Solving Higher Order Ordinary Differential Equations Directly*, Mathematical Problems in Engineering, Vol 2016, Article ID 9823147, 8 pages.

[10] Waeleh, N. and Abdul Majid, Z. (2017), *Numerical Algorithm of Block Method for General Second Order ODEs using Variable Step Size*, Malaysiana, Vol 46(5), 817-824.

[11] Alkasassbeh, M. and Omar, Z. (2015), *hybrid one step block method for the solution of fourth order initial value problems of ordinary differential equations*, International Journal of Pure and Applied Mathematics, Vol 104(2), 159-169.

[12] Alkasassbeh, M. and Omar, Z. (2018), *hybrid one-step block fourth derivative method for the direct solution of third order initial value problems of ordinary differential equations*, International Journal of Pure and Applied Mathematics, Vol 119(1), 207-224.

[13] Rasedee, A. F.N. (2009), *Direct method using backward difference for solving higher order ordinary differential equations*, Selangor: University Putra of Malaysia.

[14] Rasedee, A. F. N., Suleiman, M. B and Ibrahim, Z. B. (2014), *Solving nonstiff higher order odes using variable order step size backward difference directly*, Mathematical Problems in Engineering, Vol 2014, Article ID 565137, 10 pages.

[15] Rasedee, A. F. N., Abdul Sathar, M. H., Deraman, F., Mohd Ijam, H., Suleiman, M., Saaludin, N., and Rakhimov, A. (2016), *2 point block backward difference method for solving Riccati type differential problems*, AIP Conference Proceedings, Vol 1775(1), 030005.

[16] Rasedee, A. F. N., Abdul Sathar, M. H., Ishak, N., Kamarudin, N. S., Nazri, M. A., Ramli, N. A., Ismail, I. and Sahrim, M. (2017), *Solution for nonlinear Duffing oscillator using variable order variable stepsize block method*, Matematika, Vol 33(2): 165–176.

[17] Lambert, J.D. (1973), *Computational Methods in Ordinary Differential Equations*, Wiley, New York.

[18] Suleiman, M. B., Ibrahim, Z. B. and Rasedee, A. F. N. (2011), *Solution of higher-order ODEs using backward difference method*, Mathematical Problems in Engineering, Vol 2011, Article ID 810324, 18 pages.

[19] Rasedee, A. F. N., Ishak, N., Hamzah, S. R., Mohd Ijam, H., Suleiman, M., Ibrahim, Z. B., Abdul Sathar, Ramli, N. A. and Kamarudin, N. S.(2017), *Solution for nonlinear riccati equation by block method*, Variable order variable stepsize algorithm for solving nonlinear Duffing Oscillator. *Journal of Physics: Conference Series*. Vol 890(1): 012045.

[20] Rasedee, A. F. N., Ijam, H. M., Abdul Sathar, M. H., Ishak, N., Hamzah, S. R., Sahrim, M., and Ismail,I. (2018), *Solution for nonlinear riccati equation by block method*, *AIP Conference Proceedings*. Vol 1974(1), 020071.

[21] Simon, W. E. (1965), *Numerical Technique for Solution and Error Estimate for the Initial Value Problem*, Mathematics of Computation, Vol 19(91): 387–393.

[22] Fair, W. and Luke, Y. L. (1966), *Rational approximations to the solution of the second order Riccati equation*, Mathematics of Computation, Vol 20(96): 602–606.

Chapter 15

Second Order Slip Effect on Boundary Layer Flow of Carbon Nanotubes over a Moving Plate with Stability Analysis

Nur Syazana Anuar[1], **Norfifah Bachok**[1,2,*], Norihan Md Arifin[1,2], Haliza Rosali[1]

[1] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: norfifah@upm.edu.my

Abstract

The study of boundary layer flow of water based nanofluids containing single (SWCNTs) and multi-walled (MWCNTs) carbon nanotubes past a moving plate is investigated with the effect of second order slip flow. After initiating the appropriate similarity variables, the resulting nonlinear ordinary differential equations are obtained. The system of equation is computed numerically using the bvp4c solver from Matlab. Influences of the selected values of parameters involved in the governing equations such as first and second order slip parameter, velocity ratio parameter and nanoparticle volume fraction parameter on the velocity, temperature, skin friction coefficient and local Nusselt number are explained graphically. It is revealed that for a certain range of the velocity ratio parameter i.e., the plate moves in opposite direction, dual solutions exist. Existence of slip parameter also increase the range of solution and heat transfer rate, whereas the skin friction decreased. We found that SWCNTs have a greater impact in heat transfer rate than MWCNTs. A stability analysis is executed to verify which solution is linearly stable and its physical properties could be realizable.

Keywords: Carbon nanotube, Moving plate, Second order slip, Stability analysis.

15.1 Introduction

Conventional heat transfer fluids limit the performance of the heat exchangers used in automobiles due to the poor heat transfer properties. It is essential to improve the cooling capabilities by using the technology of nanofluids. Nanotechnology have a great contribution to thermal science engineering by suspending particles with

nanometer-sized into base fluids and thus it helps in improving the thermal characteristics, thereby increase the heat transfer coefficient. In 1991, Iijima [1] discovered a thin needle-like tube during electron microscopy observation and it is proved to have a graphite structure which known as carbon nanotubes (CNTs) composed of multi-wall tubes. Later, Iijima and Ichihashi [2] found a single-wall carbon nanotubes on 1993. Carbon nanotubes have numerous applications including cooling, electrical conductivity, biomedical and many more. Therefore, many researchers tend to focus their research on CNTs due to its excellent thermal conductivity and mechanical properties [3–5]. Xue [6] presented the new model of effective thermal conductivity of CNTs-based composites by considering its orientation distribution. This model has been used by many researchers in their work [7–13].

The study of the flow caused by continuous flat surface has many practical applications, for instance the material handling conveyer, aerodynamic extrusion of plastic sheet, insulating materials, fine-faber matts and many more. Sakiadis [14] was the one who investigated theoretically the flow through an otherwise quiescent fluid on the moving surface. A considerable amount of work on moving plate has been reported in review papers [15–20] The pioneering work on nanofluid over a moving plate has been studied by Bachok et al. [21] and reported that non-unique solution exists in the case when the plate does not moves in the same manner with the free stream. It should be noted that the same research results are obtain by considering different effects [22]. Weidman et al. [13] performed the stability of flow and conclude that first upper branch solution is stable and the second lower branch solution is not stable. Afterwards, Najib et al. [24] and Jahan et al. [25] implement the stability analysis in their research on moving surface of nanofluid.

In the last few years, the slip flow has taken into consideration because of there are plenty applications where we cannot ignore the slip condition. Therefore, Wu [26] come up with a new formulation for the second-order slip model. Later on, many authors applied Wu's model in their work [27–29][29–31]. The research done by Rosca and Pop [30, 31] and Soid et al. [32] shows that duality exist for shrinking surface with the effect of second order slip. Most recently, the stability of flow considering second order slip was reported by Yasin et al. [33] and Najib et al. [34]. In carbon nanotubes, all these kind of flow and heat transfer issues were not considered yet.

The main idea of this research is to continue the work of Bachok et al. [21] with second order slip immersed in single-wall and multi-wall carbon nanotubes. We believe that there is no research done for this flow in carbon nanotubes. The results obtained are original and interesting for nanotechnology application.

15.2 Methodology

15.2.1 Mathematical Formulation

An incompressible boundary layer flow of carbon nanotubes past a moving plate with second order slip effects is investigated. The plate is considered to move along the $x-$axis with constant velocity U_w in opposite or same ways to the free stream velocity U_∞, while $y-$axis is perpendicular to the plate. The corresponding equations of boundary layer flow can be presented as [21, 35]

$$u_x + v_y = 0, \tag{15.1}$$

$$uu_x + vu_y = \frac{\mu_{nf}}{\rho_{nf}} u_{yy}, \tag{15.2}$$

$$uT_x + vT_y = \frac{k_{nf}}{(\rho C_p)_{nf}} T_{yy}, \tag{15.3}$$

along with the appropriate boundary conditions

$$\begin{aligned} &u = U_w + L_1 u_y + L_2 u_{yy}, \quad v = v_w, \quad T = T_w \quad \text{at} \quad y = 0, \\ &u \to U_\infty, \quad T \to T_\infty \quad \text{as} \quad y \to \infty, \end{aligned} \tag{15.4}$$

where the velocity components in x and y direction are (u, v), L_1 and L_2 are the slip factor, which are given by

$$L_1 = L(Re_w + Re_\infty)^{1/2} \quad \text{and} \quad L_2 = L(Re_w + Re_\infty), \tag{15.5}$$

where L is the initial value of slip factor, $Re_w = U_w x/\nu_f$ and $Re_\infty = U_\infty x/\nu_f$ are the Reynolds number depends on the plate velocity and free stream, respectively, where ν_f is the kinematic viscosity of the fluid. μ_{nf}, α_{nf} and ρ_{nf} are the viscosity, thermal diffusivity and density of the nanofluids which are given by [17]:

$$\begin{aligned} &\mu_{nf} = \frac{\mu_f}{(1-\varphi)^{2.5}}, \quad \frac{k_{nf}}{k_f} = \frac{1 - \varphi + 2\varphi \dfrac{k_{cnt}}{k_{cnt} - k_f} \ln \dfrac{k_{cnt} + k_f}{2k_f}}{1 - \varphi + 2\varphi \dfrac{k_f}{k_{cnt} - k_f} \ln \dfrac{k_{cnt} + k_f}{2k_f}}, \\ &\rho_{nf} = (1-\varphi)\rho_f + \varphi \rho_{cnt}, \quad (\rho C_p)_{nf} = (1-\varphi)(\rho C_p)_f + \varphi (\rho C_p)_{cnt}. \end{aligned} \tag{15.6}$$

Here, μ is the viscosity,k is the thermal conductivity, (ρC_p) is the heat capacity, ρ is the density while φ is the nanoparticle volume fraction where the subscript cnt, nf and f refer to carbon nanotube, nanofluid and fluid, respectively. We employed the term for thermal conductivity from Xue [6] where the model considered the impact of CNT's space distribution based on Maxwell theory.

Following the similarity transformation approach, the new variables are introduced:

$$\eta = \left(\frac{U}{\nu_f x}\right)^{\frac{1}{2}} y, \quad \psi = (\nu_f x U)^{\frac{1}{2}} f(\eta), \quad T = (T_w - T_\infty)\theta(\eta) + T_\infty, \tag{15.7}$$

where η is the similarity variable, $\theta(\eta)$ is the dimensionless temperature, $U = U_w + U_\infty$ is the composite velocity [39] and the stream function ψ is introduced as $u = \partial\psi/\partial y$ and $v = -\partial\psi/\partial x$. Using (15.7), equation (15.1) is satisfied.

We considered $v_w = -\dfrac{1}{2}\left(\dfrac{\nu_f U}{x}\right)^{1/2} s$, where $s > 0$ represents suction, $s < 0$ represents injection and $s = 0$ for impermeable surface. Using the variables defined by equation (15.7), equations (15.1)–(15.3) may be rewritten as:

$$\frac{1}{(1-\varphi)^{2.5}(1 - \varphi + \varphi\rho_{cnt}/\rho_f)} f''' + \frac{1}{2} f f'' = 0, \tag{15.8}$$

$$\frac{1}{\Pr} \frac{k_{nf}/k_f}{(1 - \varphi + \varphi(\rho C_p)_{cnt}/(\rho C_p)_f)} \theta'' + \frac{1}{2} f \theta' = 0, \tag{15.9}$$

the boundary conditions now take the following forms:

$$f(0) = s, \quad f'(0) = \lambda + \sigma f''(0) + \delta f'''(0), \quad \theta(0) = 1, \tag{15.10}$$

$$f'(\eta) \to 1-\lambda, \quad \theta(\eta) \to 0, \quad \text{as} \quad \eta \to \infty,$$

where prime refers to differentiation with respect to η. Meanwhile, $\Pr, \lambda, \sigma$ and δ are the Prandtl number, velocity parameter, first order slip and second order slip, respectively. These parameters are declared as follows:

$$\Pr = \frac{\nu_f}{\alpha_f}, \quad \lambda = \frac{U_w}{U}, \quad \sigma = L\frac{U}{\nu_f}, \quad \delta = L\left(\frac{U}{\nu_f}\right)^2. \tag{15.11}$$

The skin frictions coefficient C_f and local Nusselt number Nu_x are given by:

$$C_f = \frac{\tau_w}{\rho_f U^2}, \quad Nu_x = \frac{xq_w}{k_f(T_w - T_\infty)}, \tag{15.12}$$

with τ_w and q_w are the surface shear stress and local heat flux which are defined as:

$$\tau_w = \mu_{nf}\left(\frac{\partial u}{\partial y}\right)_{y=0}, \quad -k_{nf}\left(\frac{\partial T}{\partial y}\right)_{y=0}, \tag{15.13}$$

using equation (15.7) and (15.13) into (15.12), we obtain:

$$C_f Re_x^{1/2} = \frac{1}{(1-\varphi)^{2.5}} f''(0), \quad Nu_x Re_x^{-1/2} = -\frac{k_{nf}}{k_f}\theta'(0), \tag{15.14}$$

where $Re_x = Ux/\nu_f$ is the local Reynolds number.

15.2.2 Stability Analysis

We need to consider the unsteady state of our governing model in order to conduct the stability of the solution for the current problem. The unsteady governing equations can be written as follows:

$$u_t + uu_x + vu_y = \frac{\mu_{nf}}{\rho_{nf}} u_{yy}, \tag{15.15}$$

$$T_t + uT_x + vT_y = \frac{k_{nf}}{(\rho C_p)_{nf}} T_{yy}. \tag{15.16}$$

The new dimensionless similarity variables and time variable τ are introduced, hence equation (15.7) can be replaced by:

$$\eta = \left(\frac{U}{\nu_f x}\right)^{\frac{1}{2}} y, \quad \psi = (\nu_f x U)^{\frac{1}{2}} f(\eta, \tau), \tag{15.17}$$
$$T = (T_w - T_\infty)\theta(\eta, \tau) + T_\infty, \quad \tau = \frac{U}{x}t,$$

the governing equations (15.15) and (15.16) become

$$\begin{aligned} &\frac{1}{(1-\varphi)^{2.5}(1-\varphi+\varphi\rho_{cnt}/\rho_f)}\frac{\partial^3 f}{\partial \eta^3} + \frac{1}{2} f \frac{\partial^2 f}{\partial \eta^2} \\ &+ \tau\left(\frac{\partial f}{\partial \eta}\frac{\partial^2 f}{\partial \eta \partial \tau} - \frac{\partial f}{\partial \tau}\frac{\partial^2 f}{\partial \eta^2}\right) - \frac{\partial^2 f}{\partial \eta \partial \tau} = 0, \\ &\frac{1}{\Pr}\frac{k_{nf}/k_f}{(1-\varphi+\varphi(\rho C_p)_{cnt}/(\rho C_p)_f)}\frac{\partial^2 \theta}{\partial \eta^2} + \frac{1}{2} f \frac{\partial \theta}{\partial \eta} \end{aligned} \tag{15.18}$$

$$+\tau\left(\frac{\partial f}{\partial \eta}\frac{\partial \theta}{\partial \tau}-\frac{\partial f}{\partial \tau}\frac{\partial \theta}{\partial \eta}\right)-\frac{\partial \theta}{\partial \tau}=0, \tag{15.19}$$

The boundary conditions (15.4) are in following forms:

$$\begin{aligned} &f(0,\tau)=s, \frac{\partial f}{\partial \eta}(0,\tau)=\lambda+\sigma\frac{\partial^2 f}{\partial \eta^2}(0,\tau)+\delta\frac{\partial^3 f}{\partial \eta^3}(0,\tau), \theta(0,\tau)=1, \\ &\frac{\partial f}{\partial \eta}(\eta,\tau)\to 1-\lambda, \quad \theta(\eta,\tau)\to 0, \quad \text{as} \quad \eta\to\infty, \end{aligned} \tag{15.20}$$

The stability of the solution $f(\eta)=f_o(\eta)$ and $\theta(\eta)=\theta_o(\eta)$ that meet equations (15.1)–(15.4) can be determined by incorporating the analysis that recommended by Merkin [12] and Weidman et al. [13]:

$$f(\eta,\tau)=f_o(\eta)+e^{\gamma\tau}F(\eta,\tau), \quad \theta(\eta,\tau)=\theta_o(\eta)+e^{\gamma\tau}G(\eta,\tau), \tag{15.21}$$

here, function $F(\eta,\tau)$ is small in comparison with $f_o(\eta)$, $G(\eta,\tau)$ is relatively small compared to $\theta_o(\eta)$ and γ is the unknown eigenvalue. To determine the initial growth or decay of the solutions, the stability of $f_o(\eta)$ and $\theta_o(\eta)$ are determined by defining $\tau=0$ and thereby $F(\eta)=F_o(\eta)$ and $G(\eta)=G_o(\eta)$. Hence, we obtained a final equation:

$$\frac{1}{(1-\varphi)^{2.5}(1-\varphi+\varphi\rho_{cnt}/\rho_f)}F_o'''+\frac{1}{2}\left(f_oF_o''+f_o''F_o\right)+\gamma F_o'=0, \tag{15.22}$$

$$\frac{1}{\Pr}\frac{k_{nf}/k_f}{(1-\varphi+\varphi(\rho C_p)_{cnt}/(\rho C_p)_f)}G_o''+\frac{1}{2}\left(f_oG_o'+\theta_o'F_o\right)+\gamma G_o=0, \tag{15.23}$$

subjected to the boundary conditions:

$$\begin{aligned} &F_o(0)=s, \quad F_o'(0)=\lambda+\sigma F_o''(0)+\delta F_o'''(0), \quad G_o(0)=0, \\ &F_o'(\eta)\to 0, \quad G_o(\eta)\to 0 \quad \text{as} \quad \eta\to\infty. \end{aligned} \tag{15.24}$$

The stability of solutions obtained depends on the lowest number of eigenvalues γ. The flow is considered stable if the lowest eigenvalue is positive, meanwhile the flow is unstable if the obtained lowest eigenvalue is negative. The domain of potential eigenvalues can be identified by relaxing $F_o(\eta)$ on our boundary condition, see [18]. In this study, the boundary condition of $F_o'(\eta)\to 0$ as $\eta\to\infty$ need to be relaxed and replaced by $F_o''(0)=1$.

15.3 Results

Using the bvp4c solver in Matlab, the ordinary differential equations (15.8) and (15.9) together with conditions (15.10) are solved numerically. By guessing different initial values, dual solutions were obtained and both profiles satisfy the boundary condition (15.10) asymptotically. Table 15.1 shows thermophysical properties of water, SWCNT and MWCNT used for this paper. Figures 15.1 and 15.2 show the reduced skin friction $f''(0)$ and heat transfer $-\theta'(0)$ with velocity ratio parameter λ for different value of first order slip parameter ($\sigma=0, \sigma=0.2, \sigma=0.4$) of the SWCNT suspended nanofluids. The skin friction $f''(0)$ and heat transfer $-\theta'(0)$ increases with the increase of first order slip parameter σ for the first solution and decrease with σ for the second solution in the absence of second order slip parameter.

The figures also verify that unique solution only occur when $\lambda > 0$, while there exist dual solutions in between $\lambda_c < \lambda < 0$, i.e., when the plate moves in the opposite direction from the free stream. When the values of σ increased ($|\delta|$ is absent), the range of solution tends to be wider.

Table 15.1: Thermophysical properties of water, SWCNT and MWCNT (Khan et al. [7])

Physical Properties	Nanoparticle		Base fluid
	SWCNT	MWCNT	Water
$\rho(kg/m^3)$	2 600	1 600	997
$C_p(J/kgK)$	425	796	4179
$k(W/mK)$	6 600	3 000	0.613

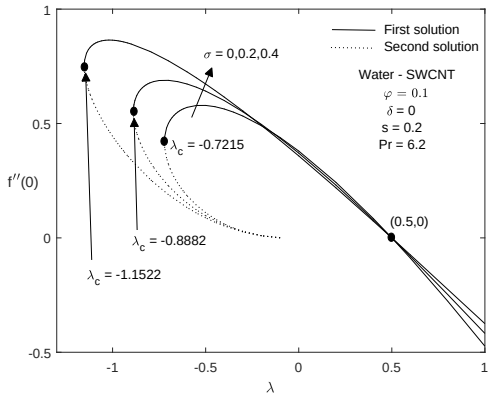

Figure 15.1: Variation of $f''(0)$ with σ

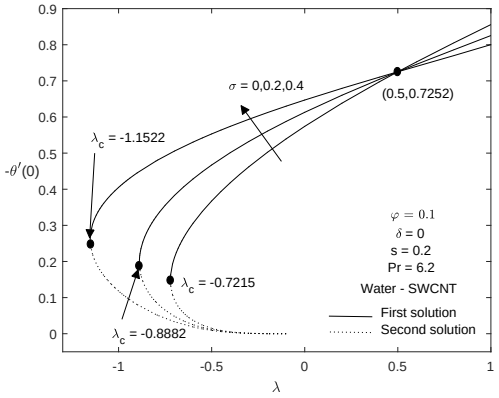

Figure 15.2: Variation of $-\theta'(0)$ with σ

The effects of second order slip parameter ($\delta = 0, \delta = -0.2, \delta = -0.4$) on the skin friction $f''(0)$ and heat transfer $-\theta'(0)$ are illustrated in Figures 15.3 and 15.4. One can observed that when only the second order slip parameter $|\delta|$ is considered, the heat loss from the plate become more quickly. Plus, the increasing values of $|\delta|$ will accelerates the $-\theta'(0)$ and $f''(0)$ from the surface. The increase of the second order slip parameter tends to expand the range of solution widely. Therefore, the second

order slip parameter leads to narrow the region of solutions while the first order slip parameter results in broaden the region of solutions. Nevertheless, the presence of slip parameters (σ and δ) causes the enlargement of the range of solutions.

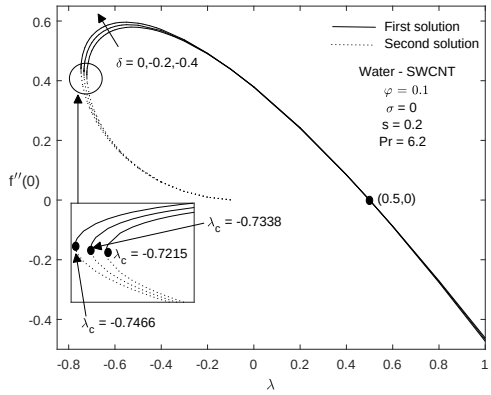

Figure 15.3: Variation of $f''(0)$ with δ

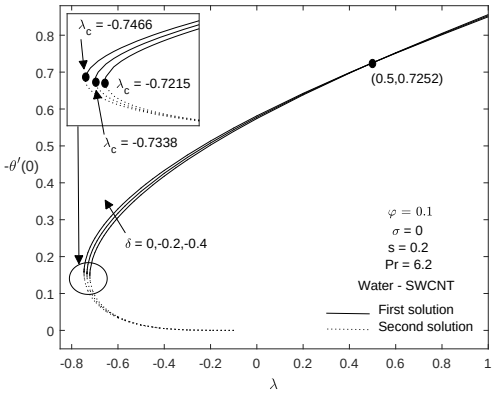

Figure 15.4: Variation of $-\theta'(0)$ with δ

Figures 15.5 and 15.6 depict the effect of solid volume fraction parameter φ on skin friction $f''(0)$ and heat transfer $-\theta'(0)$ for the MWCNT suspended nanofluids. Different observations are seen for the increment of solid volume fraction parameter where an increase in solid volume fractions caused the decreased in $f''(0)$ and $-\theta'(0)$. Basically, increasing number of Carbon nanotubes immersed in water will increase the viscosity of the fluid and results in a decrease in fluid's velocity. It is obviously seen from Figures 15.1 – 15.6, a unique solution exists when $0 < \lambda < 1$ (the plate moves in the assisting direction of the fluid), dual solutions were found for $\lambda_c \leq \lambda \leq 0$ (the plate moves against the direction of the fluid) and no solution was reported for $\lambda < \lambda_c$.

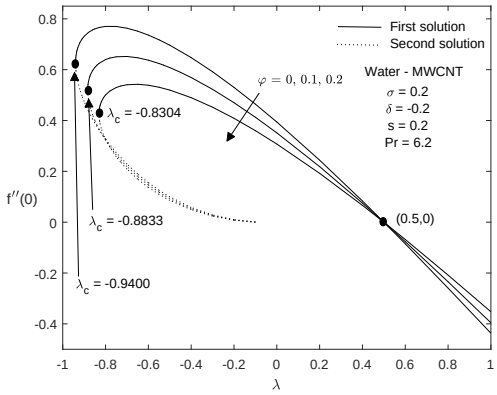

Figure 15.5: Variation of $f''(0)$ with φ

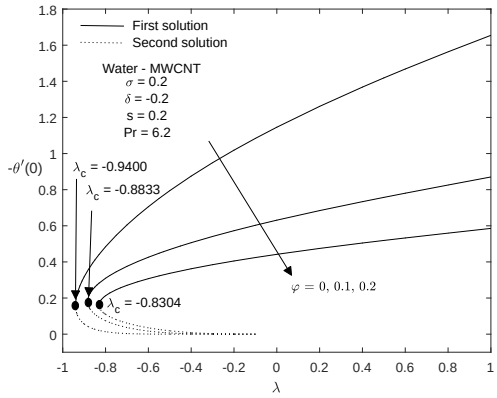

Figure 15.6: Variation of $-\theta'(0)$ with φ

The impact of slip (σ and δ) parameters on the skin friction coefficient $C_f Re_x^{1/2}$ and local Nusselt number $Nu_x Re_x^{-1/2}$ given by equation (15.14) with the solid volume fraction parameter φ are illustrated in figures 16.7 and 16.8. These figures indicate that the $C_f Re_x^{1/2}$ decrease remarkably when the slip parameters (σ and $|\delta|$) is increased. On the other hand, $Nu_x Re_x^{-1/2}$ was observed to be increased when the slip parameters increased. Also, these figures show that MWCNT have dominant impact on skin friction coefficient when compare with SWCNT. While for the case heat transfer rate, SWCNT are more dominant than MWCNT. Furthermore, the $C_f Re_x^{1/2}$ and $Nu_x Re_x^{-1/2}$ seems to increase as the φ increase.

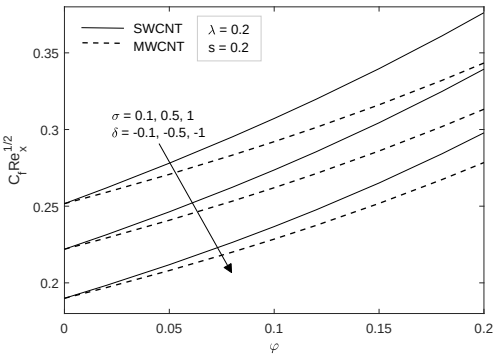

Figure 15.7: Variation of $C_f Re_x^{1/2}$ with σ and δ

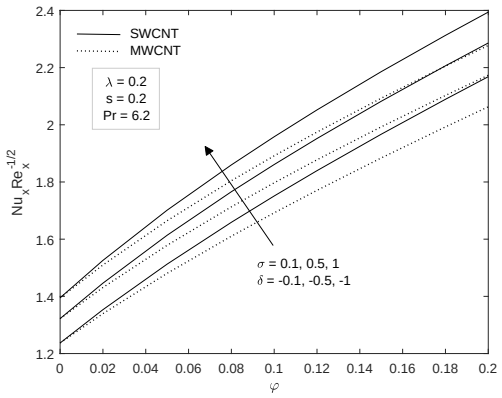

Figure 15.8: Variation of $Nu_x Re_x^{-1/2}$ with σ and δ

Finally, the impact of first and second order slip parameters (σ and δ) on the velocity $f'(\eta)$ and temperature $\theta(\eta)$ profiles are presented in Figures 16.9 — 15.12. The boundary conditions (15.10) are met asymptotically, supporting the validity of the numerical results obtained. In addition, these profiles also validate the dual solution obtained in Figures 15.1 – 16.8. Further, it is obviously seen that the second solution shows a thicker boundary layer thickness than the first solution.

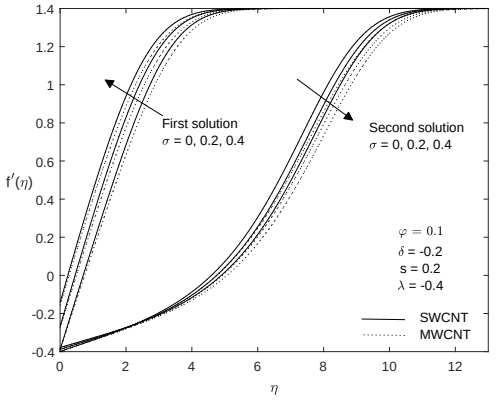

Figure 15.9: Velocity profile with σ

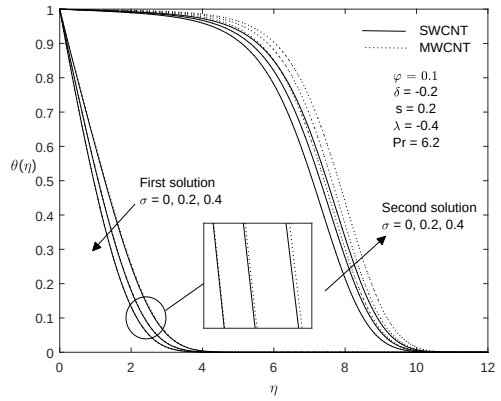

Figure 15.10: Temperature profile with σ

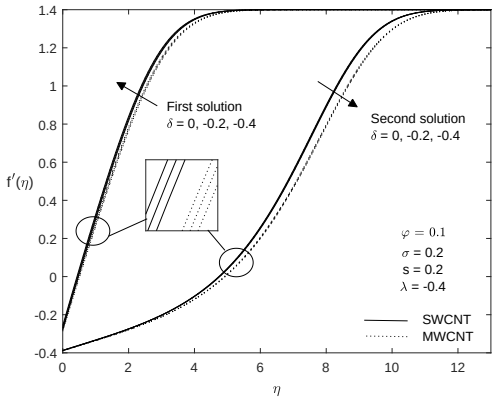

Figure 15.11: Velocity profile with δ

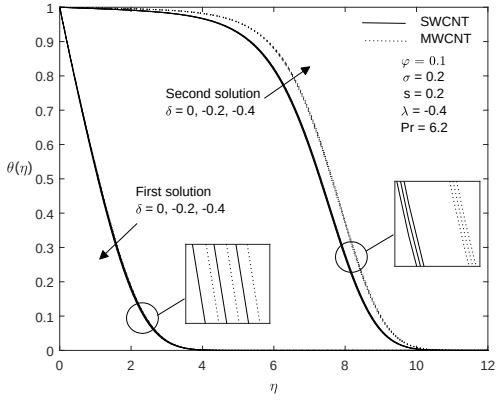

Figure 15.12: Temperature profile with δ

In the current research, the stability of solution has been performed to identify whether the first or second solution is stable and physically relevant or acts in opposite manner. The system of linear eigenvalue problems (15.22) and (15.23) with the new boundary condition (15.24) are applied into bvp4c code to determine the lowest eigenvalues γ. The flow is claimed as stable flow when the lowest eigenvalues

γ is positive and the flow is unstable when the lowest eigenvalues is negative. Table 15.2 displays the lowest eigenvalue for the variables value of λ with different values of slip parameters when $\varphi = 0.1$ for water-SWCNT. The results indicate that the eigenvalue is positive for first branch of solution and negative for second branch of solution. We can therefore verify that the first solution was physically stable, while the second solution was unstable.

Table 15.2: Smallest eigenvalues γ for λ with selected values of σ and δ when $s = 0.2$

σ	δ	λ	First solution	Second solution
		-0.803	0.0136	-0.0131
0.1	-0.1	-0.75	0.1136	-0.0849
		-0.6	0.2363	-0.1267
		-0.905	0.0183	-0.0175
0.2	-0.2	-0.85	0.1106	-0.0856
		-0.7	0.2235	-0.1307
		-1.215	0.0174	-0.0168
0.4	-0.4	-1.2	0.0505	-0.0461
		-1.0	0.1930	-0.1347

15.4 Conclusion

In this study, the numerical solution is obtained for the effect of second order slip on boundary layer flow and heat transfer over a moving plate in carbon nanotubes. We can summarize that dual solutions obtain when the plate moves in opposing direction with free stream ($\lambda < 0$). It is also found that slip parameters (first and second order) widens the range of solution and increase the heat transfer rate while the opposite behavior shown for skin friction coefficient when the plate and free stream moves in the same direction ($\lambda > 0$). Additionally, the increament in nanoparticle volume fraction parameter expand the region of the solutions. It is seen that SWCNTs is more effective in cooling process compared to MWCNTs. The stability analysis shows that the first solution was stable, whereas the second solution was unstable.

Acknowledgement

We acknowledges the financial support from Ministry of Higher Education Malaysia (FRGS/1/2018/STG06/UPM/02/4/5540155). We also grateful to the reviewers for their valuable comments and suggestions.

Bibliography

[1] Iijima S. (1991), *Helical microtubules of graphitic carbon*, Nature, Vol 354, 56–58.

[2] Iijima S., Ichihashi T. (1993), *Single-shell carbon nanotubes of 1-nm diameter*, Nature, Vol 363, 603–605.

[3] Biercuk M.J., Llaguno M.C., Radosavljevic M., Hyun J.K., Johnson A.T. and Fischer J.E. (2002), *Carbon nanotube composites for thermal management*, Applied Physics Letters, Vol 80(15), 2767–2769.

[4] Ding Y., Alias H., Wen D., and Williams R.A., (2006), *Heat transfer of aqueous suspensions of carbon nanotubes (CNT nanofluids)*, International Journal of Heat and Mass Transfer, Vol 49, 240—250.

[5] Sohel Murshed S.M., Nieto De Castro C.A., Lourenco M.J.V., Lopes M.L.M. and Santos F.J.V., (2011), *A review of boiling and convective heat transfer with nanouids*, Renewable and Sustainable Energy Reviews, Vol 15, 2342–2354

[6] Xue Q.Z., (2005), *Model for thermal conductivity of carbon nanotube-based composites*, Physica B: Condensed Matter, Vol 368, 302–307.

[7] Khan W.A., Khan Z.H., and Rahi M., (2014), *Fluid flow and heat transfer of carbon nanotubes along a flat plate with Navier slip boundary*, Applied Nanoscience, Vol 4(5), 633–641.

[8] Khan W.A., Culham R., and Haq R.U., (2015), *Heat transfer analysis of MHD water functionalized carbon nanotube flow over a static/moving wedge*, Journal of Nanomaterials , Vol 16(1), 1–13.

[9] Ellahi R., Hassan M., and Zeeshan A., (2015), *Study of natural convection MHD nanofluid by means of single and multi-walled carbon nanotubes suspended in a salt-water solution*, IEEE Transactions on Nanotechnology, Vol 14(4), 726–734.

[10] Hayat T., Farooq M., and Alsaedi A., (2015), *Stagnation point flow of carbon nanotubes over stretching cylinder with slip conditions*, Open Physics, Vol 13, 188–197.

[11] Hayat T., Hussain Z., Alsaedi A., and Ahmad B., (2016), *Heterogeneous-homogeneous reactions and melting heat transfer effects in flow with carbon nanotubes*, Journal of Molecular Liquids, Vol 220, 200–207.

[12] Hayat T., Ahmed S., Muhammad T., Alsaedi A., and Ayub M., (2017), *Computational modeling for homogeneous-heterogeneous reactions in three-dimensional flow of carbon nanotubes*, Results in Physics, Vol 7, 2651–2657.

[13] Hayat T., Muhammad K., Alsaedi A., and Asghar S., (2018), *Numerical study for melting heat transfer and homogeneous-heterogeneous reactions in flow involving carbon nanotubes*, Result in Physics, Vol 8, 415–421.

[14] Sakiadis B.C., (1961) *Boundary-layer behavior on continuous solid surfaces: I. Boundary-layer equations for two-dimensional and axisymmetric flow*, A.I.Ch.E. Journal, Vol 7, 26–28.

[15] Abdelhafez T.A., (1985), *Skin friction and heat transfer on a continuous flat surface moving in a parallel free stream*, International Journal of Heat and Mass Transfer, Vol 28(6), 1234–1237.

[16] Fang T., (2003), *Further study on a moving-wall boundary-layer problem with mass transfer*, Acta Mechanica, Vol 163, 183–188.

[17] Ishak A., Nazar R., and Pop I., (2009), *The effects of transpiration on the flow and heat transfer over a moving permeable surface in a parallel stream*, Chemical Engineering Journal, Vol 148(1), 63–67.

[18] Hayat T., Abbas Z., and Pop I., (2009), *Momentum and heat transfer over a continuously moving surface with a parallel free stream in a viscoelastic fluid*, Numerical Methods for Partial Differential Equations, Vol 26, 305–319.

[19] Rohni A.M., Ahmad S., and Pop I., (2011), *Boundary layer flow over a moving surface in a nanofluid beneath a uniform free stream*, International Journal of Numerical Methods for Heat & Fluid Flow, Vol 21, 828–846.

[20] Hayat T., Iqbal Z., Mustafa M., and Obaidat S., (2012), *Flow and heat transfer of jeffrey fluid over a continuously moving surface with a parallel free stream*, Journal of Heat Transfer, Vol 134(1), 1–7.

[21] Bachok N., Ishak A., and Pop I., (2012), *Flow and heat transfer characteristics on a moving plate in a nanofluid*, International Journal of Heat and Mass Transfer, Vol 55(4), 642–648.

[22] Bachok N., Ishak A., and Pop I., (2012), *Boundary layer flow over a moving surface in a nanofluid with suction or injection*, Acta Mechanica Sinica, Vol 28(1), 34–40.

[23] Weidman P.D., Kubitschek D.G., and Davis A.M.J., (2006), *The effect of transpiration on self-similar boundary layer flow over moving surfaces*, International Journal of Engineering Science, Vol 44, 730–737.

[24] Najib N., Bachok N., Arifin N.M., and Senu N., (2017), *Boundary layer flow and heat transfer of nanofluids over a moving plate with partial slip and thermal convective boundary condition: Stability analysis*, International Jornal of Mechanics, Vol 11, 19–24.

[25] Jahan S., Sakidin H., Nazar R., and Pop I., (2017), *Boundary layer flow of nanofluid over a moving surface in a flowing fluid using revised model with stability analysis*, International Journal of Mechanical Sciences, Vol 131–132, 1073–1081.

[26] Wu L., (2008), *A slip model for rarefied gas flows at arbitrary Knudsen number*, Applied Physics Letters, Vol 93, 1–3.

[27] Fang T., Yao S., Zhang J., and Aziz A., (2010), *Viscous flow over a shrinking sheet with a second order slip flow model*, Communications in Nonlinear Science and Numerical Simulation, Vol 15(7), 1831–1842.

[28] Fang T., and Aziz A., (2010), *Viscous Flow with Second-Order Slip Velocity over a Stretching Sheet*, A Journal of Physical Sciences, Vol 65(12), 1087–1092.

[29] Nandeppanavar M.M., Vajravelu K., Abel M.S., and Siddalingappa M.N., (2012), *Second order slip flow and heat transfer over a stretching sheet with non-linear Navier boundary condition*, International Journal of Thermal Sciences, Vol 58, 143–150.

[30] Rosca A.V., and Pop I., (2013), *Flow and heat transfer over a vertical permeable stretching/shrinking sheet with a second order slip*, International Journal of Heat and Mass Transfer, Vol 60, 355–365.

[31] Rosca N.C., and Pop I., (2014), *Boundary layer flow past a permeable shrinking sheet in a micropolar fluid with a second order slip flow model*, European Journal of Mechanics - B/Fluids, Vol 48, 115–122.

[32] Soid S.K., Kechil S.A., and Ishak A., (2016), *Axisymmetric stagnation-point flow over a stretching/shrinking plate with second-order velocity slip*, Propulsion and Power Research, Vol 5, 194–201.

[33] Yasin M.H.M., Ishak A., and Pop I., (2017), *Boundary layer flow and heat transfer past a permeable shrinking surface embedded in a porous medium with a second-order slip: A stability analysis*, Applied Thermal Engineering, Vol 115, 1407–1411.

[34] Najib N., Bachok N., Arifin N.M., and Ali F.M., (2018), *Stability analysis of stagnation-point flow in a nanofluid over a stretching/shrinking sheet with second-order slip, soret and dufour effects: A revised model*, Applied Science, Vol 8(4), 1–13.

[35] Anuar N.S., Bachok N., and Pop I., (2018), *A stability analysis of solutions in boundary layer flow and heat transfer of carbon nanotubes over a moving plate with slip effect*, Energies, Vol 11(12), 1–20.

[36] Oztop H.F., and Abu-Nada E., (2008), *Numerical study of natural convection in partially heated rectangular enclosures filled with nanofluids*, International Journal of Heat and Fluid Flow, Vol 29(5), 1326–1336.

[37] Merkin J.H.,(1986), *On dual solutions occurring in mixed convection in a porous medium*, Journal of Engineering Mathematics, Vol 20(2), 171–179.

[38] Harris S.D., Ingham D.B., and Pop I., (2009), *Mixed convection boundary-layer flow near the stagnation point on a vertical surface in a porous medium: brinkman model with slip*, Transport in Porous Media, Vol 77(2), 267–285.

[39] Afzal N., Badaruddin A., and Elgarvi A.A., (1993), *Momentum and heat transport on a continuous flat surface moving in a parallel stream*, International Journal of Heat and Mass Transfer, Vol 36(13), 3399–3403.

Chapter 16

Magnetic Field Effect on Nanofluid Flow and Heat Transfer past a Moving Horizontal Thin Needle with Stability Analysis

Siti Nur Alwani Salleh[1], **Norfifah Bachok**[1,2,*], Norihan Md Arifin[1,2], Fadzilah Md Ali[1,2]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

*Corresponding author: norfifah@upm.edu.my

Abstract

An analysis has been done to examine the boundary layer flow of an electrically conducting nanofluid passing through a horizontal thin needle. The resulting system of ordinary differential equation is obtained via similarity transformations. The Bvp4c solver in MATLAB software is applied to compute the numerical solution. The results for the local Nusselt number, skin friction coefficient and profiles are graphically portrayed with respect to the parameters of interest. The results obtained have shown that the multiple solutions are available in a certain region of the velocity ratio parameter. Stability analysis is applied to verify which of the solutions obtained are stable. It is noticed that the stable solution is represented by the upper branch solution.

Keywords: magnetic field, thin needle, dual solutions, stability analysis.

16.1 Introduction

The consideration of the boundary layer behavior around a thin needle is an essential appearance of flow occurring in a broad range of industrial and technological applications. For example, geothermal power generation, transportation, aerospace, metal spinning and coating of wires. It appears that the problem involving the boundary layer analysis in a viscous fluid near a thin needle has been first analyzed by Lee [1]. In his work, he derived an approximation solution and established the asymptotic behaviors of the fluid motion. Since then, many authors [2–5] considered the problems involving the momentum and energy transfer with the presence

of several effects such as magnetic field, thermal radiation, buoyancy force and moving surface. Krishna et al. [6] considered the study of the thin needle with the appearance of magnetic field. From their studies, it is noticed that the larger magnetic parameter enhances the resistive force, subsequently decrease the velocity and thicken the thermal boundary layer.

Nanofluid simply means a combination between the nanoparticles and base fluid with dimensions smaller than 100 nm. This fluid has been developed a decade ago by Choi [7] with the specific target to increase the performance of heat transfer fluids in high-technology applications. Previously, the usage of the conventional heat transfer fluids which include ethylene glycol, water and oil less affected the performance of heat transfer. Since nanofluid was introduced, it's become one of the important factors to overcome the limitation of conventional heat transfer fluid. Most of the systems, nowadays, had considered nanofluid as a cooling device due to its role to increase the performance of thermal conductivity of manufacturing purposes and reduces the operating costs as well. The comprehensive references on the nanofluid are reported by some researchers [8–11].

The consideration of the stability analysis has attracted many authors due to the stable solutions has a good physical meaning which can be realized. The procedure of this analysis was developed by Merkin [12]. Motivated from Merkin [12] work, Weidman et al. [13] continued their research by considering the stability analysis. In their research, they noticed that the stable solution came from the upper branch or first solution. Since then, many problems involved the stability analysis were carried out [14–16].

The purpose of the current research is to explore the impact of the magnetic parameter on the boundary layer flow and heat transfer over a moving thin needle in nanofluid. The following sections discuss the derivation of the problem and also the results obtained from this study.

16.2 Mathematical Modeling

Let us consider a moving slender needle in the boundary layer flow of a nanofluid at constant far field temperature T_∞. Let (u, v) be the velocity components of x and r directions, respectively with $r = R(x) = (\nu cx/U)^{1/2}$ is the needle radius. It is assumed the needle moves with a constant velocity U_b in the opposite or same way of free-stream of constant velocity U_∞. The magnetic field of strength B_0 is imposed perpendicular to x-axis and the fluid is electrically conducting. In this way, the equations that govern the MHD flow are

$$(ru)_x + (rv)_r = 0, \tag{16.1}$$

$$uu_x + vu_r = \frac{\mu_{nf}}{\rho_{nf}} \frac{1}{r} (ru_r)_r - \frac{\sigma}{\rho_{nf}} B_0^2 u, \tag{16.2}$$

$$uT_x + vT_r = \frac{\alpha_{nf}}{r} (rT_r)_r , \tag{16.3}$$

and the boundary conditions

$$\begin{aligned} &u = U_b, \;\; v = 0, \;\; T = T_b \;\text{ at }\; r = R(x), \\ &u \to U_\infty, \;\; T \to T_\infty \;\text{ as }\; r \to \infty, \end{aligned} \tag{16.4}$$

in which T is the nanofluid temperature, T_b is the temperature of the wall, μ is the dynamic viscosity, ρ is the density, k is the thermal conductivity, C_p is specific heat at a uniform pressure and α is the thermal diffusivity where subscripts 's', 'f' and 'nf' refer to 'solid', 'base fluid' and 'nanofluid', respectively.

Following Oztop and Abu-Nada [17], the applied relation for the physical properties of nanofluid are

$$\alpha_{nf} = \frac{k_{nf}}{(\rho C_p)_{nf}},\ \mu_{nf} = \frac{\mu_f}{(1-\phi)^{2.5}},\ \frac{k_{nf}}{k_f} = \frac{(k_s+2k_f)-2\phi(k_f-k_s)}{(k_s+2k_f)+\phi(k_f-k_s)},$$

$$\rho_{nf} = (1-\phi)\,\rho_f + \phi\rho_s,\ (\rho C_p)_{nf} = (1-\phi)\,(\rho C_p)_f + \phi\,(\rho C_p)_s\,, \tag{16.5}$$

where ϕ is the nanoparticle volume fraction parameter. We introduce the similarity transformations below

$$\psi = \nu x f(\eta),\ \eta = \frac{Ur^2}{\nu x},\ \theta(\eta) = \frac{T-T_\infty}{T_w-T_\infty}, \tag{16.6}$$

where the stream function $\psi(x,r)$ is introduced as $u = r^{-1}\partial\psi/\partial r$ and $v = -r^{-1}\partial\psi/\partial x$. Using equation (16.6), equation (16.1) is fulfill, and then equations (16.2) and (16.3) give

$$\frac{2}{D_1}\left(\eta f''' + f''\right) + ff'' - \frac{M}{D_2}f' = 0, \tag{16.7}$$

$$\frac{2}{Pr}\frac{D_3}{D_4}\left(\eta\theta'' + \theta'\right) + f\theta' = 0, \tag{16.8}$$

where

$$D_1 = (1-\phi)^{2.5}\left[1-\phi+\phi\,(\rho_s/\rho_f)\right],\ D_2 = \left[1-\phi+\phi\,(\rho_s/\rho_f)\right],$$

$$D_3 = k_{nf}/k_f,\ D_4 = 1-\phi+\phi\,(\rho C_p)_s\,/\,(\rho C_p)_f\,.$$

The appropriate boundary conditions are

$$f(c) = \frac{\varepsilon}{2}c,\ f'(c) = \frac{\varepsilon}{2},\ \theta(c) = 1,$$

$$f'(\eta) \to \frac{1-\varepsilon}{2},\ \theta(\eta) \to 0 \ \text{ as } \ \eta \to \infty. \tag{16.9}$$

Here, prime refer to differentiation with associate to similarity variable η, $M = \sigma x B_0^2/2U\rho_f$ is the magnetic parameter, $Pr = \nu/\alpha$ is a Prandtl number and $\varepsilon = U_b/U$ is the velocity ratio or moving parameter with $U = U_b + U_\infty$.

The coefficient of skin friction and local Nusselt number are

$$C_f = \frac{\mu_{nf}(u_r)_{r=c}}{\rho_f U^2}, = \frac{4}{(1-\varphi)^{2.5}}Re_x^{-1/2}c^{1/2}f''(c), \tag{16.10}$$

$$Nu_x = \frac{-xk_{nf}(T_r)_{r=c}}{k_f(T_w-T_\infty)} = -2\frac{k_{nf}}{k_f}Re_x^{1/2}c^{1/2}\theta'(c), \tag{16.11}$$

in which $Re_x = Ux/\nu$ is a local Reynold number.

16.3 Stability Analysis

In this section, the derivation for stability analysis has been done by considering the equations (16.2) and (16.3) in unsteady case as follows

$$u_t + uu_x + vu_r = \frac{\mu_{nf}}{\rho_{nf}} \frac{1}{r} (ru_r)_r - \frac{\sigma}{\rho_{nf}} B_0^2 u, \tag{16.12}$$

$$T_t + uT_x + vT_r = \frac{\alpha_{nf}}{r} (rT_r)_r , \tag{16.13}$$

where t denote the time. The similarity transformations in unsteady case are

$$\psi = \nu x f(\eta, \tau), \ \eta = \frac{Ur^2}{\nu x}, \ \theta(\eta, \tau) = \frac{T - T_\infty}{T_w - T_\infty}, \ \tau = \frac{2Ut}{x}. \tag{16.14}$$

Afterward, replacing equation (16.14) into mass and energy equations (16.12) and (16.13) to get

$$\frac{2}{D_1} \left(\eta \frac{\partial^3 f}{\partial \eta^3} + \frac{\partial^2 f}{\partial \eta^2} \right) + f \frac{\partial^2 f}{\partial \eta^2} - \frac{M}{D_2} \frac{\partial f}{\partial \eta} + \tau \frac{\partial f}{\partial \eta} \frac{\partial^2 f}{\partial \eta \partial \tau} - \tau \frac{\partial f}{\partial \tau} \frac{\partial^2 f}{\partial \eta^2} - \frac{\partial^2 f}{\partial \eta \partial \tau} = 0, \tag{16.15}$$

$$\frac{2}{Pr} \frac{D_3}{D_4} \left(\eta \frac{\partial^2 \theta}{\partial \eta^2} + \frac{\partial \theta}{\partial \eta} \right) + f \frac{\partial \theta}{\partial \eta} + \tau \frac{\partial f}{\partial \eta} \frac{\partial \theta}{\partial \tau} - \tau \frac{\partial f}{\partial \tau} \frac{\partial \theta}{\partial \eta} - \frac{\partial \theta}{\partial \tau} = 0. \tag{16.16}$$

The boundary conditions are

$$f(c, \tau) = \tau \frac{\partial f}{\partial \tau}(c, \tau) + \frac{\varepsilon}{2} c, \ \frac{\partial f}{\partial \eta}(c, \tau) = \frac{\varepsilon}{2}, \ \theta(c, \tau) = 1,$$

$$\frac{\partial f}{\partial \eta}(\eta, \tau) \to \frac{1 - \varepsilon}{2}, \ \theta(\eta, \tau) \to 0 \text{ as } \eta \to \infty. \tag{16.17}$$

According to Weidman et al. [13], we assume

$$f(\eta, \tau) = f_0(\eta) + e^{-\gamma \tau} F(\eta, \tau), \ \theta(\eta, \tau) = \theta_0(\eta) + e^{-\gamma \tau} G(\eta, \tau). \tag{16.18}$$

Thus, the stability solution $f = f_0(\eta)$ and $\theta = \theta_0(\eta)$ that meet the boundary value problem can be determined. Here, functions $F(\eta, \tau)$ is small relative to $f_0(\eta)$, $G(\eta, \tau)$ is small relative to $\theta_0(\eta)$ and γ is the eigenvalue parameter.

Replacing equation (16.18) into equations (16.15)-(16.16), we finally get the equations for the linear eigenvalue

$$\frac{2}{D_1} \left(\eta F_0''' + F_0'' \right) + f_0 F_0'' + f_0'' F_0 - M F_0' + \gamma F_0' = 0, \tag{16.19}$$

$$\frac{2}{Pr} \frac{D_3}{D_4} \left(\eta G_0'' + G_0' \right) + f_0 G_0' + F_0 \theta_0' + \gamma G_0 = 0, \tag{16.20}$$

with respect to the conditions (16.17)

$$F_0(c) = 0, \ F_0'(c) = 0, \ G_0(c) = 0$$

$$F_0'(\eta) \to 0, \ G_0(\eta) \to 0, \ \text{as } \eta \to \infty. \tag{16.21}$$

Harris et al. [18] recommend that the minimum eigenvalues γ can be computed by relaxing the boundary condition on $G_0(\eta)$ or $F_0(\eta)$. In this study, we decided to relax the condition on $F_0(\eta) \to 0$ as $\eta \to \infty$, and replace the condition by $F_0''(c) = 1$.

16.4 Discussion of Results

The interesting behaviors of all embedding physical parameters which include needle thickness c, nanoparticle volume fraction ϕ, magnetic parameter M and velocity ratio ε are highlighted in this section. The nonlinear self-similar equations (16.7) and (16.8) together with the boundary conditions (16.9) are computed via bvp4c package through MATLAB software. The detail explanation of the bvp4c package are elaborated in the work of Salleh et al. [16]. The thermo physical properties of the base fluid, alumina (Al_2O_3), titania (TiO_2) and copper (Cu) are reported in Oztop and Abu-Nada [17] work.

Figures 1 and 2 are sketched to analyze the effect of magnetic parameter on reduced skin friction $f''(c)$ and reduced Nusselt number $-\theta'(c)$ for varying values of velocity ratio parameter ε. It is seen from these figures that the higher rate of magnetic field reduces both magnitudes of $f''(c)$ and $-\theta'(c)$. The large magnetic field causes a large barrier to the fluid particles and as a consequence, heat will be generated in the system. Hence, there exists a Lorentz force that is a friction caused by the foisting of magnetic field. The friction and temperature of the wall will decrease due to the presence of this force that distracts the nanofluid motion over a thin needle. It is interesting to know that the smaller magnetic parameter expands the possible range of the dual similarity solutions exist. However, there is a limitation for the dual solutions exist where the value of ε must be in between $\varepsilon_c < \varepsilon \leq -0.6$ for $f''(c)$, while $\varepsilon_c < \varepsilon \leq -1.6$ for $-\theta'(c)$. On the other hand, no solutions were obtained for $\varepsilon < \varepsilon_c$. When the needle is not in the same way as the free-stream flow ($\varepsilon < 0$), the multiple solutions are seem to appear as shown in both figures.

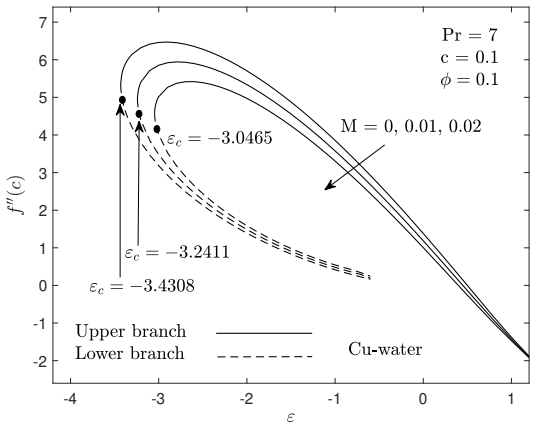

Figure 16.1: Impact of M on reduced skin friction

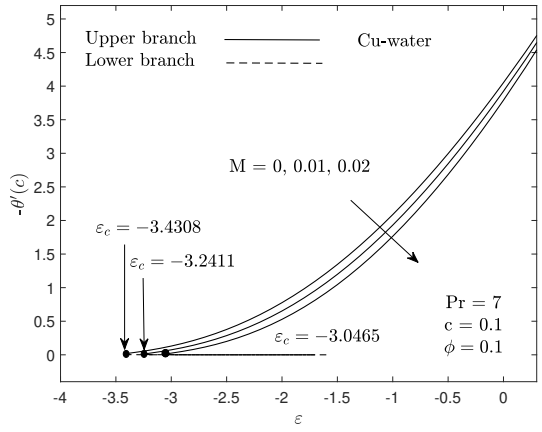

Figure 16.2: Impact of M on reduced Nusselt number

The impact of needle thickness c on the variation of reduced skin friction and reduced Nusselt number is plotted in figures 3 and 4 with ε for $M = 0.02$. It is clear from the figures that the thinner surface of the needle gives higher magnitudes of reduced skin friction and also heat transfer. Basically, the reduction of needle thickness causes the wall in contact with the fluid particles to decrease and consequently, increases the skin friction. In addition, the thinner wall also allows heat to seep quickly than the thicker one. In these figures, the dual similarity solutions are noticed to appear when $\varepsilon_c < \varepsilon \leq -0.6$ for the skin friction and when $\varepsilon_c < \varepsilon \leq -2.0$ for the heat transfer.

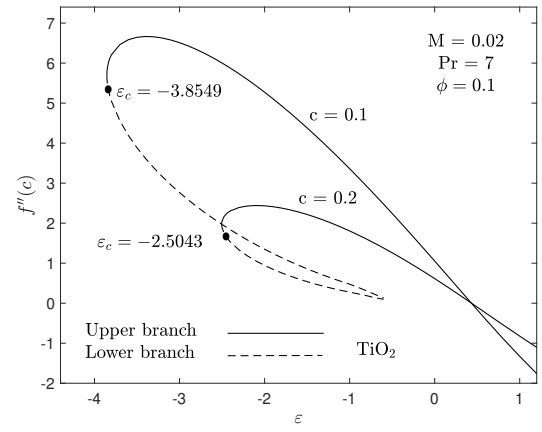

Figure 16.3: Impact of c on reduced skin friction

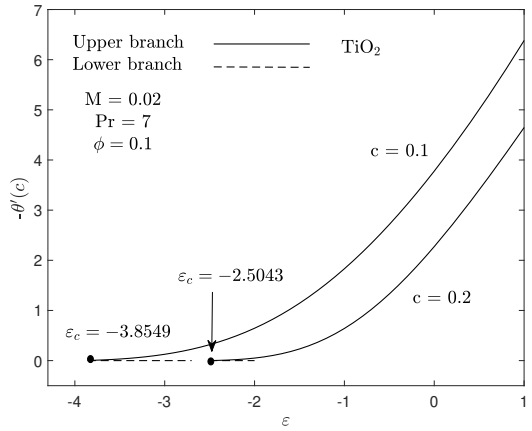

Figure 16.4: Impact of c on reduced Nusselt number

In addition, Figure 5 is plotted to see the influence of the varying magnetic parameter and nanoparticle volume fraction on the skin friction coefficient $(Re_x)^{1/2}C_f$. It is obvious from this figure that by enhancing the magnetic field rate, the magnitude of skin friction seems to decrease. This follows that an increment in the magnetic parameter thickens the boundary layer thickness for momentum and causing less shear stress occurs. This, subsequently, diminishes the coefficient of skin friction on the wall. Furthermore, the skin friction coefficient seems to increase as the ϕ increase. Physically, higher collision between the base fluid particles and nanoparticles causing the following situation to occur. The variation trend of local Nusselt number $(Re_x)^{-1/2}Nu_x$ versus ϕ for different nanoparticles, namely, Cu, Al_2O_3 and TiO_2 is displayed in figure 6. In this figure, the higher value of $(Re_x)^{-1/2}Nu_x$ is obtained for TiO_2 compared to Al_2O_3 and Cu.

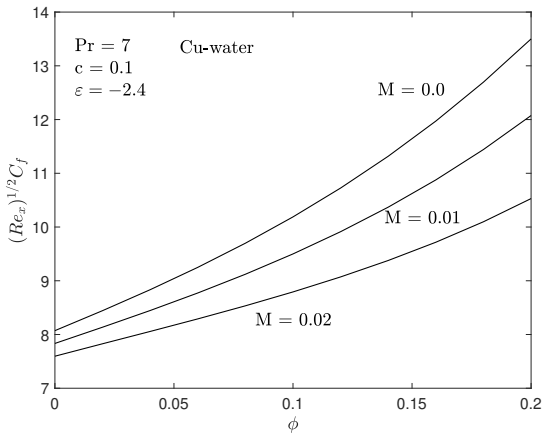

Figure 16.5: Impact of M on skin friction coefficient

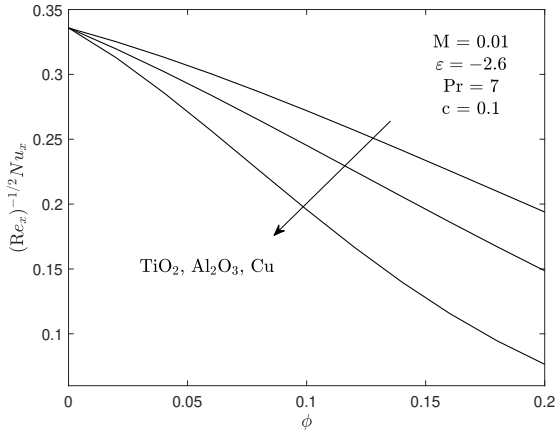

Figure 16.6: Impact of different nanoparticles on local Nusselt number

The sample profiles for the velocity and temperature are portrayed in figures 7 to 10 for different effects, namely magnetic field M and thickness of the needle c. As we can see, all the profiles obtained has complied the boundary conditions (16.9) asymptotically with various shapes of graphs. It is worth knowing that these profiles are plotted to confirm the numerical results gained for the present study and to show the appearance of the dual solutions.

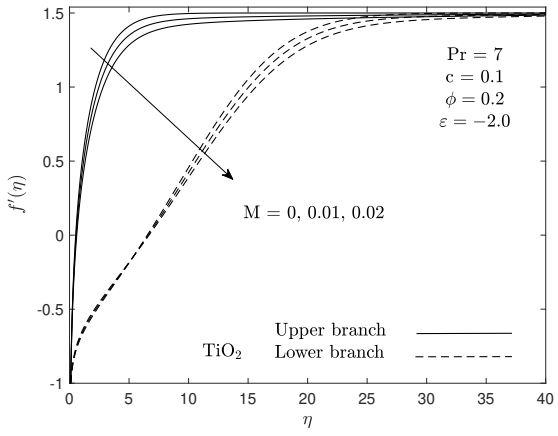

Figure 16.7: Impact of M on dual velocity profiles

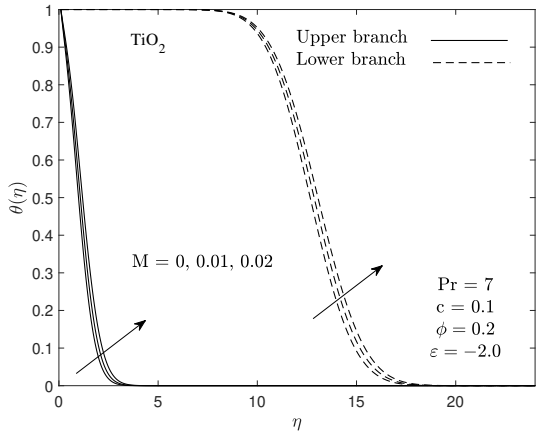

Figure 16.8: Impact of M on dual temperature profiles

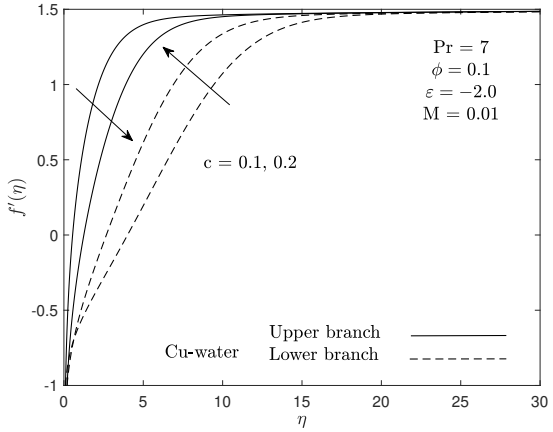

Figure 16.9: Impact of c on dual velocity profiles

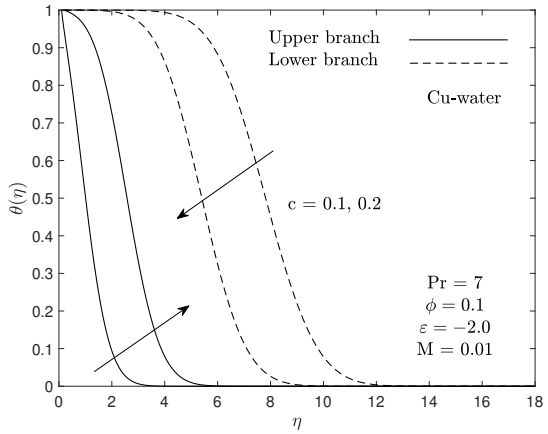

Figure 16.10: Impact of c on dual temperature profiles

The main purpose to carried out the stability analysis is to know whether the solution is stable or not by depending on the smallest eigenvalues γ. By considering

the linear eigenvalue equations (16.19) and (16.20) with the conditions (16.21), we can compute the values of γ via bvp4c solver in MATLAB. Table 1 displays the minimum eigenvalues for a few values of M and ε when $\phi = c = 0.1$ for Cu-water. The table presents that for upper branch solutions, the positive value of γ is obtained. This means that there exist an initial deteriorate of disturbances and the system is linearly stable. Nevertheless, the lower branch solutions give the opposite sign of the eigenvalue which is negative. This simply means that there is an initial growth of disturbances and the system or solution is unstable.

Table 16.1: Smallest eigenvalues γ for several values of M and ε for Cu-water when $\phi = c = 0.1$

M	ε	Upper branch	Lower branch
0	-3.4305	0.0076	-0.0075
	-3.4302	0.0110	-0.0108
	-3.43	0.0127	-0.0125
0.01	-3.2408	0.0069	-0.0068
	-3.2404	0.0109	-0.0108
	-3.24	0.0139	-0.0136
0.02	-3.0464	0.0042	-0.0041
	-3.046	0.0089	-0.0088
	-3.04	0.0321	-0.0306

16.5 Concluding Remarks

In this study, the numerical solution is obtained for the boundary layer flow of incompressible nanofluid around a slender needle. The significant impacts of the flow and heat transfer for various physical parameters are concluded below:

- The appearance of dual solutions is noticed when the needle moves in the reverse way of fluid flow ($\varepsilon < 0$).
- The decrement in magnetic parameter and needle thickness expand the region of the solutions gained.
- In stability analysis, the solutions for the upper branch represents the stable flow, whereas for the lower branch represents an unstable solution.
- Increases the magnetic parameter and needle thickness cause the skin friction coefficient to diminish, whereas the opposite trend is noticed for higher values of nanoparticle volume fraction parameters.
- The reduced Nusselt number decreases for higher magnetic field and needle thickness.
- Titania obtained the highest magnitude of the local Nusselt number, while alumina obtained the highest skin friction coefficient.

Acknowledgments

We are grateful to the referees for their valuable comments and suggestions. We also acknowledges the financial support from Universiti Putra Malaysia under Putra Grant GP-IPS/2018/9667900.

Bibliography

[1] Lee L.L. (1967), *Boundary Layer over a Thin Needle*, The Physics of Fluids, Vol 10, 1820—1822.

[2] Ahmad S., Arifin N.M., Nazar R., Pop I. (2008), *Mixed Convection Boundary Layer Flow along Vertical Thin Needles: Assisting and Opposing Flows*, International Communications in Heat and Mass Transfer, Vol 35(2), 157–162.

[3] Trimbitas R., Grosan T., Pop I. (2014), *Mixed Convection Boundary Layer Flow along Vertical Thin Needles in Nanofluids*, International Journal of Numerical Methods for Heat & Fluid Flow, Vol 24, 579–594.

[4] Hayat T., Khan M.I., Farooq M., Yasmeen T., Alsaedi A. (2016), *Water-carbon Nanofluid Flow with Variable Heat Flux by a Thin Needle*, Journal of Molecular Liquids, Vol 224, 786–791.

[5] Ahmad R., Mustafa M., Hina S. (2017), *Buongiorno's Model for Fluid Flow around a Moving Thin Needle in a Flowing Nanofluid: A Numerical Study*, Chinese Journal of Physics, Vol 55(4), 1264–1274.

[6] Krishna P.M., Sharma R.P., Sandeep N. (2017), *Boundary Layer Analysis of Persistent Moving Horizontal Needle in Blasius and Sakiadis Magnetohydrodynamic Radiative Nanofluid Flows*, Nuclear Engineering and Technology, Vol 49(8), 1654–1659.

[7] Choi S.U.S. (1995), *Enhancing Thermal Conductivity of Fluids with Nanoparticles*, Proceeding ASME International Mechanical Congress and Exposition, Vol 231, 99–105.

[8] Eid M.R. (2016), *Chemical Reaction Effect on MHD Boundary-layer Flow of Two-phase Nanofluid Model over an Exponentially Stretching Sheet with a Heat Generation*, Journal of Molecular Liquids, Vol 220, 718–725.

[9] Mustafa M., Khan J.A., Hayat T., Alsaedi A. (2017), *Buoyancy Effects on the MHD Nanofluid Flow past a Vertical Surface with Chemical Reaction and Activation Energy*, International Journal of Heat and Mass Transfer, Vol 108, 1340–1346.

[10] Turkyilmazoglu M. (2018), *Buongiorno Model in a Nanofluid filled Asymmetric Channel Fulfilling Zero Net Particle Flux at the Walls*, International Journal of Heat and Mass Transfer, Vol 126, 974–979.

[11] Zulkifli S.N., Sarif N.M., Salleh M.Z. (2019), *Numerical Solution of Boundary Layer Flow over a Moving Plate in a Nanofluid with Viscous Dissipation: A revised Model*, Journal of Advanced Research in Fluid Mechanics and Thermal Sciences, Vol 56(2), 287–295.

[12] Merkin J.H. (1985), *On Dual Solutions Occuring in Mixed Conve-ction in a Porous Medium*, Journal of Engineering Mathematics, Vol 20, 171–179.

[13] Weidman P.D., Kubitschek D.G., Davis A.M.J. (2006), *The Effect of Transpiration on Self-similar Boundary Layer Flow over Moving Surfaces*, International Journal of Engineering Science, Vol 44, 730–737.

[14] Noor M.A.M., Nazar R., Jafar K., Pop I. (2014), *Stability Analysis of Flow and Heat Transfer on a Permeable Moving Plate in a Co-flowing Nanofluid*, AIP Conference Proceeding, Vol 1614, 898–905.

[15] Najib N., Bachok N., Arifin N.M., Senu N. (2017), *Boundary Layer Flow and Heat Transfer of Nanofluids over a Moving Plate with Partial Slip and Thermal Convective Boundary Condition: Stability Analysis*, International Journal of Mechanical, Vol 11, 19–24.

[16] Salleh S.N.A., Bachok N., Arifin N.M., Ali F.M., Pop I. (2018), *Stability Analysis of Mixed Convection Flow towards a Moving Thin Needle in Nanofluid*, Applied Sciences, Vol 8, 842.

[17] Oztop H.F., Abu-Nada E. (2008), *Numerical Study of Natural Convection in Partially Heated Rectangular Enclosures filled with Nanouids*, International Journal of Heat & Fluid Flow, Vol 29, 1326–1336.

[18] Harris S.D., Ingham D.B., Pop I. (2009), *Mixed Convection Boundary-layer Flow near the Stagnation Point on a Vertical Surface in a Porous Medium: Brinkman Model with Slip*, Transport Porous Media, Vol 77, 267–285.

Chapter 17

Stability Analysis for Three Dimensional Viscous Flow over an Unsteady Permeable Stretching or Shrinking Sheet - A Mathematical Formulation

Muhammad Norsyawalludin Idris[1], **Mohd Ezad Hafidz Hafidzuddin**[2,*], Norihan Md Arifin[1], Roslinda Nazar[3]

[1] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3] Centre for Modelling & Data Science, Faculty of Science & Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia.

*Corresponding author: ezadhafidz@upm.edu.my

Abstract

This paper focuses on the mathematical formulation for the stability analysis of an unsteady three-dimensional boundary layer flow past a permeable stretching/shrinking sheet. Similarity transformation is used to reduce the governing system of nonlinear partial differential equations into a system of ordinary differential equations. These equations are then solved numerically by using the "bvp4c" function in MATLAB. Multiple solutions are found for a certain range of the governing parameters. The stability of the solutions obtained is analyzed to determine which solution branch is stable and physically realisable.

Keywords: boundary layer; multiple solutions; stability analysis; stretching/shrinking sheet; three-dimensional unsteady flow; bvp4c.

17.1 Introduction

The study of viscous flow and heat transfer due to stretching sheet has many applications in industrial and manufacturing prosesses, such as extrusion, wire drawing, hot rolling and others. Sakiadis [1, 2] was the first to consider the problem of boundary layer flow over a stretching sheet. Later, his work is verified by Tsou et al. [3] and extended by Crane [4] for the two-dimensional problem. McLeod and Rajagopal [5] discussed the uniqueness of the exact analytical solution presented in [4], while Gupta

and Gupta [6] extended [4] by investigating the effect of heat and mass transfer over a stretching sheet subject to suction or blowing. The problem in [2] was extended by Wang [7] to a three-dimensional flow due to a stretching flat surface. More studies regarding flow over a stretching sheet or surface can be found in the literature, such as Banks [8]; Rajagopal et al. [9]; Chen and Char [10]; Magyari and Keller [11, 12]; Nadeem et al. [13]; Bhattacharyya and Layek [14]; Mabood et al. [15] and recently; Turkyilmazoglu [16]; Wu [17]; El-Mistikawy [18] and Shamshuddin et al. [19] among others.

Recently, the study of flow due to shrinking sheet, where the velocity of the boundary is moving towards a fixed point, have become significantly important in the industry. This new type of flow is essentially a backward flow, as described by Goldstein [20]. Miklavcic and Wang [21] were the first to investigate the viscous flow over a shrinking sheet, followed by Fang et al. [22], who studied the viscous flow over an unsteady shrinking sheet with mass transfer. These authors have shown that from physical point of view, vorticity of the shrinking sheet is not confined within a boundary layer, and the flow is unlikely to exist unless adequate suction or injection on the boundary is imposed. Later, the study regarding shrinking sheet are extended and investigated for various types of fluid and physical properties. Hayat et al. [23] investigated the three-dimentional rotating flow induced by a shrinking sheet for suction, while Aman and Ishak [24] studied the flow and heat transfer over a permeable shrinking sheet with partial slip. Next, Rohni et al. [25] studied the flow and heat transfer at a stagnation-point over an exponentially shrinking vertical sheet with suction, while Rahman et al. [26] solved the problem of steady boundary layer flow of a nanofluid past a permeable exponentially shrinking surface with convective surface condition using Buongiorno's model. The study of heat and mass transfer flow due to permeable shrinking sheet with radiation was done by Mat Yasin et al. [27]. Recently, Mishra et al. [28] studied the free convective micropolar fluid flow and heat transfer over a shrinking sheet while Goyal et al. [29] discussed the heat and mass transfer of free convective micropolar fluid over a shrinking sheet.

Besides [22], all studies mentioned above consider the steady state problem, where the velocity and other properties such as pressure at every point do not depend upon time. Steady flow is preferred by engineers because it is easier to control. However, the study of unsteady boundary layer flow is much more important, because all boundary layer problems that occur in real-world practice are depending on time. Surma Devi et al. [30] discussed the flow, heat and species transport due to the unsteady, three-dimensional flow caused the stretching of a flat surface. Wang [31] investigated the exact solutions of the unsteady Navier-Stokes equations. The unsteady boundary layer flow due to a stretching surface in a rotating fluid has been studied by Nazar et al. [32]. Besides, Roşca and Pop [33] investigated the unsteady viscous flow over a curved stretching/shrinking surface with mass suction. Next, the study of unsteady nanofluid flow and heat transfer using Buongiorno model was explained by Sheikholeslami et al. [34] while the unsteady heat and mass transfer of nanofluid flow was studied by Khan and Azam [35]. Very recently, Khan et al. [36] explained the unsteady three-dimensional nanofluid flow with heat and mass transfer while Waini et al. [37] solved the unsteady flow and heat transfer past stretching/shrinking sheet in a hybrid nanofluid.

The purpose of this paper is to study the boundary layer flow due to the unsteady, three-dimensional laminar flow of a viscous fluid caused by a permeable stretching/shrinking sheet. The governing partial differential equations (PDE) are

transformed into a system of ordinary differential equations (ODE) by using an appropriate similarity transformation, and then solved numerically with "bvp4c" function in MATLAB. Stability analysis is performed to determine the stability of the multiple solutions obtained.

17.2 Problem Formulation

17.2.1 The Governing Equations

In this study, we consider the unsteady three-dimensional boundary layer flow of a viscous fluid past a permeable stretching/shrinking flat surface in an otherwise quiescent fluid. A locally orthogonal set of coordinates (x, y, z) is chosen with the origin O in the plane of the shrinking sheet. The $x-$ and $y-$coordinates are in the plane of the shrinking sheet, while the $z-$coordinate is measured in the perpendicular direction to the shrinking surface. It is assumed that the flat surface is stretching/shrinking continuously in both $x-$ and $y-$directions with the velocities $u(x,t) = u_w(x,t)$ and $v(y,t) = v_w(y,t)$, respectively. It is also assumed that the mass flux velocity is $w = w_0(t)$, where $w_0(t) < 0$ is for suction and $w_0(t) > 0$ is for injection or withdrawal of the fluid. Under these conditions, the boundary layer equations are expressed as [30]

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} = 0, \tag{17.1}$$

$$\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} + w\frac{\partial u}{\partial z} = \nu\frac{\partial^2 u}{\partial z^2}, \tag{17.2}$$

$$\frac{\partial v}{\partial t} + u\frac{\partial v}{\partial x} + v\frac{\partial v}{\partial y} + w\frac{\partial v}{\partial z} = \nu\frac{\partial^2 v}{\partial z^2}, \tag{17.3}$$

along with the initial and boundary conditions

$$\begin{aligned} &t < 0 : u(x,y,z) = 0,\ v(x,y,z) = 0,\ w(x,y,z) = 0 \text{ for any } x, y, z, \\ &t \geq 0 : u = u_w(x,t) = \frac{\lambda a x}{1-\alpha t},\ v = v_w(y,t) = \frac{\lambda b y}{1-\alpha t}, \\ &\qquad w(t) = \frac{w_0}{\sqrt{1-\alpha t}} \ \text{ at } \ z = 0, \\ &\qquad u(x,y,z) \to 0,\ v(x,y,z) \to 0 \ \text{ as } z \to \infty, \end{aligned} \tag{17.4}$$

where u, v and w are the velocity components along the $x-$, $y-$ and $z-$axes, respectively, t is the time, a and b are positive constants, α is the parameter showing the unsteadiness of the problem, ν is the kinematic viscosity of the fluid and λ is the stretching ($\lambda > 0$) or shrinking ($\lambda < 0$) parameter.

17.2.2 The Similarity Transformation

Following [30], we now introduce the following similarity variables

$$\begin{aligned} &u = \frac{ax}{1-\alpha t} f'(\eta),\ v = \frac{by}{1-\alpha t} g'(\eta), \\ &w = -\sqrt{\frac{a\nu}{1-\alpha t}}\left(f(\eta) + c g(\eta)\right),\ \eta = \sqrt{\frac{a/\nu}{1-\alpha t}}\, z, \end{aligned} \tag{17.5}$$

where primes denote the differentiation with respect to η. Substituting the similarity variables (17.5) into Eqs. (17.1)-(17.3), it is found that (17.1) is satisfied, while Eqs. (17.2) and (17.3) are reduced to the following ordinary differential equations

$$f''' + (f + cg)\, f'' - f'^2 - \beta \left(f' + \frac{\eta}{2} f'' \right) = 0, \tag{17.6}$$

$$g''' + (f + cg)\, g'' - cg'^2 - \beta \left(g' + \frac{\eta}{2} g'' \right) = 0, \tag{17.7}$$

and the boundary conditions (17.4) become

$$\begin{aligned} &f(0) = s,\ g(0) = 0,\ f'(0) = \lambda,\ g'(0) = \lambda, \\ &f'(\eta) \to 0,\ g'(\eta) = 0 \ \text{ as } \eta \to \infty, \end{aligned} \tag{17.8}$$

where $c = \frac{b}{a}$ is the ratio of the surface velocity gradients along the y- and x- directions, $s = -\frac{1-\alpha t}{\sqrt{a\nu}} w_0(t)$ is the surface mass transfer parameter with $s > 0$ for suction and $s < 0$ for injection, and $\beta = \frac{\alpha}{a}$ is the unsteadiness parameter.

17.2.3 The Quantities of Physical Interest

The quantities of physical interest are the local skin friction coefficients C_{fx} and C_{fy}, which are defined as

$$C_{fx} = \frac{2\tau_{wx}}{\rho u_w^2},\ C_{fx} = \frac{2\tau_{wy}}{\rho v_w^2}, \tag{17.9}$$

where τ_{wx} and τ_{wy} are the shear stresses in the $x-$ and $y-$directions of the shrinking sheet, which are given by

$$\tau_{wx} = \mu \left(\frac{\partial u}{\partial z} \right)_{z=0},\ \tau_{wy} = \mu \left(\frac{\partial v}{\partial z} \right)_{z=0}, \tag{17.10}$$

Substituting (17.5) into (17.10) and using (17.9), we obtain

$$\mathrm{Re}_x^{1/2}\, C_{fx} = 2f''(0),\ \mathrm{Re}_y^{1/2}\, C_{fy} = 2g''(0), \tag{17.11}$$

where $\mathrm{Re}_x = u_w(x,t)x/\nu_f$ and $\mathrm{Re}_y = v_w(y,t)y/\nu_f$ are the local Reynolds numbers based on the velocities $u_w(x,t)$ and $v_w(y,t)$, respectively.

17.3 Stability Analysis

In the previous section, we have mentioned about the existence of dual solutions, which categorized as upper branch for first solution, and lower branch for second solution. Weidman et al. [38] and Roşca and Pop [39] have shown in their papers that the second (lower branch) solutions are unstable, while the first (upper branch) solutions are stable and physically realizable. The stability of both branches can be shown by performing a stability analysis which is important in order to determine which solution is physically useful in practice since the existence of the non-unique solutions of the problem. Thus, this can be helpful for engineers to save more time in deciding which solution is practically meaningful for them. This analysis has also been done by previous researchers, such as Merkin [40], Weidman and Sprague [41], Mahapatra and Nandy [42], Nazar et al. [43], Naga et al. [44], Bakar et al. [45], Hamid et al. [46] and others.

Following [38], a new dimensionless time variable τ is introduced. The use of τ is associated with an initial value problem and is consistent with the question of which solution or branch will be obtained in practice (physically realizable).

Therefore, based on (17.5) and τ, we introduce the following new similarity variables

$$\begin{aligned} &u = \frac{ax}{1-\alpha t} f'(\eta,\tau),\ v = \frac{by}{1-\alpha t} g'(\eta,\tau),\ \eta = \sqrt{\frac{a}{\nu(1-\alpha t)}}z, \\ &w = -\sqrt{\frac{a\nu}{1-\alpha t}}\left(f(\eta,\tau) + cg(\eta,\tau)\right),\ \tau = \frac{at}{1-\alpha t}, \end{aligned} \tag{17.12}$$

By differentiating (17.12), we have the following

$$\begin{aligned} &\frac{\partial \eta}{\partial t} = \frac{\alpha}{1-\alpha t}\frac{\eta}{2},\ \frac{\partial \tau}{\partial t} = \frac{a}{(1-\alpha t)^2}, \\ &\frac{\partial u}{\partial t} = \frac{a^2 x}{(1-\alpha t)^2}\left[\frac{\alpha}{a}\frac{\eta}{2}\frac{\partial^2 f}{\partial \eta^2} + \frac{1}{1-\alpha t}\frac{\partial^2 f}{\partial \eta \partial \tau} + \frac{\alpha}{a}\frac{\partial f}{\partial \eta}\right], \\ &\frac{\partial v}{\partial t} = \frac{aby}{(1-\alpha t)^2}\left[\frac{\alpha}{a}\frac{\eta}{2}\frac{\partial^2 g}{\partial \eta^2} + \frac{1}{1-\alpha t}\frac{\partial^2 g}{\partial \eta \partial \tau} + \frac{\alpha}{a}\frac{\partial g}{\partial \eta}\right], \\ &\frac{\partial u}{\partial x} = \frac{a}{1-\alpha t}\frac{\partial f}{\partial \eta},\ \frac{\partial v}{\partial x} = 0,\ \frac{\partial u}{\partial y} = 0,\ \frac{\partial v}{\partial y} = \frac{b}{1-\alpha t}\frac{\partial g}{\partial \eta}, \\ &\frac{\partial u}{\partial z} = \frac{ax}{1-\alpha t}\sqrt{\frac{a}{\nu(1-\alpha t)}}\frac{\partial^2 f}{\partial \eta^2},\ \frac{\partial v}{\partial z} = \frac{by}{1-\alpha t}\sqrt{\frac{a}{\nu(1-\alpha t)}}\frac{\partial^2 g}{\partial \eta^2}, \\ &\frac{\partial^2 u}{\partial z^2} = \frac{ax}{1-\alpha t}\frac{a}{\nu(1-\alpha t)}\frac{\partial^3 f}{\partial \eta^3},\ \frac{\partial^2 v}{\partial z^2} = \frac{by}{1-\alpha t}\frac{a}{\nu(1-\alpha t)}\frac{\partial^3 g}{\partial \eta^3}, \end{aligned} \tag{17.13}$$

Substituting (17.13) into (17.2) and (17.3) yield the following

$$\frac{\partial^3 f}{\partial \eta^3} + (f+cg)\frac{\partial^2 f}{\partial \eta^2} - \left(\frac{\partial f}{\partial \eta}\right)^2 - \beta\left(\frac{\partial f}{\partial \eta} + \frac{\eta}{2}\frac{\partial^2 f}{\partial \eta^2}\right) - \frac{1}{1-\alpha t}\frac{\partial^2 f}{\partial \eta \partial \tau} = 0, \tag{17.14}$$

$$\frac{\partial^3 g}{\partial \eta^3} + (f+cg)\frac{\partial^2 g}{\partial \eta^2} - c\left(\frac{\partial g}{\partial \eta}\right)^2 - \beta\left(\frac{\partial g}{\partial \eta} + \frac{\eta}{2}\frac{\partial^2 g}{\partial \eta^2}\right) - \frac{1}{1-\alpha t}\frac{\partial^2 g}{\partial \eta \partial \tau} = 0, \tag{17.15}$$

along with the boundary conditions

$$f(0,\tau) = s,\quad g(0,\tau) = 0,\quad \frac{\partial f}{\partial \eta}(0,\tau) = \lambda,\quad \frac{\partial g}{\partial \eta}(0,\tau) = \lambda, \tag{17.16}$$

$$\frac{\partial f}{\partial \eta}(\eta,\tau) \to 0,\quad \frac{\partial g}{\partial \eta}(\eta,\tau) \to 0 \quad \text{as } \eta \to \infty. \tag{17.17}$$

To test the stability of the steady flow solution $f(\eta) = f_0(\eta)$ and $g(\eta) = G_0(\eta)$ satisfying the boundary-value problem (17.1)-(17.4), we write [38, 39]

$$f(\eta,\tau) = f_0(\eta) + e^{-\sigma\tau}F(\eta,\tau),\ g(\eta,\tau) = g_0(\eta) + e^{-\sigma\tau}G(\eta,\tau), \tag{17.18}$$

where σ is an unknown eigenvalue parameter, while $F(\eta,\tau)$ and $G(\eta,\tau)$ are small relatives to $f_0(\eta)$ and $g_0(\eta)$. By differentiating (17.18), we have

$$\frac{\partial}{\partial \eta}f(\eta,\tau) = f_0'(\eta) + e^{-\sigma\tau}\frac{\partial}{\partial \eta}F(\eta,\tau),$$

$$
\begin{aligned}
&\frac{\partial^2}{\partial\eta^2}f(\eta,\tau) = f_0''(\eta) + e^{-\sigma\tau}\frac{\partial^2}{\partial\eta^2}F(\eta,\tau),\\
&\frac{\partial^3}{\partial\eta^3}f(\eta,\tau) = f_0'''(\eta) + e^{-\sigma\tau}\frac{\partial^3}{\partial\eta^3}F(\eta,\tau),\\
&\frac{\partial^2}{\partial\eta\partial\tau}f(\eta,\tau) = -\sigma e^{-\sigma\tau}\frac{\partial}{\partial\eta}F(\eta,\tau)e^{-\sigma\tau}\frac{\partial^2}{\partial\eta\partial\tau}F(\eta,\tau),\\
&\frac{\partial}{\partial\eta}g(\eta,\tau) = g_0'(\eta) + e^{-\sigma\tau}\frac{\partial}{\partial\eta}G(\eta,\tau),\\
&\frac{\partial^2}{\partial\eta^2}g(\eta,\tau) = g_0''(\eta) + e^{-\sigma\tau}\frac{\partial^2}{\partial\eta^2}G(\eta,\tau),\\
&\frac{\partial^3}{\partial\eta^3}g(\eta,\tau) = g_0'''(\eta) + e^{-\sigma\tau}\frac{\partial^3}{\partial\eta^3}G(\eta,\tau),\\
&\frac{\partial^2}{\partial\eta\partial\tau}g(\eta,\tau) = -\sigma e^{-\sigma\tau}\frac{\partial}{\partial\eta}G(\eta,\tau) + e^{-\sigma\tau}\frac{\partial^2}{\partial\eta\partial\tau}G(\eta,\tau).
\end{aligned}
$$

Substituting above into (17.14) and (17.15) gives

$$
\begin{aligned}
&\frac{\partial^3 F}{\partial\eta^3} + f_0\frac{\partial^2 F}{\partial\eta^2} + f_0''F + cg_0\frac{\partial^2 F}{\partial\eta^2} + cf_0''G - \left(2f_0' - (1+\beta\tau)\,\sigma\right)\frac{\partial F}{\partial\eta}\\
&\qquad -\beta\left(\frac{\partial F}{\partial\eta} - \frac{\eta}{2}\frac{\partial^2 F}{\partial\eta^2}\right) - (1+\beta\tau)\frac{\partial^2 F}{\partial\eta\partial\tau} = 0, \qquad (17.19)\\
&\frac{\partial^3 G}{\partial\eta^3} + f_0\frac{\partial^2 G}{\partial\eta^2} + (F+cG)\,g'' + cg_0\frac{\partial^2 G}{\partial\eta^2} - \left(2cg_0' - (1+\beta\tau)\,\sigma\right)\frac{\partial G}{\partial\eta}\\
&\qquad -\beta\left(\frac{\partial G}{\partial\eta} + \frac{\eta}{2}\frac{\partial^2 G}{\partial\eta^2}\right) - (1+\beta\tau)\frac{\partial^2 G}{\partial\eta\partial\tau} = 0, \qquad (17.20)
\end{aligned}
$$

Meanwhile, substituting above into boundary conditions (17.16) and using (17.8) gives

$$
\begin{aligned}
f(0,\tau) &= s,\\
f_0(0) + e^{-\sigma\tau}F(0,\tau) &= s,\\
(f_0(0)-s) + e^{-\sigma\tau}F(0,\tau) &= 0,\\
e^{-\sigma\tau}F(0,\tau) &= 0,\\
F(0,\tau) &= 0.
\end{aligned}
\qquad
\begin{aligned}
g(0,\tau) &= 0,\\
g_0(0) + e^{-\sigma\tau}G(0,\tau) &= 0,\\
e^{-\sigma\tau}G(0,\tau) &= 0,\\
G(0,\tau) &= 0.
\end{aligned}
$$

$$
\begin{aligned}
\frac{\partial f}{\partial\eta}(0,\tau) &= \lambda,\\
f_0'(0) + e^{-\sigma\tau}\frac{\partial}{\partial\eta}F(0,\tau) &= \lambda,\\
\left(f_0'(0)-\lambda\right) + e^{-\sigma\tau}\frac{\partial}{\partial\eta}F(\eta,\tau) &= 0,\\
e^{-\sigma\tau}\frac{\partial}{\partial\eta}F(\eta,\tau) &= 0,\\
\frac{\partial}{\partial\eta}F(\eta,\tau) &= 0.
\end{aligned}
\qquad
\begin{aligned}
\frac{\partial g}{\partial\eta}(0,\tau) &= \lambda,\\
g_0'(0) + e^{-\sigma\tau}\frac{\partial}{\partial\eta}G(0,\tau) &= \lambda,\\
\left(g_0'(0)-\lambda\right) + e^{-\sigma\tau}\frac{\partial}{\partial\eta}G(\eta,\tau) &= 0,\\
e^{-\sigma\tau}\frac{\partial}{\partial\eta}G(\eta,\tau) &= 0,\\
\frac{\partial}{\partial\eta}G(\eta,\tau) &= 0.
\end{aligned}
$$

$$\frac{\partial f}{\partial \eta}(\eta,\tau) \to 0, \qquad \frac{\partial g}{\partial \eta}(\eta,\tau) \to 0,$$
$$f_0'(\eta) + e^{-\sigma\tau}\frac{\partial}{\partial \eta}F(\eta,\tau) \to 0, \qquad g_0'(\eta) + e^{-\sigma\tau}\frac{\partial}{\partial \eta}G(\eta,\tau) \to 0,$$
$$e^{-\sigma\tau}\frac{\partial}{\partial \eta}F(\eta,\tau) \to 0, \qquad e^{-\sigma\tau}\frac{\partial}{\partial \eta}G(\eta,\tau) \to 0,$$
$$\frac{\partial}{\partial \eta}F(\eta,\tau) \to 0. \qquad \frac{\partial}{\partial \eta}G(\eta,\tau) \to 0.$$

Together, they form the following boundary condition

$$\begin{aligned} &F(0,\tau) = 0,\ G(0,\tau) = 0,\ \frac{\partial}{\partial \eta}F(\eta,\tau) = 0,\ \frac{\partial}{\partial \eta}G(\eta,\tau) = 0, \\ &\frac{\partial}{\partial \eta}F(\eta,\tau) \to 0,\ \frac{\partial}{\partial \eta}G(\eta,\tau) \to 0 \quad \text{as } \eta \to \infty. \end{aligned} \tag{17.21}$$

Furthermore, we investigate the stability of the steady flow $f_0(\eta)$ and $g_0(\eta)$ by setting $\eta = 0$ [38]. Hence, $F(\eta) = F_0(\eta)$ and $G(\eta) = G_0(\eta)$ in Eqs. (17.19) and (17.20) identify the initial growth or decay of the solution (17.18). To test our numerical procedure, we then solve the linear eigenvalue problem

$$\begin{aligned} F_0''' + (f_0 + cg_0)\,F_0'' + (F_0 + cG_0)\,f_0'' - \left(2f_0' - \sigma\right)F_0' \\ -\beta\left(F_0' - \frac{\eta}{2}F_0''\right) = 0, \end{aligned} \tag{17.22}$$

$$\begin{aligned} G_0''' + (f_0 + cg_0)\,G_0'' + (F_0 + cG_0)\,g_0'' - \left(2cg_0' - \sigma\right)G_0' \\ -\beta\left(G_0' + \frac{\eta}{2}G_0''\right) = 0, \end{aligned} \tag{17.23}$$

along with the following boundary conditions:

$$\begin{aligned} &F_0(0) = 0,\ F_0'(0) = 0,\ G_0(0) = 0,\ G_0'(0) = 0, \\ &F_0'(\eta) \to 0,\ G_0(\eta) \to 0 \text{ as } \eta \to \infty. \end{aligned} \tag{17.24}$$

For particular values of the governing parameters involved, such as β, S and λ, the stability of the corresponding steady flow solution $f_0(\eta)$ and $g_0(\eta)$ are determined by the smallest eigenvalue σ. Solutions of the linear eigenvalue problem (17.22) and (17.23) give an infinite set of eigenvalues $\sigma_1 < \sigma_2 < \sigma_3 < \ldots$; if the smallest eigenvalue σ_1 is positive $(\sigma_1 \geq 0)$, then there is an initial decay of disturbances and the flow is stable, and if σ_1 is negative $(\sigma_1 < 0)$, then there is an initial growth of disturbances, which indicates that the flow is unstable.

Harris et al. [47] suggested that the range of possible eigenvalues can be obtained by relaxing a boundary condition on $F_0(\eta)$ or $G_0(\eta)$. In this paper, we relax the condition $G_0'(\eta) \to 0$ as $\eta \to \infty$ and for a fixed value of σ, we solve the system of equations (17.22) and (17.23) subject to the boundary conditions (17.24), along with the new boundary condition $G_0''(0) = 1$.

17.4 Results and Discussion

The system of nonlinear ordinary differential equations (17.6)-(17.7) subject to the boundary conditions (17.8) were solved numerically using the "bvp4c" function in MATLAB [48, 49]. The numerical results for the reduced skin friction coefficients

obtained in this study are compared with those of Surma Devi et al. [30] for validation. The comparisons, which is displayed in Table 17.1, are found to be in excellent agreement, and thus we are confident that the present numerical method is accurate.

Table 17.1: Numerical comparison with [30] when $c = 1$, $S = 0$ and boundary conditions $f'(0) = 1$, $g'(0) = 0.5$.

	[30]		Present result	
β	$-f''(0)$	$-g''(0)$	$-f''(0)$	$-g''(0)$
1	1.3814	0.6261	1.3814	0.6261
0.5	1.2407	0.5480	1.2407	0.5480
0	1.0931	0.4652	1.0931	0.4652
−0.5	0.9430	0.3809	0.9430	0.3809
−1	0.7912	0.2956	0.7912	0.2956

Table 17.2: Dual solutions of $f''(0)$ and $g''(0)$ for different values of β when $S = 2.5$, $\lambda = -1$ and $c = 0.5$

	Upper branch		Lower branch	
β	$f''(0)$	$g''(0)$	$f''(0)$	$g''(0)$
0	1.7824	1.9493	0.8315	1.6452
−2	0.9787	1.2405	−0.5351	0.5270
−4	0.1010	0.4846	−1.4710	−0.3242
−6	−0.8830	−0.3362	−2.1985	−1.0453
−8	−2.2062	−1.3536	−2.5299	−1.5334

Dual solutions in this study are obtained by setting 2 different initial guesses for the missing values of $f''(0)$ and $g''(0)$. Table 17.2 displays both first (upper branch) and second (lower branch) solutions of $f''(0)$ and $g''(0)$ for different values of β when $S = 2.5$, $\lambda = -1$ and $c = 0.5$. It can be observed that the values of $f''(0)$ and $g''(0)$ from the upper branch are decreasing with the decrease of β, up until they have reach zero and become negative. This implies that there is velocity overshoot near the shrinking sheet with a higher velocity in the fluid than the wall velocity [22]. Meanwhile, different trend can be seen for the lower branch, where the values keep decreasing, and then increase as β is getting closer to -8. This trend can also be seen in Figs. 17.1 and 17.2, which also show that the solutions of $f''(0)$ and $g''(0)$ can be positive for both branches when the value of suction parameter S is small ($S < 2.4$). Furthermore, it can also be seen that the solutions keep decreasing with the decrease of β and S.

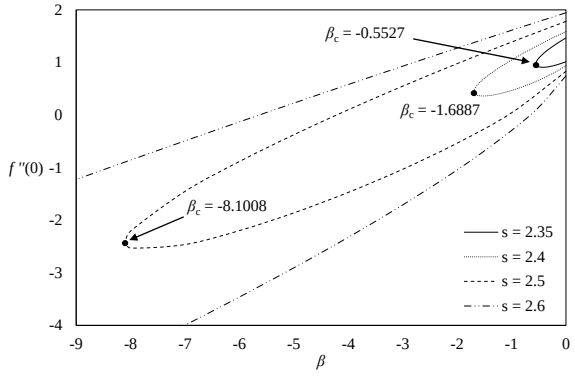

Figure 17.1: Variation of $f''(0)$ with β for different values of S when $c = 0.5$ and $\lambda = -1$

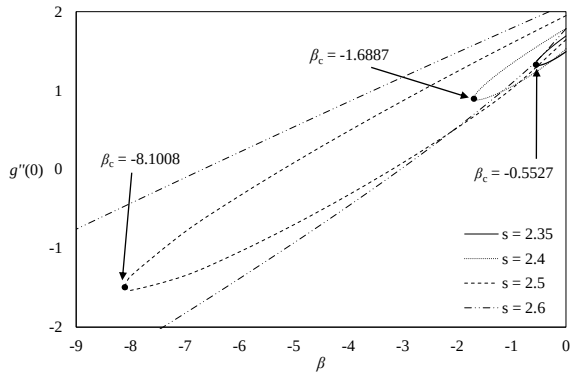

Figure 17.2: Variation of $g''(0)$ with β for different values of S when $c = 0.5$ and $\lambda = -1$

Figs. 17.1-17.4 represent the solution domain for Eqs. (17.6)-(17.7) with boundary conditions (17.8). From these figures, it can be seen that there are two (dual) solutions for each $f''(0)$ and $g''(0)$, and they exist for a certain range of β and λ. When β and λ equal to a certain value, say $\beta = \beta_c$ and $\lambda = \lambda_c$, where β_c and λ_c are the critical values of β and λ, respectively, there is only one solution. There is no solution when the values of β and λ are less than their critical values, beyond which the boundary layer separates from the surface (which is known as boundary layer separation) and the solution based upon the boundary layer approximations are not possible. From these figures, we notice that the upper branch solution is always larger than the lower branch solutions for the same value of β and λ, which is consistent with the numerical results displayed in Table 17.2.

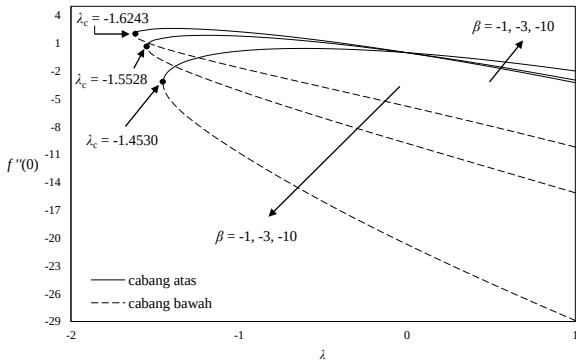

Figure 17.3: Variation of $f''(0)$ with λ for different values of β when $c = 0.5$ and $S = 3$

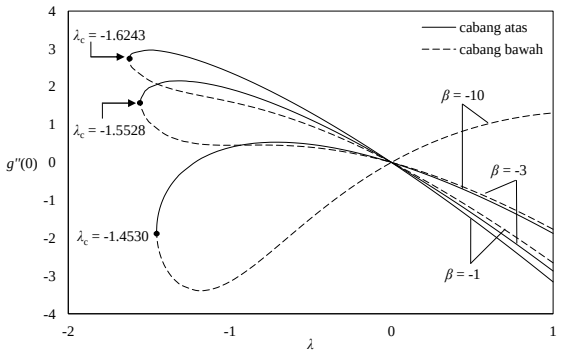

Figure 17.4: Variation of $g''(0)$ with λ for different values of β when $c = 0.5$ and $S = 3$

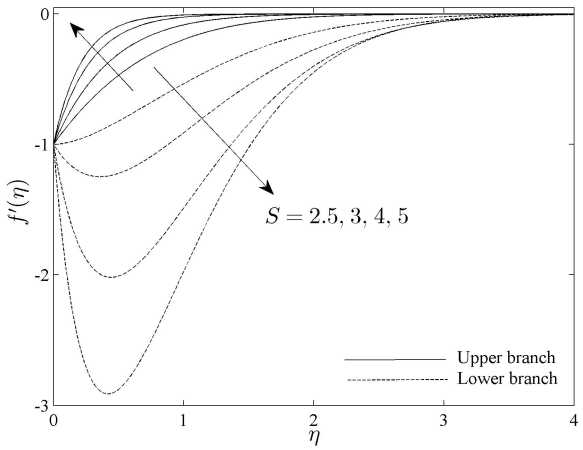

Figure 17.5: Velocity profiles $f'(\eta)$ for different values of S when $\beta = -1$, $c = 0.5$ and $\lambda = -1$

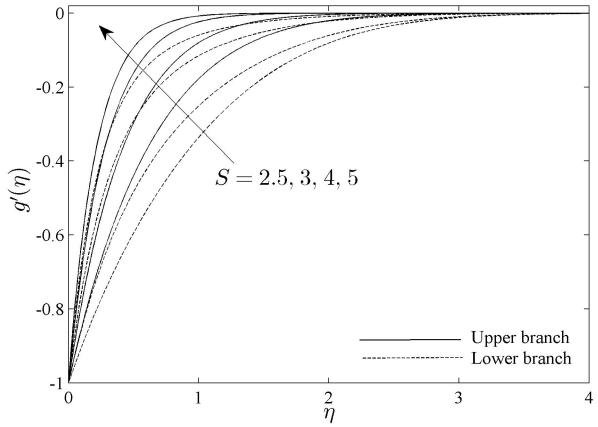

Figure 17.6: Velocity profiles $g'(\eta)$ for different values of S when $\beta = -1$, $c = 0.5$ and $\lambda = -1$

Further, velocity profiles $f'(\eta)$ and $g'(\eta)$ for some values of S when $\beta = -1$, $\lambda = -1$ and $c = 0.5$ are illustrated in Figs. 17.5 and 17.6, respectively. The boundary layer thicknesses from both figures are seen to be smaller with higher values of S, which happened because suction reduces drag force to avoid boundary layer separation. We also notice that the boundary layer thickness for the lower branch solution is larger than the upper branch solution. Both of these profiles satisfy the far field boundary conditions (17.8) asymptotically, which support the validity of the numerical results obtained and the existence of the dual solutions shown in Figs. 17.1-17.4 and Table 17.2.

Table 17.3: Smallest eigenvalues σ_1 for several values of β and S when $c = 0.5$ and $\lambda = -1$

β	S	σ_1 (Upper branch)	σ_1 (Lower branch)
-3	2.44	0.2415	-0.2358
	2.5	0.8146	-0.7548
	2.6	1.3421	-1.1924
-10	2.52	0.3617	-0.3569
	2.55	0.9406	-0.9091
	2.6	1.4857	-1.4097

To determine the stability of the dual solutions obtained, a stability analysis is performed by determining an unknown eigenvalue σ on Eqs. (17.22)-(17.23) along with the boundary conditions (17.24). This analysis was done by using the same numerical computation used in this study, which is "bvp4c" function. The smallest eigenvalue for some values of β and S when $c = 0.5$ and $\lambda = -1$ are presented in Table 17.3. It can be observed that the upper branch solutions have positive σ while the lower branch solutions have negative σ. Thus, we conclude that the first (upper branch) solution is stable and physically realizable while the second (lower branch) solution is not.

17.5 Conclusion

We have numerically studied the problem of unsteady three-dimensional boundary layer flow of a viscous fluid past a permeable stretching/shrinking sheet. The governing system of nonlinear partial differential equations are reduced to a system of ordinary differential equations by using similarity transformation, and then solved numerically using "bvp4c" function in MATLAB. A comparison has been made with previous literature and it shows an excellent agreement. Dual solutions are found for both stretching and shrinking cases when suction parameter The solutions for lower branch is always smaller than the upper branch. The magnitude of reduced skin friction coefficients are found to increase with the increase of suction parameters and the decrease of unsteadiness parameter. The boundary layer thicknesses are seen to be smaller with higher values of suction parameter. A stability analysis was performed to determine the stability of the dual solutions obtained, and it can be concluded that the first (upper branch) solution is stable and physically realizable, while the second (lower branch) solution is unstable.

Acknowledgement

This work was supported by research grant (GP-IPM/2018/9619000) from Universiti Putra Malaysia.

Bibliography

[1] Sakiadis BC (1961) Boundary-layer behavior on continuous solid surfaces: I. Boundary-layer equations for two-dimensional and axisymmetric flow. *AIChE Journal* **7**, 26–28.

[2] Sakiadis BC (1961) Boundary-layer behavior on continuous solid surfaces: II. The boundary layer on a continuous flat surface. *AIChE Journal* **7(2)**, 221–225.

[3] Tsou FK, Sparrow EM, Goldstein RJ (1967) Flow and heat transfer in the boundary layer on a continuous moving surfaces. *Int. J. Heat Mass Transfer* **10**, 219–235.

[4] Crane LJ (1970) Flow past a stretching plate. *Zeitschrift für angewandte Mathematik und Physik* **21(4)**, 645–647.

[5] McLeod JB, Rajagopal KR (1987) On the uniqueness of flow of a Navier-Stokes fluid due to a stretching boundary. *Archive for Rational Mechanics and Analysis* **98(4)**, 385–393.

[6] Gupta PS, Gupta AS (1977) Heat and mass transfer on a stretching sheet with suction or blowing. *Can. J. Chem. Eng.* **55**, 744-–746.

[7] Wang CY (1984) The three-dimensional flow due to a stretching flat surface. *Physics of Fluids* **27(8)**, 1915–1917.

[8] Banks WHH (1983) Similarity solutions of the boundary-layer equations for a stretching wall. *Journal de Mecanique Theorique et Appliquee* **2**, 375–392.

[9] Rajagopal KR, Na TY, Gupta AS (1984) Flow of a viscoelastic fluid over a stretching sheet. *Rheologica Acta* **23**, 213–215.

[10] Chen C-K, Char M-I (1988) Heat transfer of a continuous, stretching surface with suction or blowing. *Journal of Mathematical Analysis and Applications* **135(2)**, 568–580.

[11] Magyari E, Keller B (1999) Heat and mass transfer in the boundary layers on an exponentially stretching continuous surface. *J. Phys. D: Appl. Phys.* **32(5)**, 577–585.

[12] Magyari E., Keller B (2000). Exact solutions for self-similar boundary-layer flows induced by permeable stretching walls. *European Journal of Mechanics - B/Fluids* **19(1)**, 109–122.

[13] Nadeem S, Haq RU, Khan Z (2014) Numerical study of MHD boundary layer flow of a Maxwell fluid past a stretching sheet in the presence of nanoparticles. *Journal of the Taiwan Institute of Chemical Engineers* **45(1)**, 121–126.

[14] Bhattacharyya K, Layek GC (2014) Magnetohydrodynamic boundary layer flow of nanofluid over an exponentially stretching permeable sheet. *Physics Research International* **2014**, 1–12.

[15] Mabood F, Khan WA, Ismail AIM (2015) MHD boundary layer flow and heat transfer of nanofluids over a nonlinear stretching sheet: A numerical study. *Journal of Magnetism and Magnetic Materials* **374**, 569–576.

[16] Turkyilmazoglu M (2016) Flow of a micropolar fluid due to a porous stretching sheet and heat transfer *International Journal of Non-Linear Mechanics* **83**, 59–64.

[17] Wu L (2017) Effect of mass transfer induced velocity slip on heat transfer of viscous gas flows over stretching/shrinking sheets. *International Journal of Thermal Sciences* **112**, 165–173.

[18] El-Mistikawy T (2018) MHD flow and heat transfer due to a linearly stretching sheet with induced magnetic field: Exact solution. *arXiv preprint* **arXiv:1803.08561**.

[19] Shamshuddin MD, Thirupathi T, Satya Narayana PV (2019) Micropolar fluid flow induced due to a stretching sheet with heat source/sink and surface heat flux boundary condition effects. *Journal of Applied and Computational Mechanics* **5**, 816–826.

[20] Goldstein S (2006) On backward boundary layers and flow in converging passages. *Journal of Fluid Mechanics* **21(1)**, 33–45.

[21] Miklavcic M, Wang CY (2006) Viscous flow due to a shrinking sheet. *Quart. Appl. Math.* **64**, 283–290.

[22] Fang T-G, Zhang J, Yao S-S (2009) Viscous flow over an unsteady shrinking sheet with mass transfer. *Chinese Physics Letters* **26(1)**, 014703.

[23] Hayat T, Abbas Z, Javed T, Sajid M (2009) Three-dimensional rotating flow induced by a shrinking sheet for suction. *Chaos, Solitons & Fractals* **39(4)**, 1615–1626.

[24] Aman F, Ishak A (2010) Boundary layer flow and heat transfer over a permeable shrinking sheet with partial slip. *Journal of Applied Sciences Research* **6(8)**, 1111–1115.

[25] Rohni AM, Ahmad S, Pop I (2014) Flow and heat transfer at a stagnation-point over an exponentially shrinking vertical sheet with suction. *International Journal of Thermal Sciences* **75**, 164–170.

[26] Rahman MM, Rosca AV, Pop I (2015) Boundary layer flow of a nanofluid past a permeable exponentially shrinking surface with convective boundary condition using Buongiorno's model. *International Journal of Numerical Methods for Heat & Fluid Flow* **25(2)**, 299–319.

[27] Mat Yasin MH, Ishak A, Pop I (2016) MHD heat and mass transfer flow over a permeable stretching/shrinking sheet with radiation effect. *Journal of Magnetism and Magnetic Materials* **407**, 235–240.

[28] Mishra SR, Khan I, Al-Mdallal QM, Asifa T (2018) Free convective micropolar fluid flow and heat transfer over a shrinking sheet with heat source. *Case Studies in Thermal Engineering* **11**, 113–119.

[29] Goyal M, Gurjar G, Tailor V (2019) Heat and mass transfer of free convective micropolar fluid flow over a shrinking sheet. *Available at SSRN 3462956.*

[30] Surma Devi CD, Takhar HS, Nath G (1986) Unsteady, three-dimensional, boundary-layer flow due to a stretching surface, *Int. J. Heat Mass Transfer* **29**, 1996–1999.

[31] Wang CY (1989) Exact solutions of the unsteady Navier-Stokes equations. *Applied Mechanics Reviews* **42(11S)**, S269–S282.

[32] Nazar R, Amin N, Pop I (2004) Unsteady boundary layer flow due to a stretching surface in a rotating fluid. *Mechanics Research Communications* **31(1)** 121–128.

[33] Roşca NC, Pop I (2015) Unsteady boundary layer flow over a permeable curved stretching/shrinking surface. *European Journal of Mechanics - B/Fluids* **51** 61–67.

[34] Sheikholeslami M, Ganji DD, Rashidi MM (2016) Magnetic field effect on unsteady nanofluid flow and heat transfer using Buongiorno model. *Journal of Magnetism and Magnetic Materials* **416** 164–173.

[35] Khan M and Azam M (2017) Unsteady heat and mass transfer mechanisms in MHD Carreau nanofluid flow. *Journal of Molecular Liquids* **225** 554–562.

[36] Khan AS, Nie Y, Shah Z, Dawar A, Khan W, Islam S (2018) Three-dimensional nanofluid flow with heat and mass transfer analysis over a linear stretching surface with convective boundary conditions. *Applied Sciences (Switzerland)* **8** 2244.

[37] Eaini I, Ishak A, Pop I (2019) Unsteady flow and heat transfer past a stretching/shrinking sheet in a hybrid nanofluid. *International Journal of Heat and Mass Transfer* **136** 288–297.

[38] Weidman PD, Kubitschek DG, Davis AMJ (2006) The effect of transpiration on self-similar boundary layer flow over moving surfaces. *International Journal of Engineering Science* **44(11–12)**, 730–737.

[39] Roşca AV, Pop I (2013) Flow and heat transfer over a vertical permeable stretching/shrinking sheet with a second order slip. *International Journal of Heat and Mass Transfer* **60**, 355–364.

[40] Merkin JH (1986) On dual solutions occurring in mixed convection in a porous medium. *Journal of Engineering Mathematics* **20(2)**, 171–179.

[41] Weidman PD, Sprague MA (2011) Flows induced by a plate moving normal to stagnation-point flow. *Acta Mech.* **219(3–4)**, 219–229.

[42] Mahapatra TR, Nandy SK (2011) Stability analysis of dual solutions in stagnation-point flow and heat transfer over a Power-law shrinking surface. *International Journal of Nonlinear Science* **12**, 86–94.

[43] Nazar R, Noor A, Jafar K, Pop I (2014) Stability analysis of three-dimensional flow and heat transfer over a permeable shrinking surface in a Cu-water nanofluid. *International Journal of Mathematical, Computational, Physical and Quantum Engineering* **8(5)**, 776–782.

[44] Naganthran K, Nazar R, Pop I (2017) Stability analysis of impinging oblique stagnation-point flow over a permeable shrinking surface in a viscoelastic fluid. *International Journal of Mechanical Sciences* **131-132**, 663–671.

[45] Abu Bakar NA, Bachok N, Arifin NM, Pop I (2018) Stability analysis on the flow and heat transfer of nanofluid past a stretching/shrinking cylinder with suction effect. *Results in Physics* **9**, 1335–1344.

[46] Hamid M, Usman M, Khan ZH, Ahmad R, Wang W (2019) Dual solutions and stability analysis of flow and heat transfer of Casson fluid over a stretching sheet. *Physics Letters A* **383**, 2400-2408.

[47] Harris SD, Ingham DB, Pop I (2009) Mixed convection boundary-layer flow near the stagnation point on a vertical surface in a porous medium: Brinkman model with slip. *Transport in Porous Media* **77(2)**, 267–285.

[48] Kierzenka J, Shampine LF (2001) A BVP solver based on residual control and the Maltab PSE. *CM Trans. Math. Softw.* **27(3)**, 299–316.

[49] Shampine LF, Gladwell I, Thompson S (2003) Solving ODEs with MATLAB. Cambridge University Press.