MALAYSIAN JOURNAL OF SCIENCE

Vol. 38 • Special Issue (1) • 2019

3rd International Conference of Mathematical Sciences and Statistics (ICMSS2018)

MJS Guest Editors
Ong Seng Huat
Angelina Chin Yan Mui
Wong Kok Bin
Khang Tsung Fei
Loo Tee How

ICMSS2018 Editors
Chuei Yee Chen
Fudziah Ismail
Lai Soon Lee

JURNAL SAINS MALAYSIA

MJS

ISSN 1394 - 3065

The Malaysian Journal of Science is indexed or cited in the following Scientific Databases: Elsevier Bibliographic Databases (ACI, Scopus, EMBASE, Compendex, GEOBASE, EMBiology, Elsevier BIOBASE, FLUIDEX and World Textiles); CAB Abstracts and Chemical Abstracts Service Database

www.mjs.um.edu.my

http://www.myjurnal.my/public/browse-journal-view.php?id=194

Selected papers from the

3rd International Conference of Mathematical Sciences and Statistics (ICMSS2018)

Putrajaya, MALAYSIA. 6th - 8th February 2018.

We are honoured to bring you this compilation of carefully selected papers presented at the 3rd International Conference on Mathematical Sciences and Statistics (ICMSS2018) that was held in Putrajaya, Malaysia from 6th to 8th February 2018.

The primary focus of this conference was to bring together academicians, researchers and scientists for knowledge sharing in various areas of Mathematics and Statistics. The ICMSS2018 served as a good platform for the scientific community where almost 200 participants met to exchange ideas. During the three days of conference, the researchers presented the most recent discoveries over a wide spectrum of Mathematics and Statistics as well as established networking for possible joint researches and collaborations.

The editors would like to thank the authors who have contributed to the volume. A special thanks goes to the reviewers for their constructive comments and feedback. We also express our gratitude to every staff of the Department of Mathematics for their unwavering commitment as the conference organizer and the management of Faculty of Science, Universiti Putra Malaysia for their unfailing support towards ICMSS2018.

Lastly, we are most indebted for the generous support given by Institute for Mathematical Research (INSPEM), Malaysian Mathematical Sciences Society (PERSAMA), Malaysian Institute of Statistics (ISM), OEMS Intipakar Corporation Sdn. Bhd. and Bizit Systems (M) Sdn. Bhd.

26 October 2018

Guest Editors
Chuei Yee Chen
Fudziah Ismail
Lai Soon Lee

Malaysian Journal of Science Special Issue (1) 2019: 1-18

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

BASIC EPIDEMIC MODEL OF DENGUE TRANSMISSION USING THE FRACTIONAL ORDER DIFFERENTIAL EQUATIONS

Nur 'Izzati Hamdan[1*] & Adem Kilicman[1,2,3]

[1]Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[2]Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[3]Department of Electrical and Electronic Engineering, Istanbul Gelisim University, Avcilar, 34310, Istanbul, Turkey.
*Corresponding author: izzati.hamdan@gmail.com
Received: 27th Oct 2018 Revised: 27th Oct 2018 Accepted: 19th Dec 2018
DOI : https://doi.org/10.22452/mjs.sp2019no1.1

ABSTRACT Dengue is normally emerging in tropical and subtropical countries and now has become a serious health problem. In Malaysia, dengue is considered endemic for the past few years. A reliable mathematical model of dengue epidemic is crucial to provide some means of interventions in controlling the spread of the disease. Many mathematical models have been proposed and analyzed in the literature, but very little of them used fractional order derivative in analyzing the dengue transmission. In this paper, a study on a basic fractional order epidemic model of dengue transmission is conducted using the SIR-SI model, including the aquatic phase of the vector. The population size of the human is assumed to be constant. The threshold quantity R0 is attained by the next generation matrix method. The preliminary result of the study is presented. It has shown that the disease-free equilibrium is locally asymptotically stable when R0 < 1, and unstable when R0 > 1. In other words, the dengue disease is eliminated if R0 < 1, and it approaches a positive endemic equilibrium if R0 > 1. Finally, some numerical results are presented based on the real data in Malaysia in 2016.

Keywords: Dengue, Epidemic, Fractional order, Stability, Reproduction number

ABSTRAK Denggi berlaku di negara-negara tropika dan sub-tropika dan kini telah menjadi masalah kesihatan utama. Di Malaysia, denggi telah pun disifatkan sebagai endemik untuk beberapa tahun yang lepas. Model matematik bagi wabak denggi yang boleh diandalkan adalah sangat penting sebagai intervensi dalam mengawal denggi dari terus merebak. Banyak model matematik telah dikemukakan dan dianalisa, namun tidak banyak daripada kajian yang ada menggunakan pembezaan melalui tertib pecahan dalam menganalisa penularan denggi. Di dalam artikel ini, kajian terhadap model penularan wabak denggi menggunakan kaedah tertib pecahan dijalankan. Ianya berdasarkan model SIR-SI serta mengambil kira fasa kehidupan vektor di dalam air. Saiz populasi manusia dianggap tetap. Nilai ambang R_0, diperolehi menggunakan kaedah *the* *next-generation matrix*. Penemuan awal kajian ini dibentangkan. Ianya telah diperlihatkan bahawa titik keseimbangan bebas penyakit adalah stabil apabila $R_0 < 1$, dan tidak stabil apabila $R_0 > 1$. Dalam kata lainnya, penyakit denggi dapat dihapuskan jika $R_0 < 1$, dan ianya akan mendekati titik keseimbangan endemic untuk $R_0 > 1$. Pada penghujung artikel ini, beberapa keputusan berangka dibentangkan berdasarkan data sebenar di Malaysia pada tahun 2016.

Kata kunci: Denggi, Kestabilan, Nombor pembiakan, Tertib pecahan, Wabak

INTRODUCTION

Dengue is listed second after malaria, as the most prevalent vector-borne disease in the world, caused by any of four closely related virus serotypes named DEN-1, DEN-11, DEN-III, and DEN-IV. The chance of contracting dengue virus has increased dramatically since the mid-90s. Now, dengue is becoming endemic in more than hundred countries (World Health Organization (WHO)).

Dengue virus is transferred to one individual by the bite of an infected *Aedes* female mosquito. Individuals who recuperate from one of the serotypes become constantly immune to it. However, they may become partially-immune or temporarily-immune or both to the other serotypes. Up to date, there is still no vaccine available for dengue patients. The efforts to prevent and control the spread of the dengue virus focus merely on the vector population, for instance, the implementation of the larvicides, residual treatment and space sprays.

Many mathematical models have been established in the literature to study the mechanism of the dengue transmission (Esteva & Vargas, 1998) (Esteva & Yang, 2015) (Syafruddin & Noorani, 2012). Most of these models were developed using the system of ordinary differential equation.

The integer order systems are ideal in modelling system like Markov system where the current state does not depend on the previous state. However, Sardar et al. (Sardar, Rana, & Chattopadhyay, 2014) explained that based on the entomological studies on the dengue transmission, memory and associative learning in the mosquito population and awareness in human population show a significant role in the transmission (McCall & Kelly, 2002). Since the behaviour of the trajectories of the fractional operator is non-local, it is one of the best ways to incorporate memory into the dynamical process (Agarwal, Ntouyas, Ahmad, & Alhothuali, 2013).

The aims of this study are to formulate a fractional order dengue epidemic model and to study the stability of the disease-free equilibrium point. The generalized Adams-Bashforth-Moulton algorithm has been used to solve the system of differential equations (Garrappa, 2015). For our purposes, we have followed the dengue disease outbreak in Malaysia for the year 2016. In this paper, we presented the preliminary result of our study.

This paper is structured as follows. In section 2, the formulation of the model is given. The basic definition of the fractional calculus is included followed by the construction of the proposed model. Disease-free equilibrium point and its stability are discussed in section 3. Section 4 is reserved for numerical results for the model and discussions. The conclusion is presented in section 5.

FORMULATION OF THE MODEL

The history of fractional calculus started in 1695 when L'Hospitals asked in a letter to Leibniz for the nth derivative, $\frac{D^n x}{Dx^n}$, what is the result for when $n = 1/2$. For more than two centuries, fractional calculus is only popular around pure mathematics branch. However, a few years back, the study of fractional calculus has become researcher's interest in many application fields such as in engineering, genetics, biology, statistics, and even finance. Researchers believe that fractional calculus can give more genuine understandings of the real-world phenomena (Diethelm K., 2010).

There are many descriptions of fractional order differential equations introduced in the literature. Among the famous one are the Riemann-Liouville, Caputo and Grünwald-Letnikov. In this paper, the Caputo's definition is used as the initial conditions of the integer order differential equation can be taken without encountering any problems in obtaining the solutions (Diethelm & Freed, 2002).

Definition 1. *The Caputo derivative of fractional order* α *of a function* $f: R^+ \rightarrow R$ *is defined by the following equation*

$$D_C^{\alpha} f(x) = \frac{1}{\Gamma(n-\alpha)} \int_a^x \frac{d^n f}{d\epsilon^n}(\varepsilon)(x-\varepsilon)^{n-\alpha-1}\, d\varepsilon$$

where α *is the order of the derivative with* $n\text{-}1 < \alpha < n$ *and* $n = [\alpha] + 1$. $\Gamma(n\text{-}\alpha)$ *is the Euler gamma function.*

In the formulation of the model, the total number of human and mosquito population is assumed to be constant. We also assume that the infection is produced by only one serotype of dengue viruses. The dynamics of female *Aedes* mosquito includes aquatic phase, A_m, and adult mosquito stage. The adult stage is divided into two compartments which are susceptible M_s and infectious M_i. The total human population is partitioned into three compartments that are susceptible H_s, infectious H_i, and recovered H_r individuals. The derivation of the fractional order differential equation for the proposed host-vector model is based on the ordinary differential equation introduced by Bailey for a single serotype dengue transmission (Bailey, 1975) and SIR model established by Kermack and McKendrick (Kermack & McKendrick, 1996). The fractionalization is done following the work of Diethelm (Diethelm, 2013). The governing equation is as follows:

$$\begin{aligned}
D^{\alpha} A_m &= q\phi\left(1-\frac{A_m}{C}\right)M-(\sigma_A+\mu_A)A_m \\
D^{\alpha} M_s &= \sigma_A A_m-\frac{b^{\alpha}\beta_m}{H}M_sH_i-\mu_m M_s \\
D^{\alpha} M_i &= \frac{b^{\alpha}\beta_m}{H}M_sH_i-\mu_m M_i \\
D^{\alpha} H_s &= \mu_h(H-H_s)-\frac{b^{\alpha}\beta_h}{H}H_sM_i \\
D^{\alpha} H_i &= \frac{b^{\alpha}\beta_h}{H}H_sM_i-(\gamma_h+\mu_h)H_i \\
D^{\alpha} H_r &= \gamma_h H_i-\mu_h H_r
\end{aligned} \tag{1}$$

where the description of the parameters used in the model can be found in Table 1.

The effective contact rate to human $b\beta_h$, is defined as the average number of contacts per day that result in infection if the mosquito is infected. On the other hand, the effective contact rate $b\beta_{m,}$ is the average number of contacts per day that successfully transfer the infection (virus) to the vector. All parameters are assumed to be positive as the system monitors the dynamic of the human population.

Table 1: Parameter description of system (1) and their reasonable range of values.

Parameter	Biological meaning	Range of values
q	Proportion of eggs that results in female mosquito	0-1
ϕ	Oviposition rate	0-11.2 per day
σ_A	Transition rate from aquatic stage to adult	0-0.19 per day
μ_A	Per capita mortality rate of aquatic stage	0.01-0.47 per day
$1/\mu_m$	Average lifespan of adult mosquito	0-42 days
$1/\mu_h$	Average lifespan of human	50-75 years
b	The biting rate	0-1 per day
β_m	Transmission probability from human to vector	0.375
β_h	Transmission probability from vector to human	0.375
γ_h	Recovery rate in the human population	0.083-0.33 per day
C	Mosquito carrying capacity	-

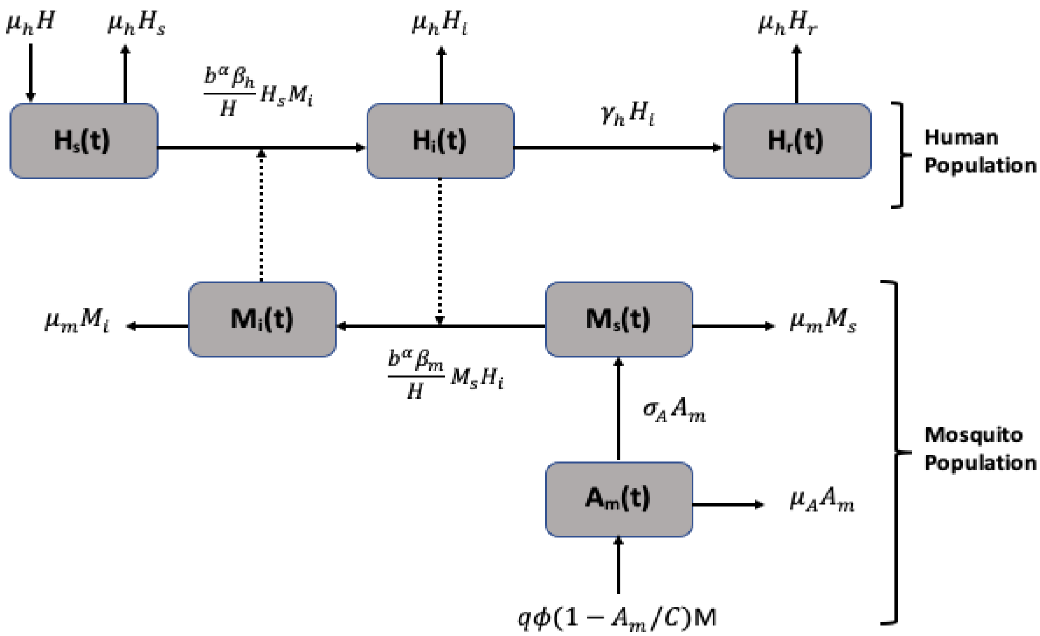


Figure 1: The schematic diagram of the dengue transmission model (1)

DISEASE-FREE EQUILIRIUM POINT AND LOCAL STABILITY

With the condition of $N_h = H = H_s + H_i + H_r$, we have $H_r = H\text{-}H_s + H_i$. Thus, we can now write down the corresponding system for human population exclusive of the H_r differential equation.

$$
\begin{aligned}
D^\alpha H_s &= \mu_h (H - H_s) - \frac{b^\alpha \beta_h}{H} H_s M_i \\
D^\alpha H_i &= \frac{b^\alpha \beta_h}{H} H_s M_i - (\gamma_h + \mu_h) H_i \\
D^\alpha A_m &= q\phi\left(1 - \frac{A_m}{C}\right) M - (\sigma_A + \mu_A) A_m \qquad (2) \\
D^\alpha M_s &= \sigma_A A_m - \frac{b^\alpha \beta_m}{H} M_s H_i - \mu_m M_s \\
D^\alpha M_i &= \frac{b^\alpha \beta_m}{H} M_s H_i - \mu_m M_i
\end{aligned}
$$

Let the set Ω be the region of biological interest that is positively invariant with respect to model (2).

$$\Omega = \left\{(A_m, M_s, M_i, H_s, H_i) \in \mathbb{R}_+^5 : H_s + H_i \le H, A_m \le kH, M_s + M_i \le mH\right\},$$

where k is the number of larvae per human and m is the number of female mosquito per human. System (2) can be written as follows:

$$\frac{dX}{dt} = M(X)X + F, \tag{3}$$

where here, $\frac{dX}{dt} = D^{\alpha}(A_m, M_s, M_i, H_s, H_i)$ and $F = (0,0,0,\mu_h H, 0)$. Meanwhile, $M(X)$ is the matrix with all off-diagonal entries are nonnegative value, and known as Metzler matrix. The Metzler matrix is in the following form

$$M(X) = \begin{pmatrix} \frac{-q\phi(M_s + M_i)}{C} - (\sigma_A + \mu_A) & q\phi & q\phi & 0 & 0 \\ \sigma_A & -\frac{b^{\alpha}\beta_m}{H}H_i - \mu_m & 0 & 0 & 0 \\ 0 & \frac{b^{\alpha}\beta_m}{H}H_i & -\mu_m & 0 & 0 \\ 0 & 0 & 0 & -\mu_h - \frac{b^{\alpha}\beta_h}{H}M_i & 0 \\ 0 & 0 & 0 & \frac{b^{\alpha}\beta_h}{H}M_i & -(\gamma_h + \mu_h) \end{pmatrix}$$

Since $F \geq 0$, we can say that system (3) is positively invariant in R_+^5. Meaning that, any solution of the equation departing from an initial state in the positive orthant R_+^5 will remain forever in R_+^5. This implies that the closed set Ω is positively invariant with respect to the system (2) (Rodrigues et al., 2012).

Now we let $\nu = (A_m, M_s, M_i, H_s, H_i) \in R_+^5 : H_s + H_i \le H, A_m \le kH, M_s + M_i \le mH$. Since $m \geq \frac{\sigma_A}{\mu_A}k$, it can be shown that ν is positively invariant with respect to (3). Hence, we suppose that m and k are chosen such that,

$$m \geq \frac{\sigma_A}{\mu_A} k \tag{4}$$

To evaluate the equilibrium point, we let $D^{\alpha}A_m = 0, D^{\alpha}M_s = 0, D^{\alpha}M_i = 0, D^{\alpha}H_s = 0, D^{\alpha}H_i = 0$. The fractional order system (2) has two disease-free equilibrium (DFE). The first one is the straightforward trivial equilibrium E_0. Here, $A_m = 0$, indicates of the none existence of mosquito population, hence, no dengue outbreaks. This DFE is not of our interest since this state does not represent the real situation for the region that we considered in the real data set.

$$E_0 = (0,0,0,H,0)$$

The second DFE obtained is given by

$$E_1 = (\bar{A}_m, \bar{M}_s, 0, H, 0)$$

where $\bar{A}_m$ and $\bar{M}_s$are given by the following equation:

$$\bar{A}_m = C(1-\frac{1}{R_m}) \quad \text{and} \quad \bar{M}_s = \frac{\sigma_A \bar{A}_m}{\mu_m}$$

Hence,

$$E_1 = (C(1 - \frac{1}{R_m}), \frac{C\sigma_A}{\mu_m}(1 - \frac{1}{R_m}), 0, H, 0)$$

where $R_m = \frac{q\phi\sigma_A}{\mu_m(\sigma_A+\mu_A)}$. R_m represent the basic offspring of the mosquito population. This is biologically interesting when $R_m > 1$, in which mosquito population exist. This is the case when disease is eradicated without taking any action on the eliminating of the mosquito population.

The basic reproduction number R_0, is a very important threshold quantity in investigating the stability of the equilibrium point of the system. In general, R_0 is biologically defined as the expected number of secondary infections in a completely susceptible population. The interpretations of R_0 in terms of the stability are as follows

- If $\mathrm{R}_0 < 1$, the transmission sequences are not self-contained, hence, incapable to cre ate a major epidemic.
- If $\mathrm{R}_0 = 1$, the infectious is maintained, no major outbreaks.
- If $\mathrm{R}_0 > 1$, the number of infected individu als will increase as infectious take over, he nce, the disease will persist

In this paper, the next generation matrix is used to obtain the R_0 for system (2).

$$R_0^2 = \frac{b^{2\alpha}\beta_m\beta_h}{(\gamma_h + \mu_h)\mu_m}\frac{\bar{M}_s}{H}$$

$$R_0 = \sqrt{\frac{b^{2\alpha}\beta_m\beta_h}{(\gamma_h + \mu_h)\mu_m}\frac{\bar{M}_s}{H}} \tag{5}$$

The calculated R_0 is not only depend on the biting rate parameter as in the integer order case but also a memory dependent threshold quantity since $\mathrm{R}_0 \propto \mathrm{b}^\alpha$ (Hamdan & Kilicman, 2018). It can be observed that if the order α is decreasing, the value of b^α will also be decreasing. This result in a less efficient the average bite rate by each mosquito per day (Sardar, Rana, & Chattopadhyay, 2014).

Theorem 1. *The trivial disease-free equilibrium* E_0*, is locally asymptotically stable if* $\mathrm{R}_0 < 1$ *and the condition of* $\mathrm{R}_\mathrm{m} < 1$ *is satisfied, otherwise it is unstable.*

Proof. The disease-free equilibrium is locally asymptotically stable if all the eigenvalues, $\lambda_\mathrm{i}, \mathrm{i} = 1, 2 \ldots, 5$ of the Jacobian matrix $\mathrm{J}(\mathrm{E}_0)$ satisfy the following condition (Matignon, 1996).

$$|\arg(\lambda_i)| > \frac{\alpha\pi}{2}$$

The Jacobian matrix of the system evaluated at the equilibrium point E_0:

$$J(E_0) = \begin{pmatrix} -(\sigma_A + \mu_A) & 0 & 0 & 0 & 0 \\ \sigma_A & -\mu_m & 0 & 0 & 0 \\ 0 & 0 & -\mu_m & 0 & 0 \\ 0 & 0 & -b^\alpha \beta_h & -\mu_h & 0 \\ 0 & 0 & b^\alpha \beta_h & 0 & -(\gamma_h + \mu_h) \end{pmatrix}$$

It is clearly shown that all eigenvalues are negative real parts;

$-(\sigma_A + \mu_A), -\mu_m, -\mu_h, -(\gamma_h + \mu_h)$. Hence, E_0 is locally asymptotically stable.

Theorem 2. *The DFE* E_1, *is locally asymptotically stable if* $R_0 < 1$ *and is unstable if* $R_0 > 1$.

Proof. Following the stability condition by Matignon, the Jacobian matrix of the system (2) evaluated at the equilibrium point E_1, we have

$$J(E_1) = \begin{pmatrix} -R_m(\sigma_A + \mu_A) & 0 & 0 & 0 & 0 \\ \sigma_A & -\mu_m & 0 & 0 & \frac{b^\alpha \beta_m}{H} \bar{M}_s \\ 0 & 0 & -\mu_m & 0 & \frac{b^\alpha \beta_m}{H} \bar{M}_s \\ 0 & 0 & -b^\alpha \beta_h & -\mu_h & 0 \\ 0 & 0 & b^\alpha \beta_h & 0 & -(\gamma_h + \mu_h) \end{pmatrix}$$

The calculated eigenvalues are $\lambda_1 = -R_m(\sigma_A + \mu_A), \lambda_2 = -\mu_m, \lambda_3 = -\mu_h$. The other roots are determined by solving the quadratic equation:

$$\lambda^2 + (\mu_m + \gamma_h + \mu_h)\lambda + \mu_m(\gamma_h + \mu_h)(1 - R_0) = 0$$

Obviously, the roots are negative real parts for when $R_0 < 1$. Hence, proved that E_1 is locally asymptotically stable if $R_0 < 1$ and is unstable if $R_0 > 1$, and the condition of $R_m > 1$ is satisfied.

NUMERICAL RESULTS AND DISCUSSION

In the case of fractional order differential equation, there is no general analytical method in solving the nonlinear systems. In fact, the fractional differential equations are difficult to solve numerically, compared to the integer order ODE. However, several analytical method and numerical schemes have been developed to solve the system. For instance, Diethelm and Freed introduced a new algorithm known as FracPECE, the generalization of the classical PECE type method (Diethelm & Freed, 1999).

In this study, the values related to the human describe the reality of an infected period in Malaysia. The data used is based on the dengue fever cases recorded in Malaysia for 2016, taken from The Ministry of Health Malaysia (From the Desk of the Director-General of Health Malaysia), (Dengue Situation Updates 2016, n.d.). However, for the mosquito population we have selected information from various sources due to the limited sources available in Malaysia.

In this work, we have not established any new numerical scheme. We used the available Matlab code (fde12) developed by Garrappa (Garrappa, 2015), based on the work of Diethelm and Freed. As of in the classical integer order derivative, we used Matlab ODE solver, ode45. The numerical simulations are done using the parameter values in Table 2 for the system (2) (see (Hamdan & Kilicman, 2019) for references). The initial conditions for the problem: $H_{s0} = H\text{-}H_{i0}, H_{i0} = 2511, A_{m0} = kH, M_{s0} = mH$, with the final time, $t_f = 52$ weeks. The initial values are chosen based on the real data in Malaysia for year 2016.

However, the choice of the parameter values is carefully selected to suit the demographic factor of Malaysia.

Table 2: Parameter values

Parameter	**Values**
H	31200000
q	0.8
ϕ	7.5
σ_A	0.08
μ_A	0.25
μ_m	0.11
μ_h	0.0000365
b	0.8
β_m	0.375
β_h	0.375
γ_h	0.334
C	kH
k	3
m	6

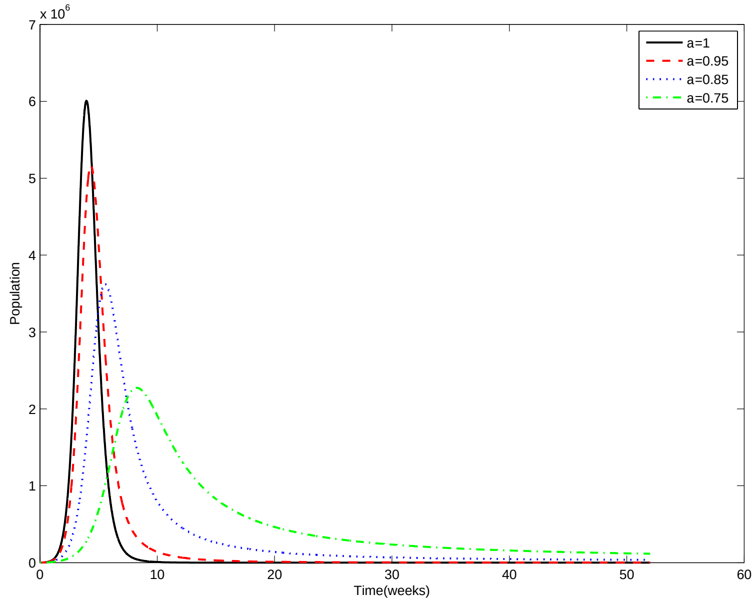


Figure 2: Solution to the classical model versus the solution of the fractional model (2) with various value of α for the infected human population.

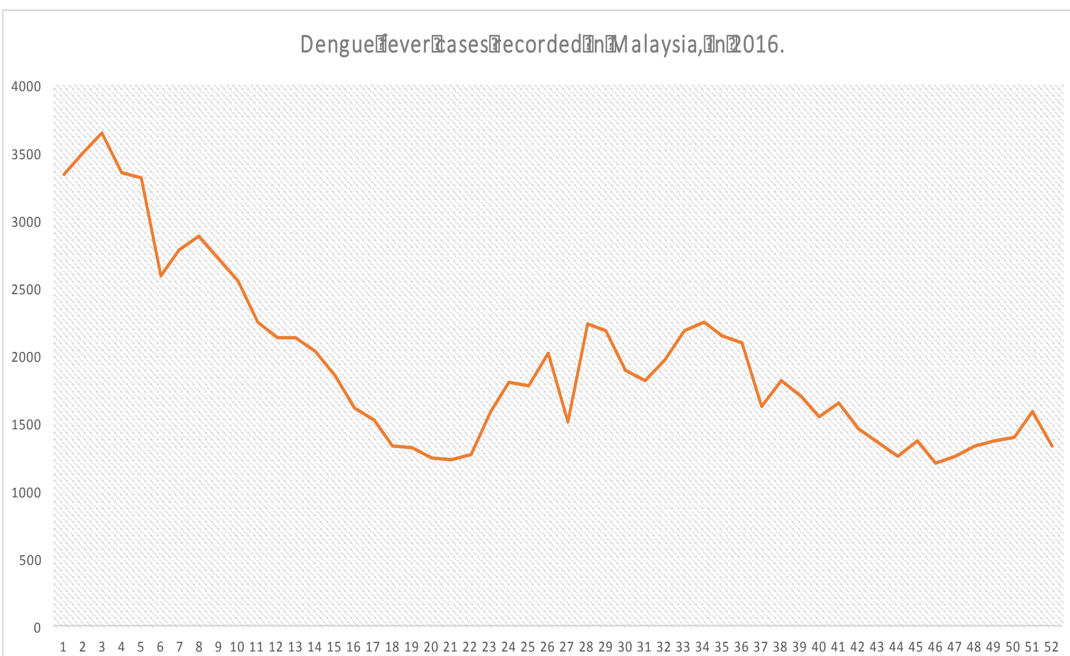


Figure 3: Number of dengue cases recorded in Malaysia, in 2016.

Figure 2 represents the trajectories of the infected human population for the classical integer order derivative and fractional order derivative with various values of α and Figure 3 is the plot of the dengue fever cases in Malaysia (2016). We can see through Figure 2, the maximum peak of the infected human solution for both integer order ODE and fractional order differential equation is in between 0 to 10 weeks, which agreed well with the real data value. We observed that in the fractional order case, the maximum peak of the infectious human population significantly drops as the value of order decreasing. However, the solutions required more time to achieve their steady state. In other words, one can say that the spread of the dengue disease can be reduced but needs more time to be eradicated. The order α can be represented as an index of memory, thus, $\alpha \to 0$, indicates an increase of memory in both human and mosquito population.

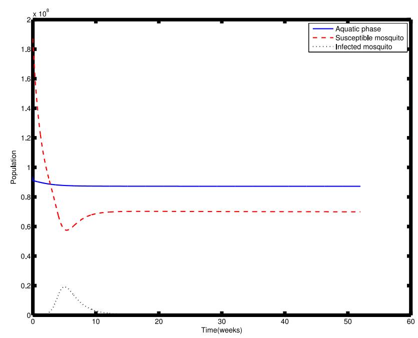


Figure 4a: Solution of the fractional order vector model, for $\alpha = 0.95$.

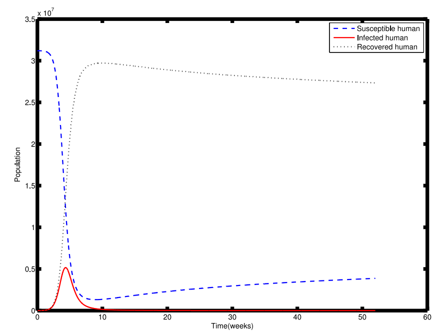


Figure 4b: Solution of the fractional order for the the human model, for $\alpha = 0.95$.

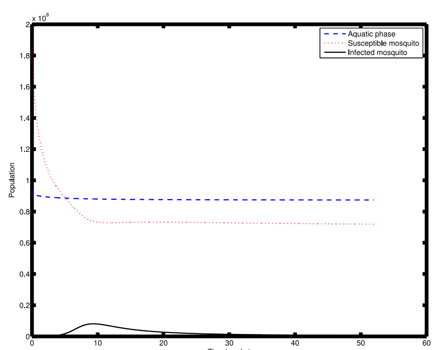


Figure 5a: Solution of the fractional order for the vector model, for $\alpha = 0.75$.

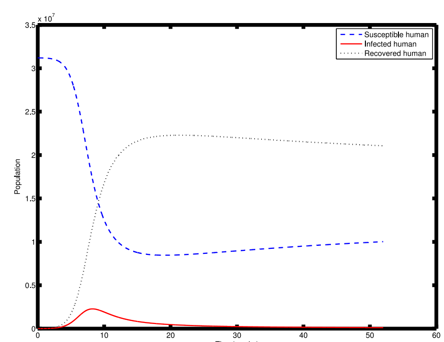


Figure 5b: Solution of the fractional order for the human model, for $\alpha = 0.75$.

Figure 4a, 4b and 5a, 5b revealed that the solution of the susceptible human population in the fractional order does not fall drastically in a relatively short period for the small value of α. We observed that the speed of convergence for the fractional order system is slower than the integer order system, and this explained the significance of time needed for the population to reach the disease-free state. Meanwhile, in Figure 6a, 6b and Figure 7a, 7b, it is shown that the solutions converge to the disease-free equilibrium for $\alpha = 0.5, 0.55$ in a very short period of time. These results verified the local stability theorem in section 3 for the disease-free equilibrium. However, we noticed that the order α, gives a significant effect on the results of the stability of the system. The required time to eliminate the disease clearly depends on the memory effect on the host and vector population, at least, to this study.

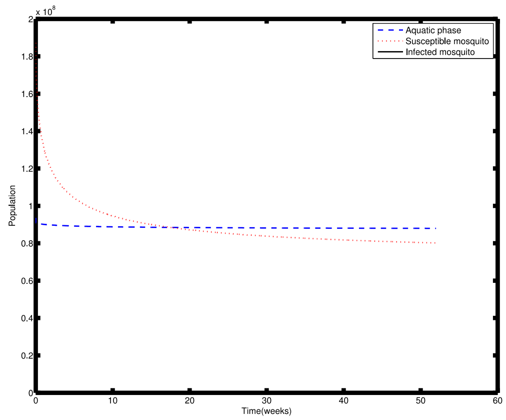


Figure 6a: Solution of the fractional order for the vector model, for $\alpha = 0.55$.

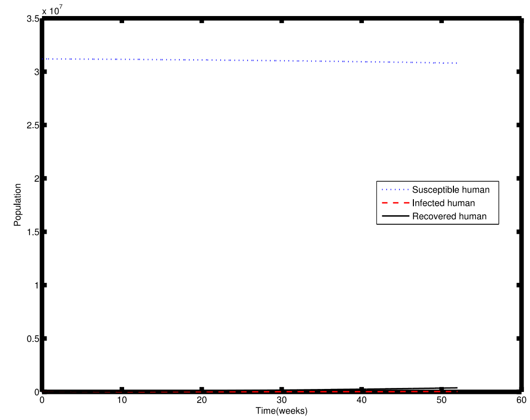


Figure 6b: Solution of the fractional order for the human model, for $\alpha = 0.5$.

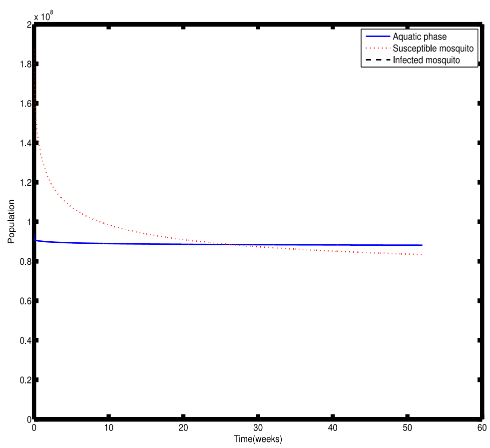


Figure 7a: Solution of the fractional order for the vector model, for $\alpha = 0.5$.

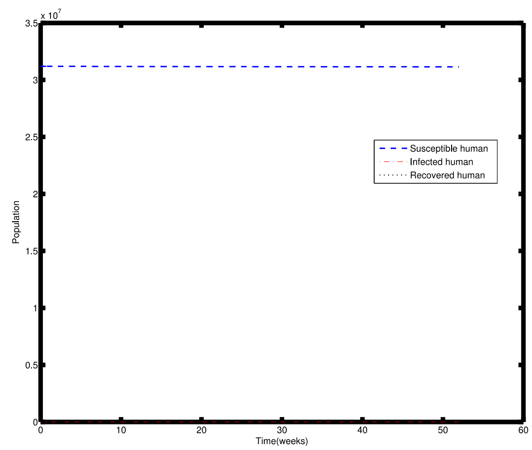


Figure 6b: Solution of the fractional order for human model, for $\alpha = 0.5$.

CONCLUSION

In this paper, we have proposed and analyzed a fractional order dengue epidemic model. The hypothetical and epidemiological findings of this study are summarized as follows:

- The disease-free equilibrium of system (2) is locally asymptotically stable if the corresponding $R_0<1$.
- Although the equilibrium points of fractional order system and integer order system are equal, the solution of the fractional order model approaches the fixed point over a longer period (Demirci, Unal, & Ozalp, 2011).
- The memory of the mosquito and human population represented by the order of the differential equation has a significant effect on the period of the disease elimination.
- An increase in order (memory) of human and mosquito population ($\alpha \to 0$), will decrease the abundance of infectious mosquito, hence, reduce the dengue transmission in a population.

The obtained results are significant with a real-life situation of dengue transmission. For instance, mosquito does not casually feed on host blood, but they somehow use their experience about human spot and defensiveness in selecting the host (Sardar et al., 2014). Thus, plenty of time and effort are needed to completely eradicate the disease, in terms of the elimination of the *Aedes* mosquito, in which reflects the results obtained in Figure 6 and 7.

We can say that from the preliminary results obtained, fractional order derivative gives us a more realistic way to model vector-borne disease dynamics as it possesses memory. In this study, we can conclude that smaller value of α, gives a better approximation in reducing the intensity of the dengue transmission. However, a thorough analysis needs to be done on the parameter values and α value chosen, so that this model can be used to successfully predict the long-term behaviour of the disease, especially in Malaysia. A model of fractional order dengue with control parameters will be our future study. This model will be developed to see how effective the current control strategies used by the government specifically in Malaysia and how does the order α, and control parameter affect the stability of the model.

ACKNOWLEDGEMENTS

This work is supported by the Ministry of Higher Education Malaysia and Universiti Teknologi MARA (UiTM). This work is also partially funded by the Universiti Putra Malaysia providing Putra Grant GP-IPS/2018/9625000.

REFERENCES

(n.d.). Retrieved February 2018, from World Health Organization (WHO): http://www.whho.int/denguecontrol/disease/en.

(n.d.). Retrieved February 2018, from From the Desk of the Director-General of Health Malaysia: https://kpkesihatan.com/2016/01/28/terkini-situasi-denggi-2016/.

Agarwal, R., Ntouyas, S., Ahmad, B., & Alhothuali, M. (2013). Existence of solutions for integro-differential equations of fractional order with nonlocal three-point fractional boundary conditions. *Advances in Difference Equation, 128*.

Bailey, N. (1975). *The Mathematical Theory of Infectious Disease and Its Applications.* London: Griffin.

Demirci, E., Unal, A., & Ozalp, N. (2011). A fractional order SEIR model with density dependent death rate. *Hacettepe University Bulletin of Natural Sciences and Engineering Series B: Mathematics and Statistics, 40*(2), 287-295.

Dengue Situation Updates 2016. (n.d.). Retrieved March 2018, from World Health Organization Western Pacific Region: http://iris.wpro.who.int/handle/10665.1/14182.

Diethelm, K. (2010). *The Analysis of Fractional Differential Equations: An Application-Oriented Exposition Using Differential Operators of Caputo Type.* Springer.

Diethelm, K. (2013). A fractional calculus based model for he simulation of an outbreak of dengue fever. *Nonlinear Dynamics, 71*(4), 613-619.

Diethelm, K., & Freed, A. (1999). The FracPECE Subroutine for the numerical solution of differential equation of fractional order. *Orschung und Wissenschaftliches Rechnen*, (pp. 57-71).

Diethelm, K., & Freed, A. D. (2002). Analysis of fractional differential equations. *Journal of Mathematical Analysis and Applications, 260*(2), 229-248.

Esteva, L., & Vargas, C. (1998). Analysis of dengue transmission model. *Mathematical Biosciences, 15*(2), 131-151.

Esteva, L., & Yang, H. (2015). Assessing the effects of temperature and dengue virus load on dengue transmission. *Journal of Biological Systems, 23*(4).

Garrappa, R. (2015). Trapezoidal methods for fractional equations: Theoretical and computational aspects. *Mathematics and Computers in Simulation, 11*, 96-112.

Hamdan, N., & Kilicman, A. (2018). A fractional order SIR epidemic model for dengue transmission. *Chaos, Solitons and Fractals, 114*, 55-62.

Hamdan, N., & Kilicman, A. (2019). Analysis of the fractional order dengue transmission model: a case study in Malaysia. *Advances in Difference Equations, 2019*, 1-13.

Kermack, W., & McKendrick, A. (1996). A contribution to the mathematical theory of epidemics. *Proceeding of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2*, pp. 963-968.

Matignon, D. (1996). Stability results for fractional differential equations with applications to control processing. *Proceedings of The Computational Engineering in Systems Application, 2*, pp. 963-968.

McCall, P. J., & Kelly, D. W. (2002). Learning and memory in disease vectors. *Trends. Parasitols, 18*(10), 429-433.

Rodrigues, H. S., Monteiro, M. T., Torres, D. F., & Zinober, A. (2012). Dengue disease, basic reproduction number and control. *International Journal of Computer Mathematics, 89*(3), 334-346.

Sardar, T., Rana, S., & Chattopadhyay, J. (2014). A mathematical model of dengue transmission with memory. *Commun Nonlinear Sci Numer Simulat, 22*, 511-525.

Sardar, T., Rana, S., Bhattacharya, S., Al-Khaled, K., & Chattopadhyay, J. (2015). A generic model for a single strain mosquito-transmitted disease with memory on the host and the vector. *Mathematical Biosciences, 263*, 18-36.

Syafruddin, S., & Noorani, M. (2012). SEIR model for transmission of dengue fever in Selangor Malaysia. *International Journal of Modern Physics: Conference Series, 9*, 380-389.

Malaysian Journal of Science Special Issue (1) 2019: 19-32

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6^{th} - 8^{th} February 2018

STABILITY ANALYSIS OF A ROTATING FLOW TOWARD A SHRINKING PERMEABLE SURFACE IN NANOFLUID

Siti Nur Alwani Salleh*, Norfifah Bachok, and Norihan Md Arifin

Department of Mathematics and Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
*Corresponding Author: alwani24salleh@gmail.com
Received: 28^{th} Oct 2018 Revised: 28^{th} Oct 2018 Accepted 19^{th} Dec 2018
DOI: https://doi.org/10.22452/mjs.sp2019no1.2

ABSTRACT The rotating boundary layer flow over a shrinking permeable surface in nanofluid is numerically studied. The similarity transformation is used to transform the partial differential equations into nonlinear ordinary differential equations. Later, these equations are determined by using bvp4c package in the MATLAB software. The numerical results reveal that there is more than one solution called dual solutions obtained for a certain range of the rotation and suction parameters. A stability analysis is performed to determine which solution is stable by depending on the sign of the eigenvalues. Based on this analysis, the results indicate that the upper branch solution (first solution) is linearly stable, while the lower branch solution (second solution) is linearly unstable.

Keywords: Dual solutions, nanofluid, rotating flow, shrinking sheet, stability analysis.

ABSTRAK Aliran putaran lapisan sempadan terhadap permukaan mengecut yang telap di dalam nanobendalir dikaji. Penjelmaan keserupaan digunakan untuk menjelmakan persamaan perbezaan separa kepada persamaan perbezaan biasa tak linear. Kemudian, persamaan ini diselesaikan dengan menggunakan pakej bvp4c dalam perisian MATLAB. Keputusan menunjukkan bahawa terdapat lebih daripada satu penyelesaian yang disebut penyelesaian dwi diperolehi untuk julat tertentu bagi parameter putaran dan sedutan. Analisis kestabilan dijalankan untuk menentukan penyelesaian mana yang stabil dengan bergantung kepada tanda nilai eigen. Berdasarkan analisis ini, keputusan menunjukkan bahawa penyelesaian cabang atas (penyelesaian pertama) adalah stabil, sementara penyelesaian cabang bawah (penyelesaian kedua) adalah tidak stabil.

INTRODUCTION

Along with the development of technology in this day and age, the usage of nanofluid became one of the hot issues to some researchers in fluid mechanics. This issue attracts researchers because conventional heat transfer fluids like ethylene glycol, oil and water have poor thermal performance in a cooling system. By using such fluid as a cooling tool will definitely enhance the manufacturing processes as well as operating costs. This fluid is formed by dispersing some of the nanoparticles into the base fluid which is water. After the discovery of nanofluid by Choi (1995), Bachok et al. (2010, 2012), Reddy et al. (2013), Das et al. (2014), Rosca and Pop (2014), Naramgari and Sulochana (2016) and Othman et al. (2017) have attempted to focus their research on the boundary layer flow of nanofluid using different effects and surfaces. Recently, the nanofluid problem with the presence of rotation in the flow is investigated by Nadeem et al. (2014) using two types of nanoparticles, namely, copper and titania over a stretching surface.

However, up to today, there are still only a few studies regarding a stability analysis of the dual solutions for the boundary layer flow and heat transfer. The idea and procedure to determine the stability of the solutions obtained has been triggered by Merkin (1985). This analysis later was continued by Weidman et al. (2006), Harris et al. (2009), Mahapatra and Nandy (2011), Sharma et al. (2014), Hafidzuddin et al. (2015), Najib et al. (2016) and Yasin et al. (2017). They concluded that the upper branch solution is always stable and physically realizable, while the lower branch solution is not.

The main focus of the present paper is to continue the work of Nadeem et al. (2014) by considering the influence of suction using a different surface, which is the shrinking surface. The effect of the involved parameter is numerically analyzed and has been elaborated in particular for the characteristics of fluid flow and heat transfer. The bvp4c package is implemented in MATLAB software in order to compute the numerical results as well as to confirm the upper branch solution is stable, while the lower branch solution is not.

FORMULATION OF THE PROBLEM

In this study, a steady three-dimensional rotating boundary layer flow in nanofluid past a shrinking sheet at $z = 0$ is considered by taking into account the effect of suction at the surface. The velocity components corresponding to x, y and z directions are given by u, v and w, respectively. $\overline{\Omega}$ is denoted as the angular velocity of the rotating fluid in z direction and T is the temperature of the fluid. Based on the following assumptions, the governing equations for the mass, momentum and energy can be written as:

$$\frac{\partial u}{\partial x}+\frac{\partial v}{\partial y}+\frac{\partial w}{\partial z}=0, \tag{1}$$

$$u\frac{\partial u}{\partial x}+v\frac{\partial u}{\partial y}+w\frac{\partial u}{\partial z}-2\overline{\Omega}v=\frac{\mu_{nf}}{\rho_{nf}}\frac{\partial^2 u}{\partial z^2}, \tag{2}$$

$$u\frac{\partial v}{\partial x}+v\frac{\partial v}{\partial y}+w\frac{\partial v}{\partial z}+2\overline{\Omega}u=\frac{\mu_{nf}}{\rho_{nf}}\frac{\partial^2 v}{\partial z^2}, \tag{3}$$

$$u\frac{\partial T}{\partial x}+v\frac{\partial T}{\partial y}+w\frac{\partial T}{\partial z}=\alpha_{nf}\frac{\partial^2 T}{\partial z^2}, \tag{4}$$

The boundary conditions for the Equations (1)-(4) are

$$u = U(x),\ v = 0,\ w = -w_0,\ T = T_w \ \text{ at } \ z = 0, \qquad u \to 0,\ v \to 0,\ T \to T_\infty \ \text{ as } \ z \to \infty. \tag{5}$$

We assume the surface is being shrunk with the velocity $U(x) = ax$ in which $a < 0$ is a constant, w_0 is the constant mass flux with $w_0 > 0$ for injection, while $w_0 < 0$ for suction. Besides, T_∞ is the temperature outside the boundary layer and T_w is the temperature at the wall. μ_{nf}, α_{nf}, ρ_{nf} and k_{nf} are dynamic viscosity, thermal diffusivity, density and thermal conductivity of nanofluid and k_f is the thermal conductivity of the base fluid. The above mentioned parameters relate to the nanoparticle volume fraction, ϕ are as follows:

$$\mu_{nf} = \frac{\mu_f}{(1-\phi)^{2.5}},\ \alpha_{nf} = \frac{k_{nf}}{(\rho C_p)_{nf}},\ \frac{k_{nf}}{k_f} = \frac{(k_s + 2k_f) - 2\phi(k_f - k_s)}{(k_s + 2k_f) + \phi(k_f - k_s)}, \qquad \rho_{nf} = (1-\phi)\rho_f + \phi\rho_s,\ (\rho C_p)_{nf} = (1-\phi)(\rho C_p)_f + \phi(\rho C_p)_s, \tag{6}$$

where ρC_p refers to volumetric heat capacity, ρ_f and μ_f are the density and dynamic viscosity of the base fluid, respectively, and k_s is the thermal conductivity of solid nanoparticles.

Equation (1) is satisfied and Equations (2)-(4) with the conditions (5) can be written in a simpler form by using the linear similarity transformations below:

$$u = axf'(\eta),\ v = axh(\eta),\ w = -\sqrt{a\nu_f}\, f(\eta),\ \eta = z\sqrt{\frac{a}{\nu_f}},\ \theta(\eta) = \frac{T - T_\infty}{T_w - T_\infty}. \tag{7}$$

Next, Equations (6) and (7) are substituted into Equations (2)-(4) to obtain the following ordinary differential equations below:

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi) + \phi(\rho_s/\rho_f)\right]} f''' + ff'' - f'^2 + 2\Omega h = 0, \tag{8}$$

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi) + \phi(\rho_s/\rho_f)\right]} h'' + fh' - hf' - 2\Omega f' = 0, \tag{9}$$

$$\frac{k_{nf}/k_f}{\Pr\left[(1-\phi) + \phi(\rho C_p)_s/(\rho C_p)_f\right]} \theta'' + f\theta' = 0, \tag{10}$$

and the conditions (5) become

$$f(0)=S,\ f'(0)=-1,\ h(0)=0,\ \theta(0)=1,$$
$$f'(\eta)\to 0,\ h(\eta)\to 0,\ \theta(\eta)\to 0 \text{ as } \eta\to\infty. \tag{11}$$

In the above equations, primes refer to differentiation with respect to similarity variable, η and the Prandtl number is defined as $\Pr=\nu_f/\alpha_f$. Besides that, the rotation and constant mass flux parameters are given by $\Omega=\overline{\Omega}/a$ and S, respectively, where $S<0$ for injection and $S>0$ for suction.

The skin friction coefficients in terms of wall shear stresses and the heat transfer coefficient in terms of Nusselt number can be expressed as:

$$Cf_x=\mu_{nf}(\partial u/\partial z)_{z=0}/\rho(ax)^2=\frac{1}{(1-\phi)^{2.5}}\mathrm{Re}_x^{-1/2}\ f''(0), \tag{12}$$

$$Cf_y=\mu_{nf}(\partial v/\partial z)_{z=0}/\rho(ax)^2=\frac{1}{(1-\phi)^{2.5}}\mathrm{Re}_x^{-1/2}\ h'(0), \tag{13}$$

$$Nu_x=-xk_{nf}(\partial T/\partial z)_{z=0}/k_f(T_w-T_\infty)=\frac{-k_{nf}}{k_f}\mathrm{Re}_x^{1/2}\ \theta'(0), \tag{14}$$

where $\mathrm{Re}_x=Ux/\nu_f$ is the local Reynold number and Nu_x is the local Nusselt number.

FORMULATION FOR STABILITY ANALYSIS

The first step to perform a stability analysis is to consider the problem in unsteady case. Hence, Equations (2)-(4) are substituted by

$$\frac{\partial u}{\partial t}+u\frac{\partial u}{\partial x}+v\frac{\partial u}{\partial y}+w\frac{\partial u}{\partial z}-2\overline{\Omega}v=\frac{\mu_{nf}}{\rho_{nf}}\frac{\partial^2 u}{\partial z^2}, \tag{15}$$

$$\frac{\partial v}{\partial t}+u\frac{\partial v}{\partial x}+v\frac{\partial v}{\partial y}+w\frac{\partial v}{\partial z}+2\overline{\Omega}u=\frac{\mu_{nf}}{\rho_{nf}}\frac{\partial^2 v}{\partial z^2}, \tag{16}$$

$$\frac{\partial T}{\partial t}+u\frac{\partial T}{\partial x}+v\frac{\partial T}{\partial y}+w\frac{\partial T}{\partial z}=\alpha_{nf}\frac{\partial^2 T}{\partial z^2}, \tag{17}$$

where t refers the time. From Equation (7), the new dimensionless variables for unsteady problem take place as:

$$u=axf'(\eta,\tau),\ v=axh(\eta,\tau),\ w=-\sqrt{a\nu_f\, f(\eta,\tau)},\ \eta=z\sqrt{\frac{a}{\nu_f}},\ \theta(\eta,\tau)=\frac{T-T_\infty}{T_w-T_\infty},\ \tau=\frac{Ut}{x}. \tag{18}$$

Substituting Equation (18) into Equations (15)-(17), we obtain the following:

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}\frac{\partial^3 f}{\partial\eta^3}+f\frac{\partial^2 f}{\partial\eta^2}-\left(\frac{\partial f}{\partial\eta}\right)^2-\frac{\partial^2 f}{\partial\eta\partial\tau}+2\Omega h=0, \quad (19)$$

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}\frac{\partial^2 h}{\partial\eta^2}+f\frac{\partial h}{\partial\eta}-h\frac{\partial f}{\partial\eta}-\frac{\partial h}{\partial\tau}-2\Omega\frac{\partial f}{\partial\eta}=0, \quad (20)$$

$$\frac{k_{nf}/k_f}{\Pr\left[(1-\phi)+\phi(\rho C_p)_s/(\rho C_p)_f\right]}\frac{\partial^2\theta}{\partial\eta^2}+f\frac{\partial\theta}{\partial\eta}-\frac{\partial\theta}{\partial\tau}=0, \quad (21)$$

subject to the boundary conditions

$$\begin{gathered} f(0,\tau)=S,\ \frac{\partial f}{\partial\eta}(0,\tau)=-1,\ h(0,\tau)=0,\ \theta(0,\tau)=1, \\ \frac{\partial f}{\partial\eta}(\eta,\tau)\to 0,\ h(\eta,\tau)\to 0,\ \theta(\eta,\tau)\to 0 \ \text{ as } \ \eta\to\infty. \end{gathered} \quad (22)$$

Furthermore, to identify the stability of the steady flow solution $f(\eta)=f_0(\eta),\ h(\eta)=h_0(\eta)$ and $\theta(\eta)=\theta_0(\eta)$ which complying the boundary value problem (19)-(22), we assume

$$\begin{gathered} f(\eta,\tau)=f_0(\eta)+e^{-\gamma\tau}F(\eta,\tau), \quad h(\eta,\tau)=h_0(\eta)+e^{-\gamma\tau}H(\eta,\tau), \\ \theta(\eta,\tau)=\theta_0(\eta)+e^{-\gamma\tau}G(\eta,\tau), \end{gathered} \quad (23)$$

where γ is an unknown eigenvalue, $F(\eta,\tau)$, $H(\eta,\tau)$ and $G(\eta,\tau)$ are small relative to $f_0(\eta)$, $h_0(\eta)$ and $\theta_0(\eta)$, respectively. Substituting Equation (23) into Equations (19)-(22), we obtain the linearized problem

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}\frac{\partial^3 F}{\partial\eta^3}+f_0\frac{\partial^2 F}{\partial\eta^2}+F\frac{\partial^2 f_0}{\partial\eta^2}-2\frac{\partial f_0}{\partial\eta}\frac{\partial F}{\partial\eta}+\gamma\frac{\partial F}{\partial\eta}-\frac{\partial^2 F}{\partial\eta\partial\tau}+2\Omega h=0, \quad (24)$$

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}\frac{\partial^2 H}{\partial\eta^2}+f_0\frac{\partial H}{\partial\eta}+F\frac{\partial h_0}{\partial\eta}-H\frac{\partial f_0}{\partial\eta}-h_0\frac{\partial F}{\partial\eta}+\gamma H-\frac{\partial H}{\partial\tau}-2\Omega\frac{\partial F}{\partial\eta}=0, \quad (25)$$

$$\frac{k_{nf}/k_f}{\Pr\left[(1-\phi)+\phi(\rho C_p)_s/(\rho C_p)_f\right]}\frac{\partial^2 G}{\partial\eta^2}+f_0\frac{\partial G}{\partial\eta}+F\frac{\partial\theta_0}{\partial\eta}+\gamma G-\frac{\partial G}{\partial\tau}=0, \quad (26)$$

together with the boundary conditions

$$F(0,\tau)=0,\ \frac{\partial F}{\partial \eta}(0,\tau)=0,\ H(0,\tau)=0,\ G(0,\tau)=0,$$
$$\frac{\partial F}{\partial \eta}(\eta,\tau)\to 0,\ H(\eta,\tau)\to 0,\ G(\eta,\tau)\to 0 \ \text{ as } \ \eta\to\infty. \tag{27}$$

As discussed by Weidman et al. (2006), we are setting $\tau=0$ to identify the initial growth or decay of the solution (23). Thus, functions $F=F_0(\eta)$, $H=H_0(\eta)$ and $G=G_0(\eta)$. To test our numerical method, we consider the following linear eigenvalue problems

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}F_0''' + f_0F_0'' + f_0''F_0 - 2f_0'F_0' + \gamma F_0'' + 2\Omega H_0 = 0, \tag{28}$$

$$\frac{1}{(1-\phi)^{2.5}\left[(1-\phi)+\phi(\rho_s/\rho_f)\right]}H_0'' + f_0H_0' + F_0h_0' - f_0'H_0 - F_0'h_0 + \gamma H_0 - 2\Omega F_0' = 0, \tag{29}$$

$$\frac{k_{nf}/k_f}{\Pr\left[(1-\phi)+\phi(\rho C_p)_s/(\rho C_p)_f\right]}G_0'' + f_0G_0' + F_0\theta_0' + \gamma G_0 = 0, \tag{30}$$

together with the new conditions

$$F_0(0)=0,\ F_0'(0)=0,\ H_0(0)=0,\ \mathrm{G}_0(0)=0,$$
$$F_0'(\eta)\to 0,\ H_0(\eta)\to 0,\ \mathrm{G}_0(\eta)\to 0 \ \text{ as } \ \eta\to\infty. \tag{31}$$

We should note that for a certain value of Pr and γ, the stability of the steady flow solutions $f_0(\eta)$, $h_0(\eta)$ and $\theta_0(\eta)$ is identified by the smallest eigenvalues. These smallest eigenvalues give two solutions, first is a negative solution and second is a positive solution. For the negative eigenvalue, there is an initial growth of interruption and the flow is said to be unstable. Meanwhile, for the positive eigenvalue, there is an initial decomposition and the flow is said to be stable. Based on the previous study by Harris et al. (2009), they suggest that the range of the possible eigenvalues can be computed by relaxing a boundary condition on $F_0(\eta)$, $H_0(\eta)$ or $G_0(\eta)$. In the present study, we solve the eigenvalue problems (28)-(31) by selecting the condition $F_0'(\eta)\to 0$ as $\eta\to\infty$ which later changes to the new condition $F_0''(0)=1$.

RESULT AND DISCUSSIONS

In order to give an understanding of the current problem, the numerical computations are carried out for the selected parameters of interest, including, rotation Ω, nanoparticle volume fraction ϕ and suction S parameters. The Equations (8)-(10) with conditions (11) are solved using bvp4c function in MATLAB software. The range of values of ϕ is between 0 to 0.2, where $\phi=0$ corresponding to a regular fluid and

$\Pr = 6.2$ (water). The thermophysical properties of the copper (Cu), titania (TiO_2), alumina (Al_2O_3) and the base fluid are given in the work of Oztop and Abu-Nada (2008). Figures 1 (a) to (c) present the effect of nanoparticle volume fraction ϕ on the variation of the skin friction coefficient of x and y components, $f''(0)$ and $h'(0)$ and the local Nusselt number $-\theta'(0)$ with suction parameter for Cu-water nanofluid when $\Omega = 0.001$. It is found that the magnitude of the skin friction coefficients for both components increase with an increment in the value of ϕ. The fact that the presence of nanoparticles in the base fluid will accelerate the fluid motion due to the collision between the nanoparticles and base fluid particle. Thus, decreasing the momentum boundary layer thickness and consequently, increasing the skin frictions at the surface. Furthermore, the opposite trend is observed for the local Nusselt number as the ϕ increase. It should be noted that the critical values of suction seem to decrease as the ϕ increase.

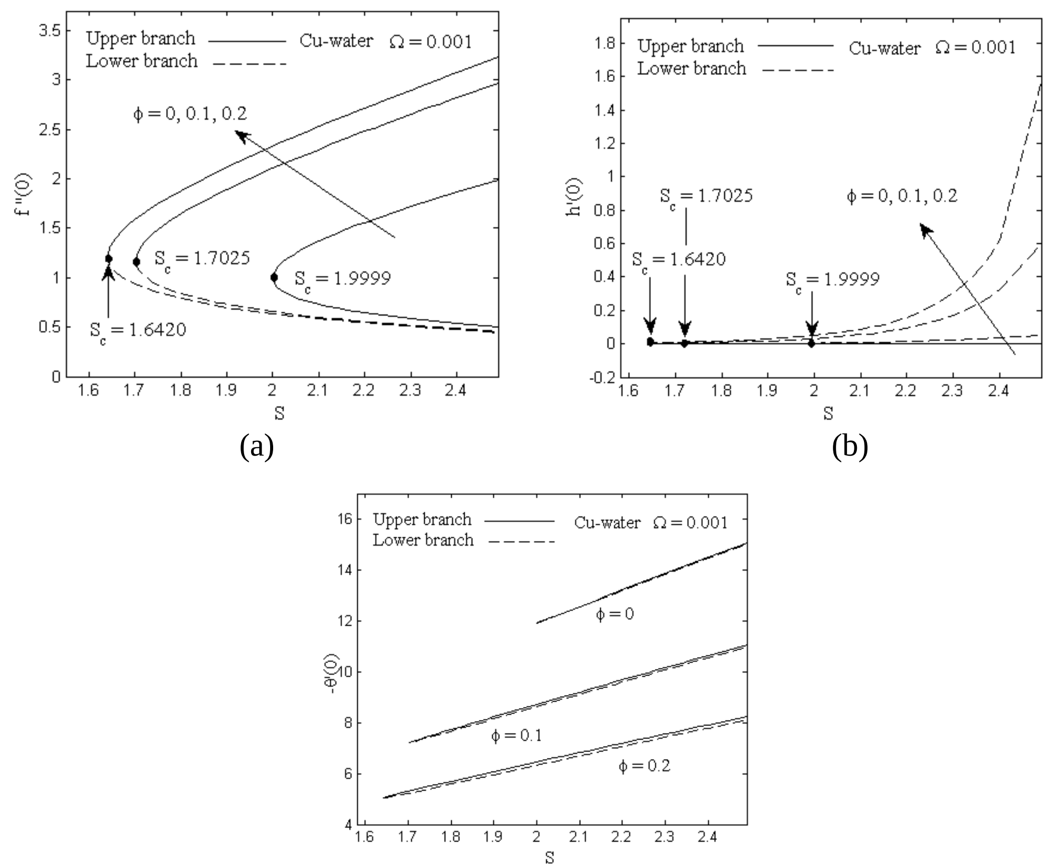


Figure 1. (a-c) Effect of nanoparticle volume fraction ϕ on the skin friction coefficient of x and y components and local Nusselt number.

Figures 2 (a) to (c) illustrate the influence of the rotation Ω on the variation of the $f''(0)$, $h'(0)$ and $-\theta'(0)$ with suction parameter for TiO_2 when $\phi = 0.2$. From these figures, the magnitude of the $f''(0)$, $h'(0)$ and $-\theta'(0)$ are noticed to increase when the values of the rotation increase. However, the dual solutions exist when $\Omega = 0.001$ for $S_c > 2.0564$, while beyond this limit no solutions exist. S_c is the critical value of suction for which Equations (8)-(10) have no solutions. It is worth mentioning that increasing the rotation in the flow reduces the momentum boundary layer thickness. Consequently, increases both the skin friction coefficients of x and y components on the wall.

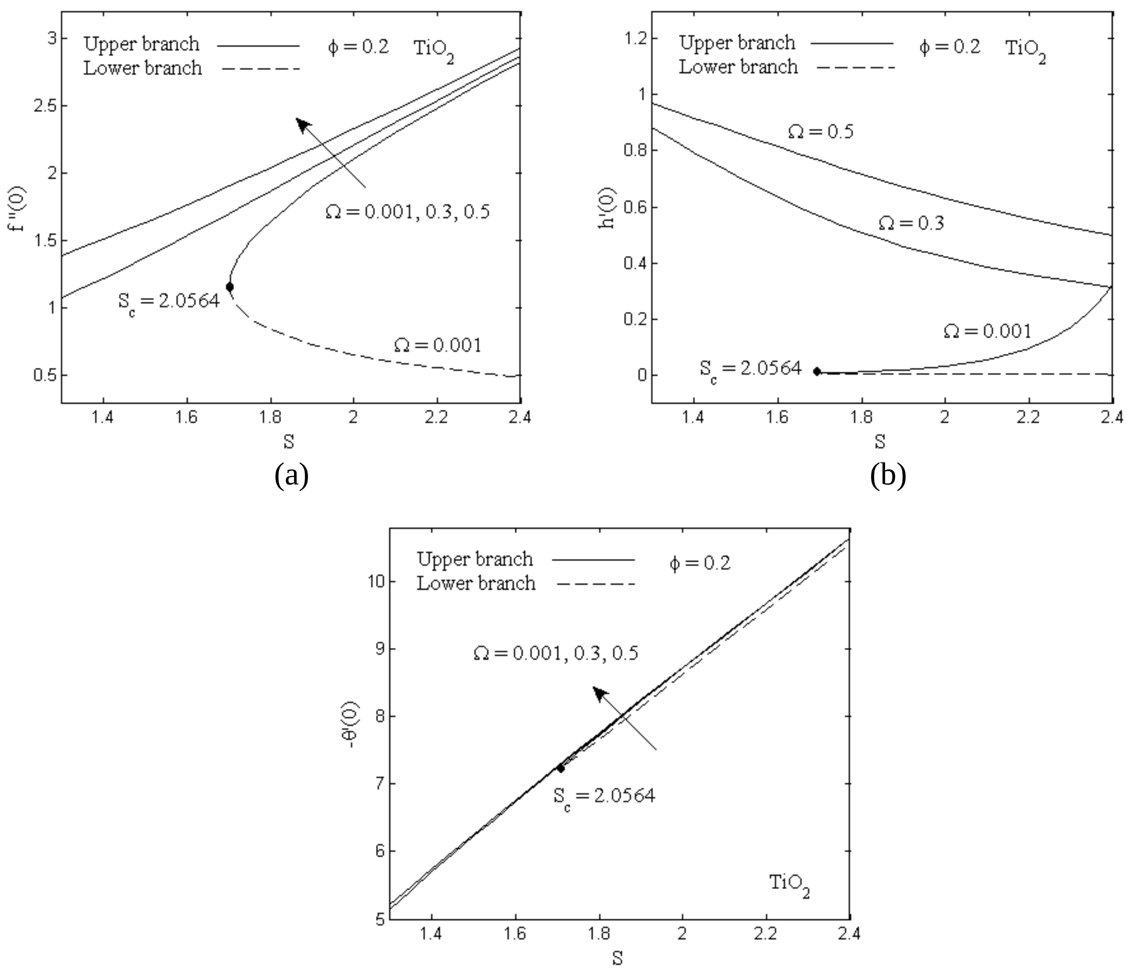


Figure 2. (a-c) Effect of rotation Ω on skin friction coefficients of x and y components and local Nusselt number.

Figures 3 and 4 demonstrate the effects of the velocities of x and y components, $f'(\eta)$, $h(\eta)$ and the temperature profiles $\theta(\eta)$. All the profiles are plotted to validate the numerical results obtained in the current study. It is shown that all profiles have satisfied the boundary conditions (11) the different nanoparticles and suction parameter on asymptotically with different patterns of graphs. As we noticed, the thickness of the boundary layer for the lower branch solution is always thicker than the upper branch solution.

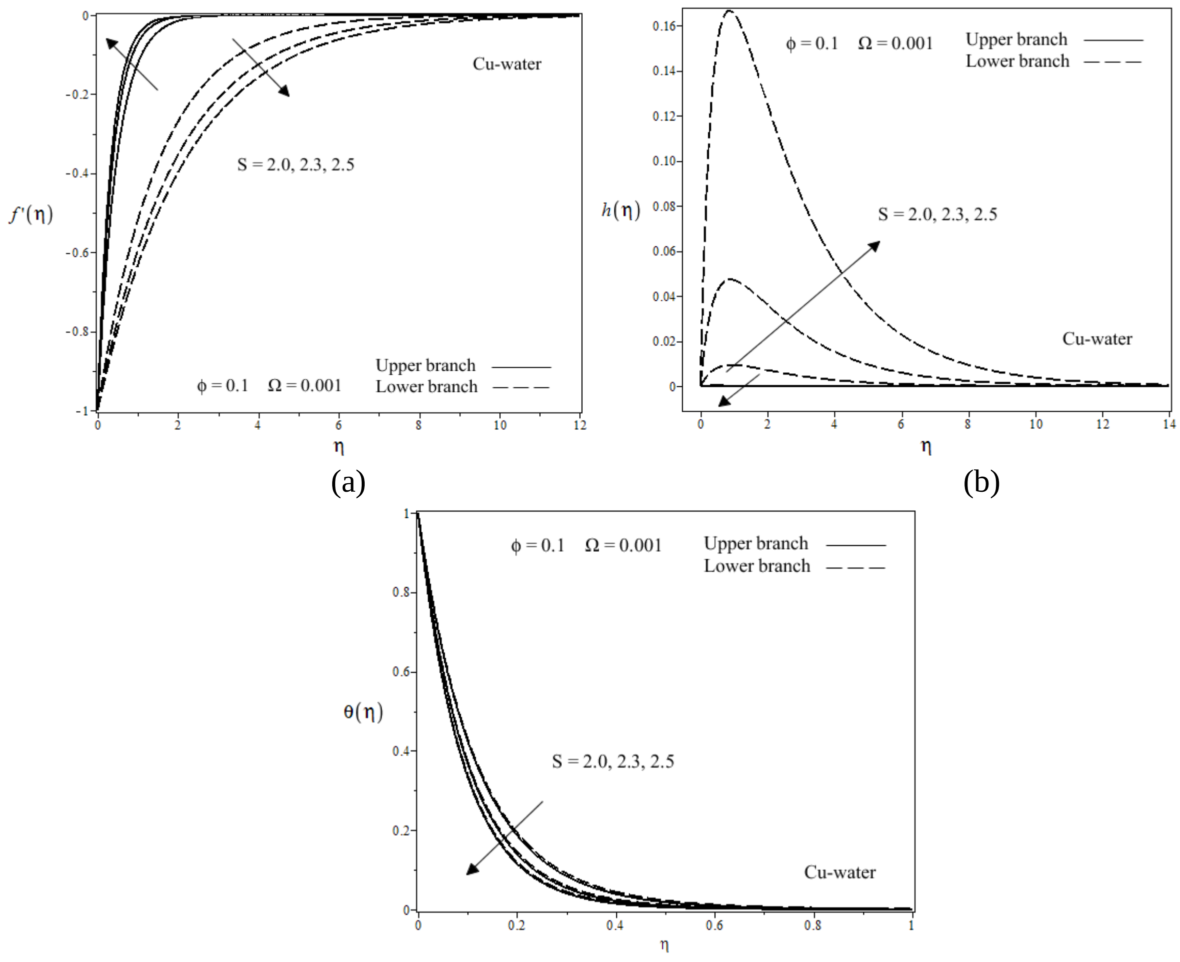


Figure 3. (a-c) Effect of suction S on the velocity of x and y components and temperature profiles.

From this study, the stability of the dual solutions are identified using bvp4c function in MATLAB software. This analysis is conducted to know which of the upper or lower branch solution is linearly stable by depending on the sign of the smallest eigenvalues obtained. The unknown eigenvalue is introduced in Equation (23) and to determine the values of γ, the linear eigenvalue problems given in Equations (28)-(30) subjected to the conditions (31) is being applied. Table 1 and 2 displays the smallest eigenvalues γ for different values of the selected parameters of interest. From the tables, the positive value of γ represents an initial decay of disturbance and the flow is said to be stable for the upper branch solution. Meanwhile, the negative value of γ refers to an initial growth of disturbance and the flow is an unstable for the lower branch solution. The stable flow is always given a good physical meaning that can be realized.

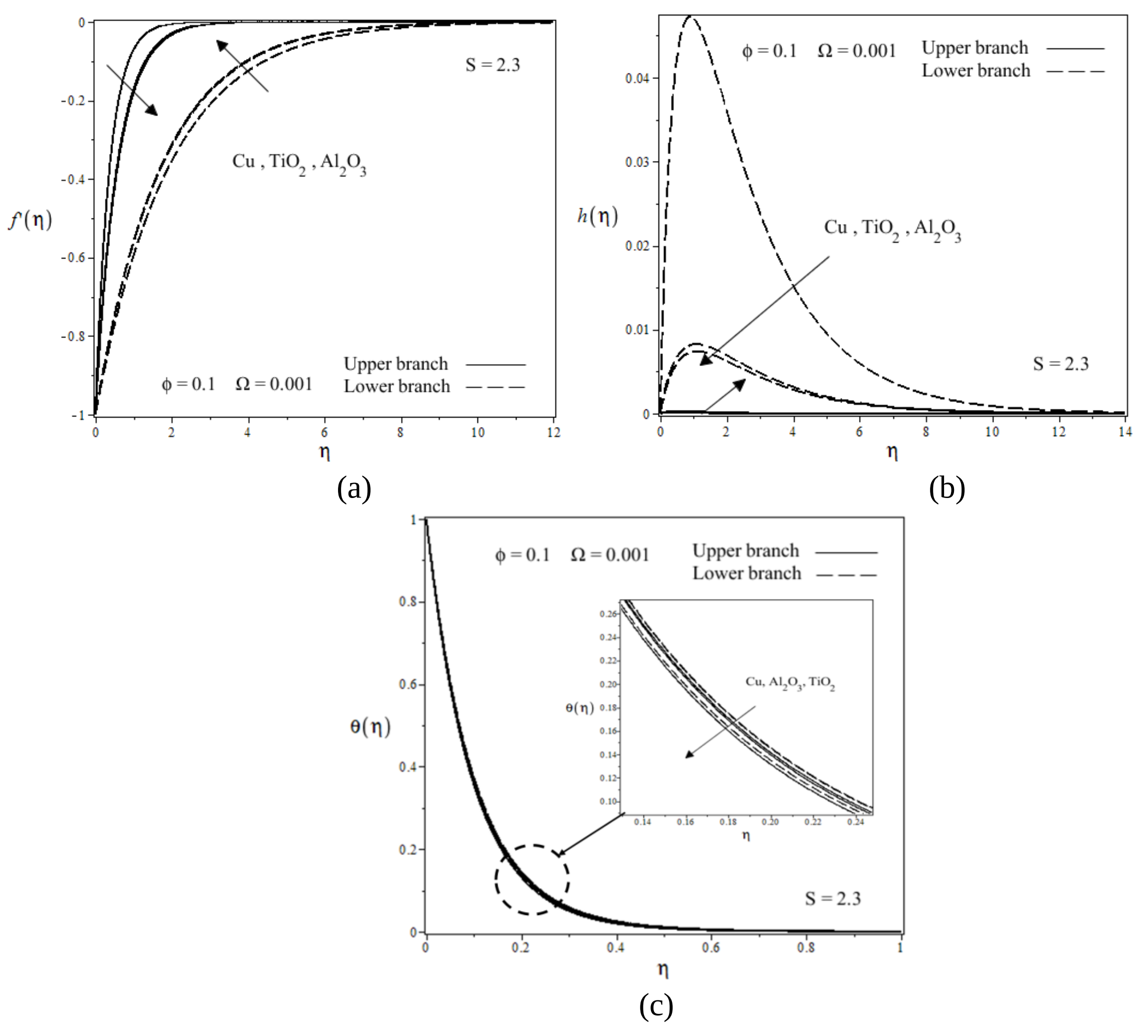


Figure 4. (a-c) Effect of nanoparticles on the velocity of x and y components and temperature profiles.

Table 1. Smallest eigenvalues γ for various values of Ω and S when $\phi = 0.1$ for Cu-water nanofluid.

Ω	S	Upper branch	Lower branch
0.0	2.1	0.9921	-0.6365
	2.2	1.1591	-0.6890
	2.3	1.3277	-0.7328
0.001	2.1	0.9922	-0.0352
	2.2	1.1593	-0.0211
	2.3	1.3279	-0.0104
0.1	2.1	1.3905	-
	2.2	1.5495	-
	2.3	1.7131	-

Table 2. Smallest eigenvalues γ for various values of ϕ and S using a different nanoparticles when $\Omega = 0.001$.

Nanoparticles	ϕ	S	Upper branch	Lower branch
Copper	0	2.1	0.4041	-0.3356
		2.2	0.5957	-0.4549
		2.3	0.7574	-0.5378
	0.1	2.1	0.9922	-0.0352
		2.2	1.1593	-0.0211
		2.3	1.3279	-0.0104
	0.2	2.1	1.1186	-0.0247
		2.2	1.2878	-0.0131
		2.3	1.4707	-0.0045
Alumina	0	2.1	0.4041	-0.3356
		2.2	0.5957	-0.4549
		2.3	0.7574	-0.5378
	0.1	2.1	0.3984	-0.3316
		2.2	0.5911	-0.4522
		2.3	0.7531	-0.5358
	0.2	2.1	0.1042	-0.0972
		2.2	0.4119	-0.3400
		2.3	0.5954	-0.4534
Titania	0	2.1	0.4041	-0.3356
		2.2	0.5957	-0.4549
		2.3	0.7574	-0.5378
	0.1	2.1	0.4463	-0.3642
		2.2	0.6306	-0.4744
		2.3	0.7903	-0.5531
	0.2	2.1	0.2557	-0.2258
		2.2	0.4869	-0.3894
		2.3	0.6590	-0.4884

CONCLUSION

In this paper, the effect of the nanoparticles volume fraction, rotation and suction parameters on the fluid flow and heat transfer analysis of the rotating flow past a shrinking surface in nanofluid is investigated. The stability analysis is performed to identify the stability of the solutions obtained. Some discussions that can be made are as follows:

- Dual solutions exist when the values of rotation are small enough, says $\Omega = 0.001$ for $S_c > 2.0564$ and beyond this limit no solutions exist for TiO_2.
- The highest values of heat transfer occur for Cu compared to Al_2O_3 and TiO_2 due to it has higher thermal conductivity than others.
- The upper branch solution is stable and physically realizable compared to the lower branch solution.
- Increasing the rotation parameter gives rise the magnitudes of the skin friction coefficients and the local Nusselt number.
- Increasing the nanoparticles volume fraction parameter leads to an increase in the skin friction coefficients, while the opposite trend is found for the local Nusselt number.

ACKNOWLEDGEMENT

The authors gratefully acknowledged the financial support received from Ministry of Higher Education Malaysia in the form of Fundamental Research Grant Scheme (FRGS/1/2018/STG06/UPM/02/4/5540155) and Putra Grant GP-IPS/2018/9667900 from Universiti Putra Malaysia.

REFERENCES

Bachok, N., Ishak, A., & Pop, I. (2010). Boundary-layer flow of nanofluids over a moving surface in a flowing fluid. *International Journal of Thermal Sciences*, 49:1663-1668.

Bachok, N., Ishak, A., & Pop, I. (2012). Unsteady boundary-layer flow and heat transfer of a nanofluid over a permeable stretching/shrinking sheet. *International Journal of Heat and Mass Transfer*, 55:2102-2109.

Choi, S. U. S. (1995). Enhancing thermal conductivity of fluids with nanoparticles. *ASME Publication*, 231:99-105.

Das, K., Duari, P. R., Pop, I., & Kundu, P. K. (2014). Nanofluid flow over an unsteady stretching surface in presence of thermal radiation. *Alexandria Engineering Journal*, 53:737-745.

Hafidzuddin, E. H., Nazar, R., Arifin, N. M., & Pop, I. (2015). Stability analysis of unsteady three-dimensional viscous flow over a permeable stretching/shrinking surface. *Journal of Quality Measurement and Analysis*, 11:19-31.

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*, 77: 267-285.

Mahapatra, T. R. & Nandy, S. K. (2011). Stability analysis of dual solutions in stagnation-point flow and heat transfer over a power-law shrinking surface. *International Journal of Nonlinear Sciences*, 12: 86-94.

Merkin, J. H. (1985). On dual solutions occurring in mixed convection in a porous medium. *Journal of Engineering Mathematics*, 20:171-179.

Nadeem, S., Rehman, A., & Mehmood, R. (2014). Boundary layer flow of rotating two phase nanofluid over a stretching surface. *Heat Transfer Asian Research*, 45:285-2

Najib, N., Bachok, N., & Ari_n, N. M. (2016). Stability of dual solutions in boundary layer flow and heat transfer over an exponentially shrinking cylinder. Indian Journal of Science and Technology, 9:1-6.

Naramgari, S. & S ulochana, C. (2016). MHD flow over a permeable stretching/shrinking sheet of a nanofluid with suction/injection. Alexandria Engineering Journal, 55:819-827

Othman, N. A., Yacob, N. A., Bachok, N., Ishak, A., & Pop, I. (2017). Mixed convection boundary-layer stagnation point flow past a vertical stretching/ shrinking surface in a nanofluid. Applied Thermal Engineering, 115:1412-1417.

Oztop, H. F. & Abu-Nada, E. (2008). Numerical study of natural convection in partially heated rectangular enclosures filled with nanofluids. International Journal of Heat Fluid Flow, 29:1326-1336.

Reddy, C. R., Murthy, P. V. S. N., Chamkha, A. J., & Rashad, A. M. (2013). Soret effect on mixed convection flow in a nanofluid under convective boundary condition. International Journal of Heat and Mass Transfer, 64:384-392.

Rosca, N. C. & Pop, I. (2014). Unsteady boundary layer flow of a nanofluid past a moving surface in an external uniform free stream using Buongiorno's model. Computers and Fluids, 95:49-55.

Sharma, R., Ishak, A., & Pop, I. (2014). Stability analysis of magnetohydrodynamic stagnation-point flow toward a stretching/shrinking sheet. Computers and Fluids, 102:94-98.

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 Sciences, 44:730-737.

Yasin, M. H. M., Ishak, A., & 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, 115:1407-1]

Malaysian Journal of Science Special Issue (1) 2019: 33-42

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

COMPARISONS OF HEINZ OPERATOR MEANS WITH DIFFERENT PARAMETERS

Aliaa Abed Al-Jawwad Burqan*

Department of Mathematics
Zarqa University, Zarqa, Jordan
*Corresponding author: Aliaaburqan@yahoo.com
Received: 28th Oct 2018 Revised: 28th Oct 2018 Accepted: 19th Dec 2018
DOI : https://doi.org/10.22452/mjs.sp2019no1.3

ABSTRACT This article aims to present new comparisons of Heinz operator means with different parameters by the help of appropriate scalar comparisons and the monotonicity principle for bounded self-adjoint Hilbert space operators. In particular, for any positive operators $A, B \in B(H)$, we establish the inequality

$$H_\tau(A,B) \leq \left(1 - \frac{(1-2\mu)^2}{(1-2\tau)^2}\right)(A\nabla B) + \frac{(1-2\mu)^2}{(1-2\tau)^2} H_\mu(A,B),$$

where $\mu, \tau \in [0,1]$ satisfying

$$\tau \neq \frac{1}{2},\ \left|\tau - \frac{1}{2}\right| \geq \left|\mu - \frac{1}{2}\right| \text{ and } |2\tau - 1| + |2\mu - 1| \leq 1.$$

2010 MSC: 47A30, 15A45, 15A60.

Key words and phrases: Heinz means, positive operator, unitarily invariant norm, inequality, monotonicity principle.

INTRODUCTION

The Heinz mean of positive numbers a, b in the parameter $v \in [0,1]$, defined by

$$H_v(a,b) = \frac{a^v b^{1-v} + a^{1-v} b^v}{2}$$

is one of the means which intermediates between the arithmetic mean and geometric mean, that is

$$\sqrt{ab} \le H_v(a,b) \le \frac{a+b}{2}, \qquad 0 \le v \le 1 \tag{1}$$

The function $H_v(a,b)$, is decreasing on $\left[0,\frac{1}{2}\right]$ and increasing on $\left[\frac{1}{2},1\right]$. Thus,

$$H_\mu(a,b) \le H_\tau(a,b), \qquad 0 \le \tau \le \mu \le \frac{1}{2} \tag{2}$$

and

$$H_\mu(a,b) \le H_\tau(a,b), \qquad \frac{1}{2} \le \mu \le \tau \le 1 \tag{3}$$

More interesting inequalities related to the Heinz means can be found in (Bhatia, 2006). An operator version of (1) due to (Bhatia and Davis, 1993) is the following inequalities

$$\left\|A^{\frac{1}{2}}B^{\frac{1}{2}}\right\| \le \left\|\frac{A^vB^{1-v}+A^{1-v}B^v}{2}\right\| \le \left\|\frac{A+B}{2}\right\|, \qquad 0 \le v \le 1, \tag{4}$$

where A, B are positive operators on a complex separable Hilbert space and $\|.\|$ is a unitarily invariant norm. Usually, $\left\|\frac{A^vB^{1-v}+A^{1-v}B^v}{2}\right\|$ is called the Heinz mean of A and B. Several inequalities improving the inequalities in (4) have been given by (Kittaneh, 2010; Kittaneh & Manasrah, 2010; Zhan, 1998).

Throughout this article, the space of all bounded linear operators on a Hilbert space H will be denoted by $B(H)$. In the case when $\dim H = n$, $B(H)$ is identified with the matrix algebra M_n of all $n \times n$ matrices with complex entries.

In the following, another operator version of Heinz mean is considered. By recognizing the definition in the scalar case, the Heinz mean is the arithmetic mean of two weighted geometric means. Hence, such definition can be raised up to the level of operators via the operator means. Following (Kittaneh et al., 2012), the weighted arithmetic operator mean ∇_v and geometric mean $\#_v$ are defined as follows:

$$A\nabla_v B = (1-v)A + vB,$$

$$A\#_v B = A^{\frac{1}{2}}\left(A^{\frac{-1}{2}}BA^{\frac{-1}{2}}\right)^v A^{\frac{1}{2}},$$

for $v \in [0,1]$ and positive invertible operators $A, B \in B(H)$.

If $v = \frac{1}{2}$, we write $A\nabla B$ and $A\#B$ to denote the arithmetic operator mean and geometric operator mean, respectively.

By regarding the above definitions, the Heinz operator mean is defined as

$$H_v(A,B) = \frac{A\#_v B + A\#_{1-v}B}{2}.$$

It is well known that the Heinz operator mean intermediates between the arithmetic operator mean and geometric operator mean, that is

$$A\#B \leq H_v(A,B) \leq A\nabla B. \tag{5}$$

In recent years such operator means and related comparisons have been under active investigations. The authors in (Kittaneh et al., 2012) established the following improvement of the second inequality in equation (5) above

$$2min\{v, 1-v\}(A\nabla B - A\#B) \leq A\nabla B - H_v(A,B).$$

The same result was established, in (Kittaneh & Manasrah, 2011), for matrices. Moreover, Kittaneh and Krnić (2013), derived a series of improvements of the Heinz operator inequality by using the *Hermite - Hadamard inequality*.

$$A\#B \leq H_{\frac{2v+1}{4}}(A,B) \leq \frac{1}{4}H_v(A,B) + \frac{1}{2}H_{\frac{2v+1}{4}}(A,B) + \frac{1}{4}A\#B$$

$$\leq \frac{1}{2}H_v(A,B) + \frac{1}{2}A\#B \leq H_v(A,B).$$

In this paper, we are concerned with finding new ordering relations between the Heinz operator means with different parameters by the help of appropriate scalar inequalities and the monotonicity principle for bounded self-adjoint operators on Hilbert space (see, e.g. Pečarić et al., 2005): Let $X \in B(H)$ be self-adjoint with a spectrum $Sp(X)$ and let g and h be continuous real functions such that $g(x) \geq h(x)$ for all $x \in Sp(X)$. Then $g(X) \geq h(X)$.

MAIN RESULTS

The main objective of this section is to derive new comparisons of Heinz means with different parameters for scalars and operators.

Theorem 2.1. *If $a, b > 0$ and $\mu, \tau \in [0,1]$ satisfying*

$$\tau \neq \frac{1}{2}, \ \left|\tau - \frac{1}{2}\right| \geq \left|\mu - \frac{1}{2}\right| \text{ and } |2\tau - 1| + |2\mu - 1| \leq 1,$$

then

$$H_\tau(a,b) \leq \left(1 - \frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{a+b}{2}\right) + \frac{(1-2\mu)^2}{(1-2\tau)^2} H_\mu(a,b). \tag{6}$$

Proof: Let $\rho = 1 - 2\tau$ and $\omega = 1 - 2\mu$. Then $\rho \neq 0, 0 \leq |\omega| \leq |\rho| \leq 1$.

By using the Taylor expansion of $\cosh x$, we have

$$\cosh \rho x = 1 + \frac{\rho^2 x^2}{2!} + \frac{\rho^4 x^4}{4!} + \cdots$$

$$\leq 1 + \left(1 - \frac{\omega^2}{\rho^2} + \frac{\omega^4}{\rho^4}\right)\frac{x^2}{2!} + \left(1 - \frac{\omega^2}{\rho^2} + \frac{\omega^6}{\rho^2}\right)\frac{x^4}{4!} + \ldots$$

$$= \left(1 - \frac{\omega^2}{\rho^2}\right)\cosh x + \frac{\omega^2}{\rho^2}\cosh \omega x.$$

Replacing x by $\frac{x-y}{2}$, we have

$$\cosh\left((1-2\tau)(\frac{x-y}{2})\right) \leq \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\cosh\left(\frac{x-y}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}\cosh\left((1-2\mu)(\frac{x-y}{2})\right).$$

Put $a=e^x$ and $b=e^y$, to get

$$\frac{a^\tau b^{1-\tau}+a^{1-\tau}b^\tau}{2} \leq \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{a+b}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{a^\mu b^{1-\mu}+a^{1-\mu}b^\mu}{2}\right).$$

This completes the proof.

In view of Theorem 2.1, we have

- if $0 \leq \tau \leq \mu \leq \frac{1}{2}$, $\tau \neq \frac{1}{2}$ and $|2\tau-1|+|2\mu-1| \leq 1$, then

$$H_\tau(a,b) \leq \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{a+b}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}H_\mu(a,b)$$

- if $\frac{1}{2} \leq \mu \leq \tau \leq 1$, $\tau \neq \frac{1}{2}$ and $|2\tau-1|+|2\mu-1| \leq 1$, then

$$H_\tau(a,b) \leq \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{a+b}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}H_\mu(a,b),$$

for $a,b>0$.

Thus, our result in Theorem 2.1 is a reverse of inequalities in (2) and (3) under the given conditions.

Now, by virtue of the monotonicity principle and based on the inequality (6), we obtain our first comparison of Heinz operator means.

Theorem2.2
If $A,B \in B(H)$ *are positive definite and* $\mu,\tau \in [0,1]$ *satisfying*

$$\tau \neq \frac{1}{2},\ \left|\tau-\frac{1}{2}\right| \geq \left|\mu-\frac{1}{2}\right| \text{ and } |2\tau-1|+|2\mu-1| \leq 1,$$

then

$$H_\tau(A,B) \le \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)(A\nabla B)+\frac{(1-2\mu)^2}{(1-2\tau)^2}H_\mu(A,B). \tag{7}$$

Proof: Let $X = A^{\frac{-1}{2}}BA^{\frac{-1}{2}}$. Then for any $x \in Sp(X)$, we have

$$\frac{x^\tau+x^{1-\tau}}{2} \le \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{x+1}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{x^\mu+x^{1-\mu}}{2}\right).$$

Now, by the monotonicity principle, we have

$$\frac{X^\tau+X^{1-\tau}}{2} \le \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{X+I}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{X^\mu+X^{1-\mu}}{2}\right).$$

Replacing X by $A^{\frac{-1}{2}}BA^{\frac{-1}{2}}$ and multiplying both sides by $A^{\frac{1}{2}}$, we obtain

$$H_\tau(A,B) \le \left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)(A\nabla B)+\frac{(1-2\mu)^2}{(1-2\tau)^2}H_\mu(A,B).$$

This completes the proof.

In the following, we establish a refinement of the second inequality in (4) for the Hilbert-Schmidt norm under given conditions.

Theorem 2.3. *If $A, B, X \in M_n$, where A and B are positive definite and $\mu, \tau \in [0,1]$ satisfying*

$$\tau \ne \tfrac{1}{2},\ \left|\tau-\tfrac{1}{2}\right| \ge \left|\mu-\tfrac{1}{2}\right| \text{ and } |2\tau-1|+|2\mu-1| \le 1,$$

then

$$\left\|\frac{A^{\tau}XB^{1-\tau}+A^{1-\tau}XB^{\tau}}{2}\right\|_h \leq \left\|\left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{AX+XB}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{A^{\mu}XB^{1-\mu}+A^{1-\mu}XB^{\mu}}{2}\right)\right\|_h.$$

Proof: Every positive definite matrix is unitarily diagonalizable and this implies that there are unitary matrices $U, V \in M_n$ such that $A = UD_1U^*$ and $B = VD_2V^*$, where $D_1 = diag(\gamma_1, \dots, \gamma_n)$ and $D_2 = diag(\sigma_1, \dots, \sigma_n)$ with $\gamma_i, \sigma_i > 0,\ i = 1, \dots, n.$ Let $Y = U^*XV = [y_{ij}]$. Then, we get $AX + XB = U[(\gamma_i + \sigma_j)y_{ij}]V^*$, and $A^{\tau}XB^{1-\tau} + A^{1-\tau}XB^{\tau} = U[(\gamma_i^{\tau}\sigma_j^{1-\tau} + \gamma_i^{1-\tau}\sigma_j^{\tau})y_{ij}]V^*$.

Thus,

$$\left\|\frac{A^{\tau}XB^{1-\tau}+A^{1-\tau}XB^{\tau}}{2}\right\|_h^2 = \sum_{i,j=1}^{n}\left(\frac{\gamma_i^{\tau}\sigma_j^{1-\tau}+\gamma_i^{1-\tau}\sigma_j^{\tau}}{2}\right)^2 |y_{ij}|^2$$

$$\leq \sum_{i,j=1}^{n}\left(\left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{\gamma_i+\sigma_j}{2}\right) + \frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{\gamma_i^{\mu}\sigma_j^{1-\mu}+\gamma_i^{1-\mu}\sigma_j^{\mu}}{2}\right)\right)^2 |y_{ij}|^2$$

$$= \left\|\left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}\right)\left(\frac{AX+XB}{2}\right) + \frac{(1-2\mu)^2}{(1-2\tau)^2}\left(\frac{A^{\mu}XB^{1-\mu}+A^{1-\mu}XB^{\mu}}{2}\right)\right\|_h^2.$$

This completes the proof.

In what follows, we turn to another mean that intermediates between the geometric mean and arithmetic mean, which is the logarithmic mean. The logarithmic mean is defined as

$$L(a,b)=\frac{log\ a-log\ b}{a-b},$$

where, $a,b>0$ and

$$\sqrt{ab}\le L(a,b)\le\frac{a+b}{2}. \tag{8}$$

In order to establish a series of refinements of Heinz inequalities, Kittaneh and Krnić, (2013) considered the parameterized class of continuous functions $F_v\colon R^+\to R, v\in[0,1]$, defined by

$$F_v(x)=\begin{cases}\dfrac{x^v-x^{1-v}}{\log x}, & x>0, x\neq 1,\\ 2v-1, & x=1.\end{cases}$$

In the following theorem, we construct another refinement of Heinz inequalities, which is a generalization of the second inequality in (8).

Theorem 2.4. $If\ a,b>0,\ \frac{1}{3}\le k\le 1\ and\ \mu,\tau\in[0,1]\ satisfying$

$$\tau\neq\frac{1}{2},\ \left|\tau-\frac{1}{2}\right|\ge\left|\mu-\frac{1}{2}\right| \text{ and } |2\tau-1|+|2\mu-1|\le 1,$$

$then$

$$\frac{a^{1-\tau}b^{\tau}-a^{\tau}b^{1-\tau}}{(1-2\tau)(\log a-\log b)}\le\left(1-\frac{(1-2\mu)^2}{(1-2\tau)^2}k\right)\left(\frac{a+b}{2}\right)+\frac{(1-2\mu)^2}{(1-2\tau)^2}kH_\mu(a,b). \tag{9}$$

Proof: Let $\rho=1-2\tau$ and $\omega=1-2\mu$. Then $\rho\neq 0, 0\le|\omega|\le|\rho|\le 1$.

By using the Taylor expansion of $\sinh x$ and $\cosh x$, we have

$$\frac{\sinh \rho x}{\rho x} = 1 + \frac{\rho^2 x^2}{3!} + \frac{\rho^4 x^4}{5!} + \cdots$$

$$\leq 1 + \left(1 - \frac{\omega^2}{\rho^2} + \frac{\omega^4}{\rho^2}\right)\frac{x^2}{3!} + \left(1 - \frac{\omega^2}{\rho^2} + \frac{\omega^6}{\rho^2}\right)\frac{x^4}{5!} + \ldots$$

$$\leq 1 + \left(\frac{1}{k} - \frac{\omega^2}{\rho^2} + \frac{\omega^4}{\rho^2}\right)\frac{x^2}{3!} + \left(\frac{1}{k} - \frac{\omega^2}{\rho^2} + \frac{\omega^6}{\rho^2}\right)\frac{x^4}{5!} + \ldots$$

$$\leq 1 + k\left(\frac{1}{k} - \frac{\omega^2}{\rho^2} + \frac{\omega^4}{\rho^2}\right)\frac{x^2}{2!} + k\left(\frac{1}{k} - \frac{\omega^2}{\rho^2} + \frac{\omega^6}{\rho^2}\right)\frac{x^4}{4!} + \ldots$$

$$= 1 + \left(1 - \frac{\omega^2 k}{\rho^2} + \frac{\omega^4 k}{\rho^2}\right)\frac{x^2}{2!} + \left(1 - \frac{\omega^2 k}{\rho^2} + \frac{\omega^6 k}{\rho^2}\right)\frac{x^4}{4!} + \ldots$$

$$= \left(1 - \frac{\omega^2}{\rho^2}k\right)\cosh x + \frac{\omega^2}{\rho^2}k \cosh \omega x.$$

Replacing x by $\frac{x-y}{2}$, we have

$$\frac{sinh((1-2\tau)\left(\frac{x-y}{2}\right))}{(1-2\tau)\left(\frac{x-y}{2}\right)} \leq \left(1 - \frac{(1-2\mu)^2}{(1-2\tau)^2}k\right)\cosh\left(\frac{x-y}{2}\right) + \frac{(1-2\mu)^2}{(1-2\tau)^2}k \cosh\left((1-2\mu)(\frac{x-y}{2})\right).$$

Put $a = e^x$ and $b = e^y$, to get

$$\frac{a^{1-\tau}b^{\tau} - a^{\tau}b^{1-\tau}}{(1-2\tau)(\log a - \log b)} \leq \left(1 - \frac{(1-2\mu)^2}{(1-2\tau)^2}k\right)\left(\frac{a+b}{2}\right) + \frac{(1-2\mu)^2}{(1-2\tau)^2}k\left(\frac{a^{1-\mu}b^{\mu} + a^{\mu}b^{1-\mu}}{2}\right).$$

This completes the proof.

Taking $\tau = 1$ or 0 in Theorem 2.4, this yields $\mu = \frac{1}{2}$ and so the second inequality in (8) is obtained.

Finally, an operator version of the inequality (9) is obtained by using the monotonicity principle in a similar way as in the proof of Theorem 2.2.

Theorem 2.5. *If* $A, B \in B(H)$ *are positive definite,* $\frac{1}{3} \leq k \leq 1$ *and* $\mu, \tau \in [0,1]$ *satisfying*

$$\tau \neq \frac{1}{2}, \ \left|\tau - \frac{1}{2}\right| \geq \left|\mu - \frac{1}{2}\right| \text{ and } |2\tau - 1| + |2\mu - 1| \leq 1,$$

then

$$\frac{1}{(2\tau-1)} A^{\frac{1}{2}} F_\tau (A^{\frac{-1}{2}} B A^{\frac{-1}{2}}) A^{\frac{1}{2}} \leq \left(1 - \frac{(1-2\mu)^2}{(1-2\tau)^2} k\right)(A\nabla B) + \frac{(1-2\mu)^2}{(1-2\tau)^2} k\, H_\mu(A,B).$$

REFERENCES

Bhatia R. and Davis C. (1993). More matrix forms of the arithmetic-geometric mean inequality. SIAM Journal on Matrix Analysis and Applications 14: 132-136.

Bhatia R. (2006). Interpolating the arithmetic-geometric mean inequality and its operator version. Linear Algebra and its Applications 413: 355-363.

Kittaneh F. (2010). On the convexity of the Heinz means. Integral Equations and Operator Theory 68: 519-527.

Kittaneh F., Krnić M., Lovričević N. and Pečarić J. (2012). Improved arithmetic-geometric and Heinz means inequalities for Hilbert space operators. Publicationes Mathematicae Debrecen 80: 465-478.

Kittaneh F.and Krnić M. (2013). Refined Heinz operator inequalities. Linear and Multilinear Algebra 61: 1148-1157.

Kittaneh F. and Manasrah Y. (2010). Improved young and Heinz inequalities for matrices. Journal of Mathematical Analysis and Applications 361: 262-269.

Kittaneh F. and Manasrah Y. (2011). Reverse Young and Heinz inequalities for matrices. Linear and Multilinear Algebra 59: 1031-1037.

Pečarić J. , Furuta T., Mićić Hot J. and Seo Y. (2005). Mond-Pečarić Method in Operator Inequalities. Inequalities for bounded selfadjoint operators on a Hilbert space. Monographs in Inequalities, 1. Zagreb: Element.

Zhan X. (1998). Inequalities for unitarily invariant norms. SIAM Journal on Matrix Analysis and Applications 20: 466-470.

Malaysian Journal of Science Special Issue (1) 2019: 43-54

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

A GUARANTEED PURSUIT TIME IN A DIFFERENTIAL GAME IN HILBERT SPACE

Gafurjan Ibragimov[1,3]*, Usman Waziri[1,2], Idham Arif Alias[1,3], Zarina Bibi Ibrahim[1]

[1]Department of Mathematics, Faculty of Science Universiti Putra Malaysia, Serdang, Malaysia
[2]Department of Mathematics, Faculty of Science Bauchi State University Gadau, Nigeria
[3]Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Malaysia
*Corresponding author: ibragimov@upm.edu.my[1,3] , usmanwazirimth@yahoo.com[1,2], idham_aa@upm.edu.my[1,3] , zarinabb@upm.edu.my[1]
Received: 29th Oct 2018 Revised: 29th Oct 2018 Accepted: 19th Dec 2018
DOI: https://doi.org/10.22452/mjs.sp2019no1.4

ABSTRACT We study a pursuit differential game problem of one pursuer and one evader in the Hilbert space l_2. The differential game is described by an infinite number of first-order 2-systems of linear differential equations. The control functions of players are subjected to integral constraints. A game is started from the given initial position z^0. It is given another point z^1 in the space l_2. If the state of the infinite system coincides with the point z^1 at some time, then pursuit is considered completed. Our purpose is to obtain an equation to find a guaranteed pursuit time and construct a strategy for the pursuer.

ABSTRAK Kami mengkaji satu permasalahan permainan pembezaan pengejaran bagi satu pengejar dan satu pengelak di dalam ruang Hilbert l_2. Permainan pembezaan diterangkan oleh bilangan tak terhingga sistem-2 persamaan pembezaan linear peringkat satu. Fungsi kawalan pemain bergantung kepada kekangan kamiran. Permainan dimulakan dari kedudukan awal z^0 yang diberi. Satu lagi titik z^1 diberi dalam ruang l_2. Jika keadaan sistem tak terhingga berkenaan bertepatan dengan titik z^1 pada suatu masa, maka pengejaran dianggap tamat. Tujuan kami adalah untuk memperolehi satu persamaan untuk mencari satu masa pengejaran yang pasti dan membina satu strategi untuk pengejar.

INTRODUCTION

Differential games were initiated by Isaacs, (1965). Differential games in finite dimensional Euclidian spaces were studied by many researchers. A large and growing body of literature has investigated two person differential games and fundamental contributions were made by researchers such as Friedman, 1971; Krasovskii & Subbotin, 1988; Lewin, 1994; Petrosyan, 1993; Pontryagin, 1988.

There are mainly two constraints on control functions of players: geometric and integral constraints. In-views of the amount of works been done in developing the differential games, the integral constraints have been extensively discussed by many researchers with various approaches.

Differential games of many players were first studied and a sufficient condition of completion of pursuit was obtained in the work of Satimov et al., (1983). In the works of Azamov & Samatov, 2000; Samatov, 2013; Π-strategy is defined for pursuer with integral constraint. The paper of Chikrii & Belousov, (2010) is devoted to a linear pursuit differential game with integral constraint. In the works of Ibragimov et al., 2011; Kuchkarov, 2013; Subbotin & Ushakov, 1975; optimal strategies of players were constructed and a formula to find the optimal pursuit time or the value of the game was found. A sufficient condition of evasion was obtained in the paper of Ibragimov & Salleh, (2012) for a differential game with coordinate-wise integral constraints. Also, the works of Huseyin & Huseyin, 2012; Konovalov, 1987; Lokshin, 1990; Nikolskii, 1969; Okhezin, 1977; Solomatin, 1984; relate to linear differential games with integral constraints where games of kind were studied.

One of the powerful methods in studying the differential game and control problems in systems with distributed parameters is the decomposition method. This method was used to study the control problems described by partial differential equations in the works of Avdonin & Ivanov, 1995; Azamov & Ruziboyez, 2013; Butkovsky, 1969; Chernous'ko, 1992.

Using the same method, differential game problems were reduced to ones described by infinite systems of differential equations in the papers of Ibragimov, 2002; Mamatov, 2008; Satimov & Tukhtasinov, 2006; Tukhtasinov & Mamatov, 2008; Tukhtasinov & Mamatov, 2009. It should be noted that in the paper of Ibragimov, (2002), optimal pursuit time was found and optimal strategies of players were constructed.

Hence, there is an important connection between the control problems described by PDE and those described by infinite systems of differential equations. Control and differential game problems described by infinite system of differential equations are of independent interest and can be investigated within one theoretical framework independently of those described by PDE.

There are many works devoted to control and differential game problems described by infinite system of differential equations. In the paper of Alias et al., (2017), an evasion differential game of infinitely many evaders from infinitely many pursuers was studied in Hilbert space l_2 and evasion strategies were constructed in explicit form. In the paper of Ibragimov, (2013), the full solution of optimal pursuit differential game problem was obtained for the infinite system of differential equations with positive coefficients in Hilbert space l_2^r. In the case of negative coefficients a control problem was studied in the paper of Ibragimov & Ja'afaru, (2011), and optimal pursuit differential game problem was studied in the paper of Ibragimov et al., (2017). Optimal strategies of inertial players were constructed in the paper of Ibragimov et al., (2015), where the control resources of pursuers need not be greater than that of evader.

In the paper Ibragimov, (2013), a differential game problem described by the infinite system

$$\begin{cases} \dot{x}_k = -\alpha_k x_k - \beta_k y_k + u_{1k} - v_{1k}, & x_k(0) = x_{k0} \\ \dot{y}_k = \beta_k x_k - \alpha_k y_k + u_{2k} - v_{2k}, & y_k(0) = y_{k0} \end{cases}, \; k = 1, 2, \cdots, \tag{1}$$

was examined in l_2, where α_k, β_k are given real numbers, $u = (u_{11}, u_{12}, u_{21}, u_{22}, \cdots)$ and $v = (v_{11}, v_{12}, v_{21}, v_{22}, \cdots)$ are control parameters of pursuer and evader, respectively, $x_0 = (x_{10}, x_{20}, \cdots) \in l_2$, $y_0 = (y_{10}, y_{20}, \cdots) \in l_2$.

The purpose of pursuer is to bring the state to the origin of the space l_2 against any action of the Evader who exactly tries to avoid this. In that paper, optimal pursuit time was found and optimal strategies of players were constructed.

In the present paper, we investigate a pursuit differential game problems described by (1) where pursuer tries to bring the state of the system from a given initial state z^0 to another given one z^1 for a finite time. We find conditions under which pursuit can be completed. Note that previous studies of differential games described by (1) have only dealt with the case $z^1 = 0$.

STATEMENT OF PROBLEM

We consider the space

$$l_2 = \left\{ \xi = (\xi_1, \xi_2, \ldots) \mid \sum_{j=1}^{\infty} |\xi_k|^2 < \infty, \; \xi_k \in \mathbb{R}^2 \right\}$$

with inner product and norm defined by

$$\langle \xi, \eta \rangle = \sum_{j=1}^{\infty} \xi_k \eta_k, \; \xi, \eta \in l_2, \;\; \|\xi\| = \left(\sum_{j=1}^{\infty} |\xi_k|^2 \right)^{1/2}.$$

In the space l_2, we study a differential game described by the following infinite system of 2-systems of 1st-order differential equations

$$\begin{aligned} \dot{x}_k &= -\alpha_k x_k - \beta_k y_k - u_{1k} + v_{1k}, & x_k(0) = x_k^0 \\ \dot{y}_k &= \beta_k x_k - \alpha_k y_k - u_{2k} + v_{2k}, & y_k(0) = y_k^0 \end{aligned}, \; k = 1, 2, \ldots, \tag{2}$$

with initial states of pursuer $x^0 = (x_1^0, x_2^0, \ldots) \in l_2$ and evader $y^0 = (y_1^0, y_2^0, \ldots) \in l_2$ where α_k, β_k are real numbers and $\alpha_k > 0$, $k = 1, 2, \ldots$, $u = (u_{11}, u_{12}, u_{21}, u_{22}, \ldots)$ is a control parameter of the pursuer and $v = (v_{11}, v_{12}, v_{21}, v_{22}, \ldots)$ is that of evader.

Let $x^1 = (x_1^1, x_2^1, ...) \in l_2$, $y^1 = (y_1^1, y_2^1, ...) \in l_2$ be another state, and let T be a sufficiently large positive number.

Definition 2.1 *A function* $w(\cdot)$, $w:[0,T] \to l_2$, *with measurable coordinates* $w_{1k}(t), w_{2k}(t)$, $0 \le t \le T$, $k = 1, 2, \dots$, *so that* $w(\cdot) = (w_{11}(\cdot), w_{21}(\cdot), w_{12}(\cdot), w_{22}(\cdot), ...)$ *is subjected to*

$$\sum_{k=1}^{\infty} \int_0^T \left(w_{1k}^2(s) + w_{2k}^2(s) \right) ds \le \rho_0^2,$$

is called admissible control, where ρ_0 *is a given positive number.*

Let $S(\rho_0)$ denote the set of all admissible controls.

Definition 2.2 *Admissible controls of pursuer and evader are defined as the functions* $u(\cdot) \in S(\rho)$ *and* $v(\cdot) \in S(\sigma)$ *, respectively, where* ρ *and* σ *are given positive numbers.*

Definition 2.3 *The strategy of pursuer is defined as a function*

$$u(t,v) = (u_1(t,v), u_2(t,v), ...), \quad u:[0,T] \times l_2 \to l_2$$

whose components $u_k = (u_{1k}, u_{2k})$ *has the form*

$$u_k(t,v) = v_k(t) + w_k(t), \ w_k = (w_{k1}, w_{k2}), \ v_k = (v_{1k}, v_{2k}),$$

for which the system (2) *has a unique solution at* $u(t) = u(t,v)$, *where* $v(\cdot) = (v_1(\cdot), v_2(\cdot), ...)$ *is any admissible control of evader, and* $w(\cdot) = (w_1(\cdot), w_2(\cdot), ...) \in S(\rho - \sigma)$ *is any function.*

Denote

$$z(t) = \left(z_1(t), z_2(t), ...\right), \ z_k(t) = \left(x_k(t), y_k(t)\right), |z_k| = \sqrt{x_k^2 + y_k^2},$$
$$z^0 = \left(z_1^0, z_2^0, ...\right) = \left(x_1^0, y_1^0, x_2^0, y_2^0, ...\right),$$
$$z^1 = \left(z_1^1, z_2^1, ...\right) = \left(x_1^1, y_1^1, x_2^1, y_2^1, ...\right).$$

Definition 2.4 *We say that pursuit can be completed for the time* $\theta > 0$ *in the game* (2) *if for a strategy* $u(t,v)$ *of pursuer and any admissible control* $v(t)$ *of evader,* $z(\tau) = z^1$ *at some* τ, $0 \le \tau \le \theta$. *The number is also called a guaranteed pursuit time.*

Problem 2.5 *Find an equation for guaranteed pursuit time in differential game* (2)*, and construct the strategy of pursuer.*

Let

$$H_k(t)=\begin{bmatrix} e^{-\alpha_k t}\cos(\beta_k t) & -e^{-\alpha_k t}\sin(\beta_k t) \\ e^{-\alpha_k t}\sin(\beta_k t) & e^{-\alpha_k t}\cos(\beta_k t) \end{bmatrix}, k=1,2,...$$

The matrix $H_k(t)$ possesses the following properties

(i) $H_k(h+t)=H_k(t)H_k(h)=H_k(h)H_k(t),$

(ii) $|H_k(t)z_k|=|H_k^*(t)z_k|=e^{-\alpha_k t}|z_k|,$

(iii) $|H_k(t)H_k^*(t)z_k|=|H_k^*(t)H_k(t)z_k|=e^{-2\alpha_k t}|z_k|,$

where H^* is the transpose of matrix H .

SOLUTION OF A CONTROL PROBLEM

We study a control problem described by the following infinite system of differential equations

$$\begin{aligned} \dot{x}_k &= -\alpha_k x_k - \beta_k y_k + w_{1k}, \quad x_k(0)=x_k^0 \\ \dot{y}_k &= \beta_k x_k - \alpha_k y_k + w_{2k}, \quad y_k(0)=y_k^0 \end{aligned}, \ k=1,2,..., \tag{3}$$

where $w=(w_{11},w_{21},w_{12},w_{22},...)$ is control parameter.

Let $C(0,T;l_2)$ denote the space of continuous functions $z(\cdot)=(z_1(\cdot),z_2(\cdot),...)$ with values $z(t)\in l_2,\ 0\le t\le T$.

If $w(\cdot)\in S(\rho)$, then the infinite system of differential equations (3) has the only solution $z(t)=(z_1(t),z_2(t),...),\ 0\le t\le T$, in $C(0,T;l_2)$ (Ibragimov et al., (2008)), where

$$z_k(t)=H_k(t)\left(z_k^0+\int_0^t H_k(-s)w_k(s)ds\right),\ k=1,2,... \tag{4}$$

We study the following control problem for the infinite system of differential equations (3): find a time θ such that

$$z(0)=z^0,\ z(\theta)=z^1.$$

Let

$$E(t)=\sum_{k=1}^{\infty}\left(2\,|\,z_k^0\,|^2\;B_k(t)+2\,|\,z_k^1\,|^2\;A_k(t)\right),t>0,\;z^0,z^1\in l_2, \tag{5}$$

where

$$A_k(t)=\frac{2\alpha_k}{1-e^{-2\alpha_k t}}\,,B_k(t)=\frac{2\alpha_k}{e^{2\alpha_k t}-1},\;k=1,2,...$$

The following statement can be proved similar to Lemma 1 in Ibragimov and Ja'afaru, (2011).

Lemma 3.1 *Let* $z^0, z^1 \in l_2$ *, and the series*

$$\sum_{k=1}^{\infty}\alpha_k\,|\,z_k^1\,|^2 \tag{6}$$

be convergent. Then, for any t > 0, the series E(t) converges.

It is not difficult to see that, for any $k=1,2,...$, both of the functions $B_k(t)$ and $A_k(t)$ are decreasing on $(0,+\infty)$, $B_k(t)\to+\infty$ and $A_k(t)\to+\infty$ as $t\to 0^+$, $B_k(t)\to 0^+$ and $A_k(t)\to 2\alpha_k$ as $t\to+\infty$.

It can be shown that the series $E(t)$ possesses the following properties.

(i) $E(t)$ is decreasing on $(0,+\infty)$;
(ii) $E(t)\to+\infty$ as $t\to 0^+$,
(iii) $E(t)\to 4\sum_{k=1}^{\infty}\alpha_k\,|\,z_k^1\,|^2$ as $t\to+\infty$.

From properties *(i)* and *(iii)*, we can see that

$$E(t)>4\sum_{k=1}^{\infty}\alpha_k\,|\,z_k^1\,|^2,\,t>0. \tag{7}$$

Consider the equation

$$E(t)=\rho_0^2,\,t>0, \tag{8}$$

and the inequality

$$\rho_0^2 > 4\sum_{k=1}^{\infty}\alpha_k \,|\, z_k^1 \,|^2 . \qquad (9)$$

The above mentioned properties of $E(t)$ allows us to conclude that equation (8) has a root if and only if (9) is satisfied and the root is unique.

Now, we give a solution to the control problem.

Theorem 3.2 *Let* $z^0, z^1 \in l_2$ *and* (9) *be satisfied. Then there exists a control* $w(\cdot) \in S(\rho_0)$ *to transfer the state of the system* (3) *from the initial state* z^0 *to the state* z^1.

Proof: A. Define the control by

$$w_k(t) = H_k^*(-t)\left[H_k(-\theta)z_k^1 - z_k^0\right]B_k(\theta), \; k = 1,2,..., \; 0 \le t \le \theta. \qquad (10)$$

Show that (10) is admissible. Using the obvious inequality $|\, x - y \,|^2 \le 2\,|\, x \,|^2 + 2\,|\, y \,|^2$, properties of $H_k(t)$ and (10), we have

$$\begin{aligned}
\sum_{k=1}^{\infty}\int_0^{\theta}\left|w_k(s)\right|^2 ds &= \sum_{k=1}^{\infty}\int_0^{\theta}\left|H_k^*(-s)\left[H_k(-\theta)z_k^1 - z_k^0\right]B_k(\theta)\right|^2 ds \\
&\le \sum_{k=1}^{\infty}\left(2e^{2\alpha_k\theta}\,|\, z_k^1 \,|^2 + 2\,|\, z_k^0 \,|^2\right)B_k^2(\theta)\int_0^{\theta} e^{2\alpha_k s}ds \\
&= \sum_{k=1}^{\infty}\left(2\,|\, z_k^0 \,|^2\; B_k(\theta) + 2\,|\, z_k^1 \,|^2\; A_k(\theta)\right) \\
&= E(\theta) = \rho_0^2.
\end{aligned}$$

Thus, (10) is admissible.

B. Show that $z(\theta) = z^1$. Indeed,

$$\begin{aligned}
z_k(\theta) &= H_k(\theta)\left(z_k^0 + \int_0^{\theta} H_k(-s)\left(H_k^*(-s)\left[H_k(-\theta)z_k^1 - z_k^0\right]B_k(\theta)\right)ds\right) \\
&= H_k(\theta)\left(z_k^0 + \left(H_k(-\theta)z_k^1 - z_k^0\right)B_k(\theta)\int_0^{\theta} e^{2\alpha_k s}ds\right) \\
&= H_k(\theta)z_k^0 + H_k(\theta)\left(H_k(-\theta)z_k^1 - z_k^0\right) \\
&= z_k^1.
\end{aligned}$$

Thus, the system $z(t)$ can be transferred from z^0 to z^1 for the time θ. The proof of Theorem 3.2 is complete.

GUARANTEED PURSUIT TIME

Let us consider differential game (2). It is not difficult to verify that

$$z_k(t) = H_k(t)\left(z_k^0 - \int_0^t H_k(-s)u_k(s)ds + \int_0^t H_k(-s)v_k(s)ds\right). \tag{11}$$

Consider the equation

$$E(t) = (\rho-\sigma)^2,\ t>0, \tag{12}$$

and the inequality

$$(\rho-\sigma)^2 > 4\sum_{k=1}^{\infty}\alpha_k\,|z_k^0|^2\,. \tag{13}$$

As mentioned above that (12) has a root $t=\theta_1$ if and only if (13) holds, and the root is unique. We can assume, by choosing T if necessary, that $\theta_1 < T$. We prove the following statement.

Theorem 4.1 *If* (13) *is satisfied and* $\rho>\sigma$*, then* θ_1 *is guaranteed pursuit time in the game* (2).

Proof: A. We construct the pursuer's strategy on [0, θ_1] as follows

$$u_k(t,v) = v_k(t) - H_k^*(-t)\left[H_k(-\theta_1)z_k^1 - z_k^0\right]B_k(\theta_1),\ 0\le t\le\theta_1,\ k=1,2,... \tag{14}$$

Show that strategy (14) is admissible. Using the Minkowskii inequality and the fact that $v(\cdot)$ belongs to $S(\sigma)$, we have

$$\begin{aligned}\left(\sum_{k=1}^{\infty}\int_0^{\theta_1}|u_k(s)|^2ds\right)^{1/2} &= \left(\sum_{k=1}^{\infty}\int_0^{\theta_1}\left|v_k(s) - H_k^*(-s)\left[H_k(-\theta_1)z_k^1 - z_k^0\right]B_k(\theta_1)\right|^2ds\right)^{1/2}\\ &\le \left(\sum_{k=1}^{\infty}\int_0^{\theta_1}|v_k(s)|^2ds\right)^{1/2}\\ &+\left(\sum_{k=1}^{\infty}\int_0^{\theta_1}\left|H_k^*(-s)\left[H_k(-\theta_1)z_k^1 - z_k^0\right]B_k(\theta_1)\right|^2ds\right)^{1/2}\\ &\le \sigma + \left(\sum_{k=1}^{\infty}\left|H_k(-\theta_1)z_k^1 - z_k^0\right|^2 B_k^2(\theta_1)\int_0^{\theta_1}e^{2\alpha_k s}ds\right)^{1/2}.\end{aligned} \tag{15}$$

Applying the obvious inequality $|x-y|^2 \le 2|x|^2 + 2|y|^2$ in (15), we have

$$\begin{aligned}\left(\sum_{k=1}^{\infty}\int_0^{\theta_1}|u_k(s)|^2 ds\right)^{1/2} &\le \sigma + \left(\sum_{k=1}^{\infty}\left(2|z_k^0|^2 + 2|z_k^1|^2 e^{2\alpha_k\theta_1}\right)B_k^2(\theta_1)\int_0^{\theta_1} e^{2\alpha_k s}ds\right)^{1/2} \\ &= \sigma + \left(\sum_{k=1}^{\infty}\left(2|z_k^0|^2 B_k(\theta_1) + 2|z_k^1|^2 A_k(\theta_1)\right)\right)^{1/2} \\ &= \sigma + \rho - \sigma = \rho.\end{aligned}$$

B. Show that pursuit is completed. Using (11) and (14), we obtain

$$\begin{aligned}z_k(\theta_1) &= H_k(\theta_1)\Big(z_k^0 + \int_0^{\theta_1} H_k(-s)v_k(s)ds \\ &\quad - \int_0^{\theta_1} H_k(-s)\left(v_k(s) - H_k^*(-s)\left[H_k(-\theta_1)z_k^1 - z_k^0\right]B_k(\theta_1)\right)ds\Big) \\ &= H_k(\theta_1)\left(z_k^0 + \left[H_k(-\theta_1)z_k^1 - z_k^0\right]B_k(\theta_1)\int_0^{\theta_1} e^{2\alpha_k s}ds\right) \\ &= H_k(\theta_1)z_k^0 + H_k(\theta_1)\left[H_k(-\theta_1)z_k^1 - z_k^0\right] = z_k^1.\end{aligned}$$

The proof of the theorem is complete.

CONCLUSION

In the present paper, a pursuit differential game problem described by an infinite system of 2-systems of 1st-order differential equations has been studied in Hilbert space l_2. Integral constraints on the control functions of the players are imposed.

We have solved a control problem to transfer the state of the system (3) from the given initial state z^0 to another given state z^1 for finite time. Also, we have obtained sufficient conditions for the completion of the game, we have given an equation for guaranteed pursuit time and constructed a strategy for the pursuer to complete the pursuit in the game (2).

ACKNOWLEDGMENTS

This research was partially supported by Geran Putra Berimpak, UPM/700-2/1/GPB/2017/9590-
200.

REFERENCES

Alias, I. A., Ibragimov, G., & Rakhmanov, A. (2017). Evasion differential game of infinitely many evaders from infinitely many pursuers in Hilbert space. Dynamic Games and Applications, 7(3), 347-359.

Avdonin, I., Avdonin, S. A., & Ivanov, S. A. (1995). Families of exponentials: the method of moments in controllability problems for distributed parameter systems. Cambridge University Press.

Azamov, A. A., & Ruziboyev, M. B. (2013). The time-optimal problem for evolutionary partial differential equations. Journal of Applied Mathematics and Mechanics, 77(2), 220-224.

Azamov, A. A., & Samatov, B. (2000). Π-strategy. An elementary introduction to the theory of differential games. Taskent: National Univ. of Uzb.

Butkovsky, A. (1969). Theory of optimal control of distributed parameter systems, New York: Elsevier.

Chernous' ko, F. L. (1992). Bounded controls in distributed-parameter systems. Journal of Applied Mathematics and Mechanics, 56(5), 707-723.

Chikrii, A. A., & Belousov, A. A. (2010). On linear differential games with integral constraints. Proceedings of the Steklov Institute of Mathematics, 269(1), 69.

Friedman, A. (1971). Differential games, New York: John Wiley and Sons.

Huseyin, A., & Huseyin, N. (2012). Precompactness of the set of trajectories of the controllable system described by a nonlinear Volterra integral equation. Mathematical Modelling and Analysis, 17(5), 686-695.

Ibragimov, G. (2002). An optimal pursuit problem in systems with distributed parameters. Prikladnaya Matematika i Mekhanika, 66(5):753–759.

Ibragimov, G. (2013). Optimal pursuit time for a differential game in the Hilbert space l_2. Differential Equations, 6(8), 9.

Ibragimov, G. I. & Ja'afaru, A. B. (2011). Australian Journal of Basic and Applied Science, 5:736-742.

Ibragimov, G. I. (2013). The optimal pursuit problem reduced to an infinite system of differential equations. Journal of Applied Mathematics and Mechanics, 77(5):470–476.

Ibragimov, G. I., Azamov, A. A., & Khakestari, M. (2011). Solution of a linear pursuit-evasion game with integral constraints. ANZIAM Journal, *52*, 59-75.

Ibragimov, G. I., Azamov, A., & Hasim, R. M. (2008). Existence and uniqueness of the solution for an infinite system of differential equations. Journal KALAM, International Journal of Mathematics and Statistics, 1(2), 9-14.

Ibragimov, G., & Salleh, Y. (2012). Simple motion evasion differential game of many pursuers and one evader with integral constraints on control functions of players. Journal of Applied Mathematics, 2012.

Ibragimov, G., Alias, I. A., Waziri, U., & Ja'afaru, A. B. (2017). Differential Game of Optimal Pursuit for an Infinite System of Differential Equations. Bulletin of the Malaysian Mathematical Sciences Society, 1-13.

Ibragimov, G., Rasid, N. A., Kuchkarov, A., & Ismail, F. (2015). Multi pursuer differential game of optimal approach with integral constraints on controls of players. Taiwanese Journal of Mathematics, 19(3), 963-976.

Isaacs, R. (1965). Differential games, a mathematical theory with applications to optimization, control and warfare, New York: Wiley.

Konovalov, A. P. (1987). Linear differential evasion games with lag and integral constraints. Cybernetics, 41-45.

Krasovskiĭ, N. N. & Subbotin, A. I. (1988). Game-theoretical control problems, New York: Springer.

Kuchkarov, A. S. (2013). On a differential game with integral and phase constraints. Automation and Remote Control, 74(1), 12-25.

Lewin, J. (1994). Differential Games, London: Springer.

Lokshin, M. D. (1990). Differential games with integral constraints on disturbances. Journal of Applied Mathematics and Mechanics, 54(3), 331-337.

Mamatov, M. S. (2008). On the theory of differential pursuit games in distributed parameter systems. Automatic Control and Computer Sciences, 43(1), 1-8.

Nikolskii, M. S. (1969). The direct method in linear differential games with integral constraints. Controlled systems, IM, IK, SO AN SSSR, 2, 49-59.

Okhezin, S. P. (1977). Differential encounter-evasion game for parabolic system under integral constraints on the player's controls. Prikl Mat I Mekh,41(2):202–209.

Petrosyan, L. A. (1993). Differential Games of Pursuit, Singapore, London: World Scientific.

Pontryagin, L. S. (1988). Selected Scientific Works. Vol. II.

Samatov, B. T. (2013). Problems of group pursuit with integral constraints on controls of the players. I. Cybernetics and Systems Analysis, 49(5), 756-767.

Satimov, N. Y., & Tukhtasinov, M. (2006). Game problems on a fixed interval in controlled first-order evolution equations. Mathematical notes, *80*(3-4), 578-589.

Satimov, N., Rikhsiev, B. B., & Khamdamov, A. A. (1983). On a pursuit problem for n-person linear differential and discrete games with integral constraints. Sbornik: Mathematics, 46(4), 459-471.

Solomatin, A. M. (1984). A game theoretic approach-evasion problem for a linear system with integral constraints imposed on the player control. Journal of Applied Mathematics and Mechanics, 48(4), 401-405.

Subbotin, A. and Ushakov, V. N. (1975). Alternative for an encounter-evasion differential game with integral constraints on the players' controls. J. Appl. Maths Mekhs, 39(3):367–375.

Tukhtasinov, M., & Mamatov, M. S. (2008). On pursuit problems in controlled distributed systems. Mathematical notes, 84(1-2), 256-262.

Tukhtasinov, M., & Mamatov, M. S. (2009). On transfer problems in control systems. Differential Equations, 45(3),439-444.

Malaysian Journal of Science Special Issue (1) 2019: 55-66

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

PERFORMANCE ANALYSIS OF FOUR-POINT EGAOR ITERATIVE METHOD APPLIED TO POISSON IMAGE BLENDING PROBLEM

Jeng Hong Eng[1*], Azali Saudi[2] and Jumat Sulaiman[3]

[1,3]Faculty of Science and Natural Resources, Universiti Malaysia Sabah,
88400 Kota Kinabalu, Sabah, Malaysia
[2]Knowledge Technology Research Unit, Faculty of Computing and Informatics, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia
*Corresponding author:jenghong93@gmail.com[1], azali@ums.edu.my[2] and jumat@ums.edu.my[3]
Received: 29th Oct 2018 Revised: 29th Oct 2018 Accepted: 19th Dec 2018
DOI : https://doi.org/10.22452/mjs.sp2019no1.5

ABSTRACT Poisson image blending is one of the useful editing tools in image processing to generate a desirable image which is impossible to acquire. The key to this solution is to obtain the unique solution of Poisson equation. Thus, the motivation of this paper is to examine the effectiveness of 4-EGAOR iterative method to solve the linear system generated from the Poisson image blending problem. To evaluate its effectiveness, the formulation and implementation of 4-EGAOR, SOR and AOR iterative methods are demonstrated. The numerical results revealed that 4-EGAOR iterative method improved the computational time taken and reduced the number of iterations used. In fact, the new images generated by the proposed block iterative method give a satisfactory visual effect.

Keywords Poisson equation, Poisson image blending, finite difference method, 4-EGAOR iteration, five-point Laplacian operator

ABSTRAK Penyuntingan imej Poisson merupakan salah satu alat pengeditan yang berguna dalam dunia pemprosesan imej untuk menghasilkan suatu imej yang diinginkan di mana ia adalah mustahil untuk diperoleh. Kunci penyelesaian permasalahan ini ialah mendapatkan penyelesaian unik persamaan Poisson. Oleh itu, motivasi kajian ini adalah untuk menganalisis kecekapan kaedah lelaran 4-EGAOR untuk menyelesaikan sistem linear yang terjana daripada permasalahan penyuntingan imej Poisson. Untuk menilai kecekapannya, perumusan dan pelaksanaan kaedah 4-EGAOR, SOR dan AOR telah ditunjukkan. Dapatan kajian menunjukkan bahawa kaedah lelaran 4-EGAOR telah mengurangkan masa dan bilangan lelaran untuk menyelesaikan permasalahan imej Poisson berbanding dengan kaedah lelaran SOR dan AOR. Kualiti imej yang dihasilkan oleh semua kaedah lelaran yang dicadangkan tiada mempunyai perbezaan yang ketara.

INTRODUCTION

When the photographs are represented in digital form, it is known as digital images and when it is being processed by a digital computer, it is regarded as digital image processing. Digital image processing is present in many aspects of our daily life, with broad applications such as medical imaging, geographical mapping, remote sensing and observation of the earth resources. The origins of digital image processing can be traced back to Gonzalez and Woods (2001).

Nevertheless, in this research study, we focus on examining the Poisson image blending problem, which is also known as Poisson Image Editing (PIE). Solving image blending problem by imposing Poisson partial differential equation with Dirichlet boundary condition was invented by Pérez *et al*. (2003). Generally, PIE is defined as inserting a desired region from source image into the target image seamlessly by solving the Poisson equation. However, the Dirichlet boundary condition often caused the issue of color inconsistency. An extra inner constrained boundary condition was added to the edited region by Qin *et al*. (2008), therefore the Laplacian values was enlarged in order to overcome the issue.

In addition, Morel *et al*. (2012) reviewed that PIE is a lengthy process which involved a longer composition time. On account of this, Fourier method was implemented. This is a fast and efficient non-iterative type of solver. More recently, Hussain and Kamel (2015) proposed the method of image pyramid and divide-and-conquer to solve the Poisson equation more efficiently. The Poisson equation was solved for three pyramid levels in this method. Besides, modified Poisson blending (MPB) solver had proposed by Afifi and Hussain (2015) in order to overcome the issues of bleeding artifacts and colour bleeding. To overcome the bleeding artifacts problem which occurred in the traditional methods, both the boundary pixels on the source and destination images were considered.

There are plenty of techniques being applied in Poisson image blending problem and their efficiency in resolving this problem are high. Generally, the linear system generated from the Poisson equation can be solved by direct and iterative methods. In this paper, we discretized the Poisson equation based on finite difference approach and then solved the linear system by using iterative method. Only few researches employed iterative method in Poisson image blending problem, Hussain and Kamel (2015), Eng *et al*. (2017a), Eng *et al*. (2017b), Eng *et al*. (2018a) and Eng *et al*. (2018b). Thus, this paper is examining the efficiency of the Four-Point Explicit Group Accelerated Over Relaxation (4-EGAOR) when applied to Poisson image blending problem as none of the researches have employed this technique in the problem.

In the meantime, Martino *et al*. (2016) evaluated that finite difference approach is well performed in most of the Poisson image blending problem. Thus, three selected iterative methods based on this approach are proposed in this study: 4-EGAOR and point iterative methods, Successive Over Relaxation (SOR) and Accelerated Over Relaxation (AOR). Besides solving image blending problem, 4-EGAOR, SOR and AOR iterative methods and its variants had been used to solve other problems as well, for example in Akhir *et al*. (2011), Dahalan *et al*. (2017) and Saudi and Sulaiman (2017). Moreover, the Laplace's equation which is generated from Poisson equation by simply assigning the value of zero to the right hand side of Poisson equation, is also applied in path planning problem (Saudi & Sulaiman, 2012; Saudi & Sulaiman, 2016).

MODEL DESCRIPTION

An image is a two-dimensional array of finite number of pixels where each of the pixels represent its own intensity value or brightness. The coordinate system of an image is the rotated conventional two-dimensional Cartesian coordinate system by 90º in clockwise direction. Besides, a colour image is formed by various mixtures of three primary colours, Red, Green and Blue (RGB) and the size or resolution of an image is determined by the number of rows and columns in the image. Referring to Figure 1, the image is partitioned into many smaller square parts where each of them is representing a pixel.

Figure 1. Illustration of an image partitioned into 28 × 18 small square blocks.

For convenience purpose, the image shown in Figure 1 will be simplified by considering the location of the pixels from the solution domain, as shown in Figure 2.

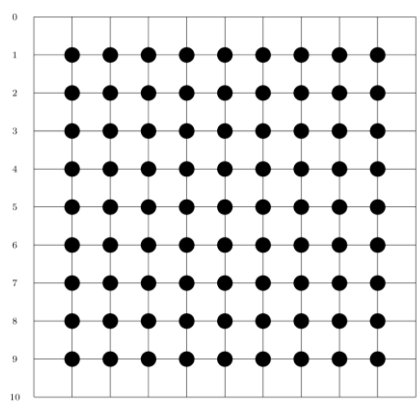


Figure 2. Finite grid network of pixels for n=10.

PIE is a type of gradient domain image editing method where it manipulates the gradients instead of the pixels of the image. The Poisson blending process begins by selecting the desired region Ω with $\partial\Omega$ defined as its boundary from a source image

g. Then, extract the desired region and blend into a destination image f^* to generate a new output image f. As stated by Pérez *et al*. (2003), a guidance vector field v needs to be generated first from the source image. After that, a new set of intensity values f in the desired region which will minimize the difference between the gradient of the new image and the vector field is computed. The minimization problem is defined as,

$$\min_f \iint_O |\nabla f - v|^2 \text{ with } f|_{\partial O} = f^*|_{\partial O} \tag{1}$$

where the intensity values are set to be the same at the boundary to generate a seamless image. The intensity values are extracted from the image itself. It will be used as the initial values for the generated linear system constructed from the discretization Poisson equation via finite difference method. The details are discussed in the following section.

The solution of the minimization problem (1) is the unique solution of the Poisson equation with Dirichlet boundary condition,

$$\Delta f = \text{div } \mathbf{v} \text{ at } O \text{ with } f|_{\partial O} = f^*|_{\partial O} \tag{2}$$

To generate a new image seamlessly, the vector field v is a gradient field directly extracted from the source image and thus, Equation (2) can be rewritten as,

$$\Delta f = \Delta g \text{ at } O \text{ with } f|_{\partial O} = f^*|_{\partial O} \tag{3}$$

The Δ in Equation (3) denotes the Laplacian operator.

DERIVATION AND IMPLEMENTATION OF THE PROPOSED METHOD

To implement the three proposed iterative methods, Poisson equation is first to be discretized based on finite difference approach via Laplacian operator. The standard two-dimensional Poisson equation is defined as,

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = g(x, y) \tag{4}$$

Equation (4) is then discretized via five-point Laplacian operator. From the discretization process of Equation (4), the approximation equation is derived as,

$$f_{i,j} \cong \frac{1}{4}\left[f_{i+1,j} + f_{i-1,j} + f_{i,j+1} + f_{i,j-1} - h^2 g_{i,j}\right] \tag{5}$$

where $h = \Delta x = \Delta y$. By adding a weighted parameter, ω to Equation (5), it can be redefined as,

$$f_{i,j}^{(k+1)} \cong \frac{\omega}{4}\left[f_{i+1,j}^{(k)} + f_{i-1,j}^{(k+1)} + f_{i,j+1}^{(k)} + f_{i,j-1}^{(k+1)} - h^2 g_{i,j}\right] + (1-\omega) f_{i,j}^{(k)} \qquad (6)$$

and by adding another accelerated parameter, r into Equation (6), it can also be redefined as,

$$f_{i,j}^{(k+1)} \cong \frac{r}{4}\left(f_{i-1,j}^{(k+1)} - f_{i-1,j}^{(k)} + f_{i,j-1}^{(k+1)} - f_{i,j-1}^{(k)}\right) + \frac{\omega}{4}\left(f_{i-1,j}^{(k)} + f_{i+1,j}^{(k)} + f_{i,j-1}^{(k)} + f_{i,j+1}^{(k)} - h^2 g_{i,j}\right) + (1-\omega) f_{i,j}^{(k)} \qquad (7)$$

Thus, Equation (6) and (7) is the formulation of SOR (Young, 1954) and AOR (Hadjidimos, 1978) iterative methods respectively with $1 \le \omega, r < 2$ (Ali & Chong, 2007; Yousif & Martins, 2008).

On the other hand, to implement the 4-EGAOR iterative method, let us consider a group of four points as shown in Figure 3 as follows,

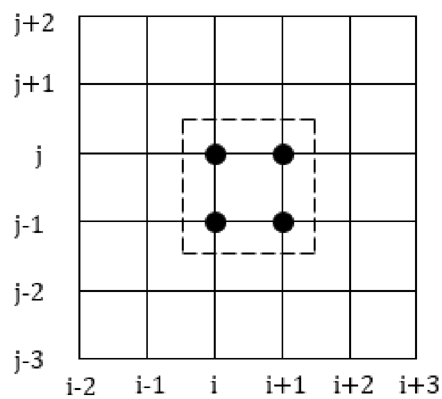


Figure 3. Four points block iterative method.

and the 4-EG iterative method (Saudi & Sulaiman, 2012; Evans, 1985) is defined as,

$$\begin{bmatrix} 4 & -1 & -1 & 0 \\ -1 & 4 & 0 & -1 \\ -1 & 0 & 4 & -1 \\ 0 & -1 & -1 & 4 \end{bmatrix} \begin{bmatrix} f_{i,j} \\ f_{i+1,j} \\ f_{i,j+1} \\ f_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix} \qquad (8)$$

where,

$S_1 = g_{i,j} + f_{i-1,j} + f_{i,j-1}$,
$S_2 = g_{i+1,j} + f_{i+2,j} + f_{i+1,j-1}$,
$S_3 = g_{i,j+1} + f_{i-1,j+1} + f_{i,j+2}$,
$S_4 = g_{i+1,j+1} + f_{i+2,j+1} + f_{i+1,j+2}$.

Then, the inverse of the coefficient matrix (8) is determined as follows,

$$\begin{bmatrix} f_{i,j} \\ f_{i+1,j} \\ f_{i,j+1} \\ f_{i+1,j+1} \end{bmatrix} = \frac{1}{24}\begin{bmatrix} 7 & 2 & 2 & 1 \\ 2 & 7 & 1 & 2 \\ 2 & 1 & 7 & 2 \\ 1 & 2 & 2 & 7 \end{bmatrix}\begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix} \quad (9)$$

To implement 4-EGAOR (Martins *et al*., 2002) iterative method from Equation (9), let,

$$\begin{aligned} S_a &= \frac{1}{24}[S_1 + 2S_2 + 2S_3 + S_4], \\ S_b &= \frac{1}{24}[2S_1 + S_2 + S_3 + 2S_4]. \end{aligned} \quad (10)$$

$$\begin{aligned} a_1 &= f_{i-1,j}^{(k+1)} - f_{i-1,j}^{(k)}, \\ a_2 &= f_{i,j-1}^{(k+1)} - f_{i,j-1}^{(k)}, \\ a_3 &= f_{i+1,j-1}^{(k+1)} - f_{i+1,j-1}^{(k)}, \\ a_4 &= f_{i-1,j+1}^{(k+1)} - f_{i-1,j+1}^{(k)}. \end{aligned} \quad (11)$$

Then, Equations (10) and (11) are substituted into Equation (9) and two weighted parameters, ω and r with $1 \le \omega, r < 2$ are added. Thus, the 4-EGAOR iterative method can be implemented simultaneously by using the following formulation,

$$\begin{bmatrix} f_{i,j} \\ f_{i+1,j} \\ f_{i,j+1} \\ f_{i+1,j+1} \end{bmatrix}^{(k+1)} = \frac{r}{24}\begin{bmatrix} 7 & 7 & 2 & 2 \\ 2 & 2 & 7 & 1 \\ 2 & 2 & 1 & 7 \\ 1 & 1 & 2 & 2 \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} + \frac{\omega}{4}\begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix} + \omega\begin{bmatrix} S_a \\ S_b \\ S_b \\ S_a \end{bmatrix} + (1-\omega)\begin{bmatrix} f_{i,j} \\ f_{i+1,j} \\ f_{i,j+1} \\ f_{i+1,j+1} \end{bmatrix}^{(k)} \quad (12)$$

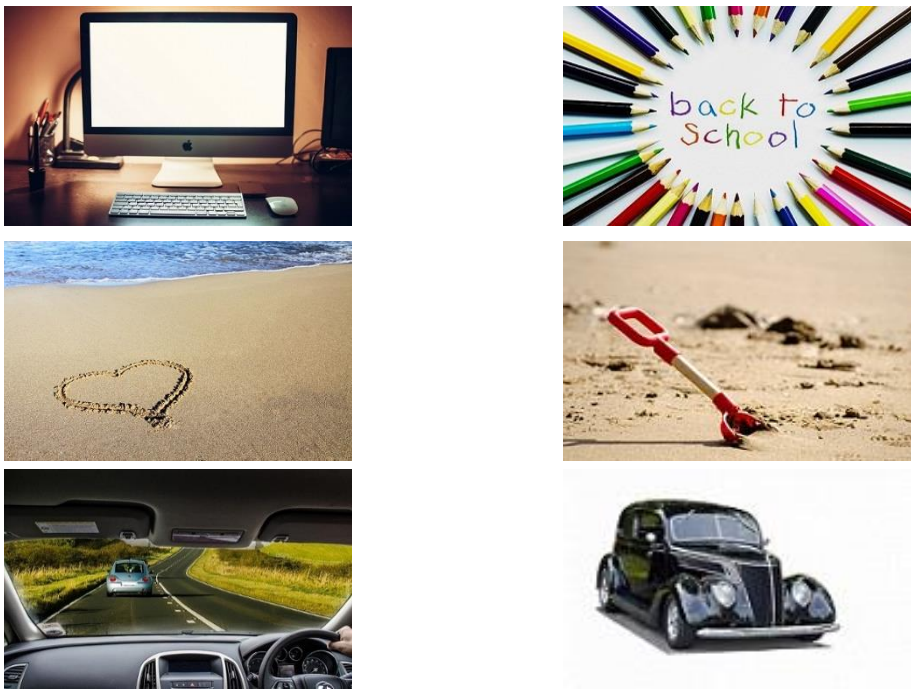
Algorithm 1: 4-EGAOR iterative method

i. Select desired region from source image.
ii. Map the desired region onto target image.
iii. Set the initial value $\underline{f}^{(0)} = 0$ and $\varepsilon = 1.0$.
iv. For all groups of four node points in the selected region, use Equation (12) to compute $f_{i,j}^{(k+1)}, f_{i+1,j}^{(k+1)}, f_{i,j+1}^{(k+1)}$ and $f_{i+1,j+1}^{(k+1)}$
v. For all ungroup node points in the selected region, use Equation (7) to compute.
vi. Examine the convergence. If it converges, go to step vii. Else, go to step iv.
vii. Display the new images obtained.

RESULTS AND DISCUSSION

In order to verify the potency of the proposed methods, three sets of images with various sizes are chosen. Each set of the images comprises of source and target images were taken from Public Domain Pictures.net refer to Figure 4. To evaluate the performance of the three selected iterative methods, two parameters are used, the number of iterations involved and the computational time taken to generate a new blended image. In this paper, we employed Root of Sum of Square (RSS) (Pérez *et al*., 2003), as stopping criterion with 1.0 threshold.

(i)
(ii)
(iii)



(a) (b)

Figure 4. (a) Target images. (b) Source images.

The performance evaluation of SOR, AOR and 4-EGAOR in terms of number of iterations used is presented in Figure 5 and the values of ω and r used are optimal. Referring to Figure 5, the number of iterations used by 4-EGAOR has reduced as compared to SOR and AOR iterative methods. It has decreased approximately 19.1 – 26.1% as compared to SOR iterative numerical result for comparison in the AOR iterative method. Meanwhile, the method and 7.3 – 21.4% as compared to composing time is presented in Figure 6. As compared to SOR iterative method, the composing time of 4-EGAOR is reduced by approximately 15.2 – 17.6% while compared to AOR iterative method, it has reduced approximately 9.6 – 15.5%. The numerical results obtained is based on the size of the selected edited region.

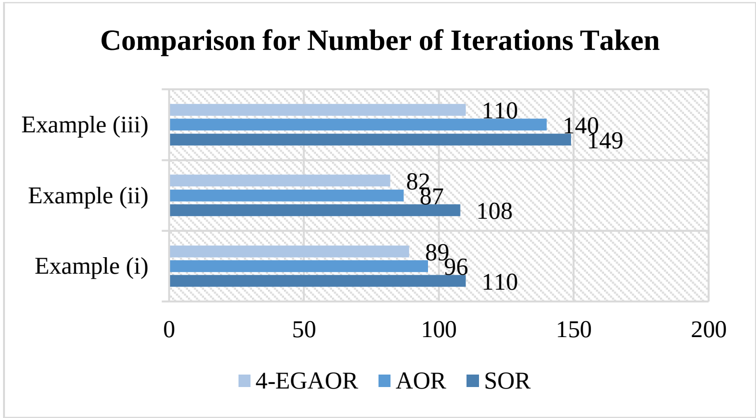


Figure 5. Number of iterations used.

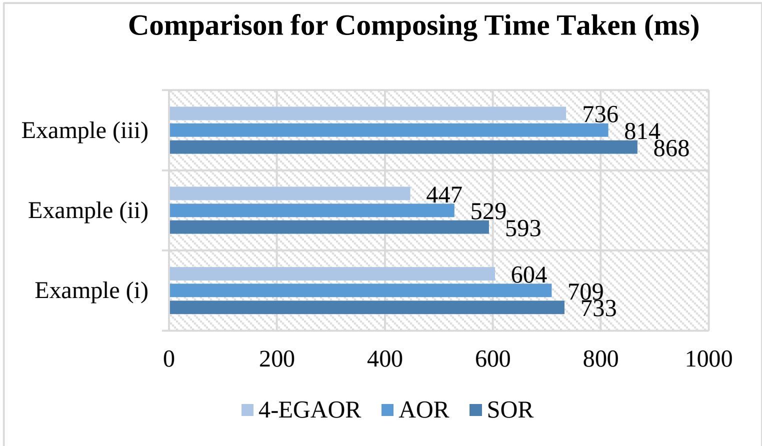


Figure 6. Composing time taken.

Subsequently, the new generated images after blending process are shown in Figures 7, 8 and 9. In order to assess the quality of the images produced, we used quantitative analysis. The quality metric used in this paper is the structural similarity index measure (SSIM) by Wang and Bovik (2002). The images produced by SOR method are used as reference image and then compared with the images produced by AOR and 4-EGAOR methods. The index values obtained are tabulated in Table 1, as follows,

Table 1. SSIM Index Values

Experiment	Iterative Methods	
	AOR	4-EGAOR
(i)	1.0000	0.9999
(ii)	1.0000	1.0000
(iii)	1.0000	1.0000

The range of SSIM index varies from -1 to 1 and value 1 indicates that both images are similar. From Table 1, all the SSIM index values obtained are close to 1 with four decimal places, which implies that the images produced by all the proposed iterative methods are very similar.

(i)

a. SOR ($\omega = 1.88$) b. AOR ($\omega = 1.86, r = 1.90$) c. 4-EGAOR ($\omega = 1.84, r = 1.92$)

Figure 7. Output images generated for Example (i) with the size of 10229 pixels.

(ii)

a. SOR ($\omega = 1.78$) b. AOR ($\omega = 1.75, r = 1.82$) c. 4-EGAOR ($\omega = 1.75, r = 1.79$)

Figure 8. Output images generated for Example (ii) with the size of 5204 pixels.

(iii)

a. SOR ($\omega = 1.90$) b. AOR ($\omega = 1.86, r = 1.91$) c. 4-EGAOR ($\omega = 1.85, r = 1.90$)

Figure 9. Output images generated for Example (iii) with the size of 6186 pixels.

CONCLUSION

In this study, both point and block iterative methods are implemented for solving Poisson image blending problem in order to examine its efficiency. From the numerical results obtained, 4-EGAOR performed the best as compared to SOR and AOR iterative methods in terms of both number of iterations and composing time. This is because the 4-

EGAOR iterative method implements the complexity reduction technique by calculating a group of 4 points simultaneously in one loop of iteration.
Thus, it performed better than the proposed point iterative methods. Finally, the new blended images generated from the three proposed iterative methods showed excellent quality as evaluated using the SSIM index.

REFERENCES

Afifi, M. & Hussain, K.F. (2015). MPB: A modified poisson blending technique. Computational Visual Media 1(4): 331-341.

Akhir, M.K.M., Othman, M., Sulaiman, J., Majid, Z.A. & Suleiman, M. (2011). Half-sweep modified successive overrelaxation for solving two-dimensional helmholtz equations. Australian Journal of Basic and Applied Sciences 5(12): 3033-3039.

Ali, N.H.M. & Chong, L.S. (2007). Group accelerated overrelaxation methods on rotated grid. Applied Mathematics and Computation 191: 533-542.

Dahalan, A.A., Saudi, A. & Sulaiman, J. (2017). Numerical evaluation of mobile robot navigation in static indoor environment via EGAOR Iteration. Journal of Physics: Conference Series 890: 012064.

Eng, J.H., Saudi, A. & Sulaiman, J. (2017a). Numerical assessment for poisson image blending problem using MSOR iteration via five-point laplacian operator. Journal of Physics: Conference Series 890: 012010.

Eng, J.H., Saudi, A. & Sulaiman, J. (2017b). Numerical analysis of the explicit group iterative method for solving poisson image blending problem. International Journal of Imaging and Robotics 17(4): 15-24.

Eng, J.H., Saudi, A. & Sulaiman, J. (2018a). Performance analysis of the explicit decoupled group iteration via five-point rotated laplacian operator in solving poisson image blending problem. Indian Journal of Science and Technology 11(12).

Eng, J.H., Saudi, A. & Sulaiman, J. (2018b). Implementation of rotated five-point laplacian operator for poisson image blending problem. Advanced Science Letters 24(3): 1727-1731.

Evans, D.J. (1985). Group explicit iterative methods for solving large linear systems. International Journal of Computer Mathematics 17: 81-108.

Gonzalez, R.C. & Woods, R.E. (2001). Digital Image Processing 2nd Edition, New Jersey: Prentice Hall.

Hadjidimos, A. (1978). Accelerated overrelaxation method. Mathematics of Computation 32: 149-157.

Hussain, K.F. & Kamel, R.M. (2015). Efficient poisson image editing. Electronic Letters on Computer Vision and Image Analysis 14(2): 45-57.

Martino, J.M.D., Facciolo, G. & Meinhardt-Llopis, E. (2016). Poisson image editing. Image Processing On Line 6: 300-325.

Martins, M.M., Yousif, W.S. & Evans, D.J. (2002). Explicit group AOR method for solving elliptic partial differential equations. Parallel and Scientific Computations 10(2): 411-422.

Morel, J.M., Petro, A.B. & Sbert, C. (2012). Fourier implementation of poisson image editing. Pattern Recognition Letters 33: 342-348.

Pérez, P., Gangnet, M. & Blake, A. (2003). Poisson image editing. ACM Transactions and Graphics 313-318.

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=211753&picture=office-computer (accessed December 29, 2017).

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=52663&picture=school (accessed December 29, 2017).

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=4433&picture=sand-heart-and-ocean (accessed December 29, 2017).

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=36643&picture=games-on-the-beach (accessed December 29, 2017).

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=87913&picture=vintage-automobile (accessed December 29, 2017).

Bobek Ltd. (2007) Public Domain Pictures.net. From: https://www.publicdomainpictures.net/en/view-image.php?image=76803&picture=traveling-by-car (accessed December 29, 2017).

Qin, C., Wang, S. & Zhang, X. (2008). Image editing without color inconsistency using modified poisson equation. In International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 15-17 August, pp. 397-401, IEEE, China: Harbin.

Saudi, A. & Sulaiman, J. (2012). Robot path planning using four point-explicit group via nine-point laplacian (4EG9L) iterative method. Procedia Engineering 41: 182-188.

Saudi, A. & Sulaiman, J. (2016). Path planning simulation using harmonic potential fields through four point-EDGSOR method via 9-point laplacian. Jurnal Teknologi 78(8-2): 12-24.

Saudi, A. & Sulaiman, J. (2017). Application of harmonic functions through modified SOR (MSOR) method for robot path planning in indoor structured environment. International Journal of Imaging and Robotics 17(3): 77-90.

Wang, Z. & Bovik, A.C. (2002). A universal image quality index. IEEE Signal Processing Letters 9(3): 81-84.

Young, D.M. (1954). Iterative methods for solving partial difference equations of elliptic type. Transactions of the American Mathematical Society 76: 92-111.

Yousif, W.S. & Martins, M.M. (2008). Explicit de-coupled group AOR method for solving elliptic partial differential equations. Neural, Parallel and Scientific Computations 16: 531-542.

Malaysian Journal of Science Special Issue (1) 2019: 67-73

ICMSS2018
3rd International Conference of Mathematical Sciences and Statistics
6th - 8th February 2018

ANOTHER PROOF OF WIENER'S SHORT SECRET EXPONENT

Muhammad Asyraf Asbullah[1*], Muhammad Rezal Kamel Ariffin[2]

[1,2]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia.
[2]Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia.
*Corresponding author: ma_asyraf@upm.edu.my
Received: 29th Oct 2018 Revised: 29th Oct 2018 Accepted: 19th December 2018
DOI: https://doi.org/10.22452/mjs.sp2019no1.6

ABSTRACT Wiener's short secret exponent attack is a well-known crypt-analytical result upon the RSA cryptosystem using a Diophantine's method called continued fractions. We recall that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later, the upper bound was improved satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof to Wiener's short secret exponent satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We remark that our result is slightly better than the previously mentioned attacks.

Keywords: RSA cryptosystem, continued fractions, secret exponent, cryptanalysis, Wiener's theorem.

INTRODUCTION

From the beginning of time until 1970's, the technology for practicing secret communication, which is widely known as encryption and decryption, was always done in a symmetrical manner. In early 1978, the RSA cryptosystem (Rivest, R., Shamir, A. and Adleman, L, 1978) that was introduced (abbreviated accordingly to its creator; Rivest, Shamir, and Adleman) became a phenomenon in the world of secrecy of which was regarded as the first practical realization of the asymmetric cryptosystem as opposed to symmetric cryptosystem.

The core design of the RSA cryptosystem is based on the number-theoretic object called the integer factorization problem. The intractability to solve the said problems with current computational power is the source of its security (i.e. particularly in factoring of the form $N = pq$). Additionally, another source of security of RSA cryptosystem lies on the difficulty to solve the RSA key equation of the form $ed \equiv 1(\bmod \phi(N))$ where $\phi(N) = (p-1)(q-1)$. Solving the RSA key equation meaning that the objective is to recover the unknown value of d, given only e and N. This will be the focus in this work.

For practicality purpose, the private exponent d of RSA decryption is tended to be made small, thus the RSA cryptosystem will have tremendous decryption speed. However, if d is upper bounded by $\frac{1}{3}N^{1/4}$, then Wiener (Wiener M., 1990) observe that such secret exponent d can be easily solved in polynomial time. The observation is made based on the key equation $ed - \phi(N)k = 1$ and can be solved efficiently via continued fraction method.

The main idea behind Wiener's attack to solve for the parameter d that satisfy the inequality $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$. In fact, a classical Legendre's theorem of continued fraction expansion shows that the value of $\frac{k}{d}$ could be efficiently obtained from the list of convergent of $\frac{e}{N}$. Thus, as the security of the RSA cryptosystem matters, it was proposed that such d must be generated by choosing an integer larger than $\frac{1}{3}N^{1/4}$ to resist Wiener's attack.

Afterward, (de Weger, B., 2002) demonstrated that the Legendre's theorem is satisfied upon $\left|\frac{e}{N-2N^{1/2}+1} - \frac{k}{d}\right|$. As a result, any secret integer d less than $\frac{N^{3/4}}{|p-q|}$ in no longer secure for RSA cryptosystem since $\frac{k}{d}$ effciently obtained from a convergent of the continued fraction $\frac{e}{N-2N^{1/2}+1}$. Note that (de Weger, B., 2002) considered the situation when p and q are too close (i.e.the difference of two primes, $|p-q|$ is small). Alternatively, even though p and q are not close, (Maitra, S. and Sarkar, S., 2008) considered the case of the primes p and $2q$ are too close. Furthermore, (Maitra, S. and Sarkar, S., 2008) showed that by replacing the $N - 2N^{1/2} + 1$ from the result in (de Weger, B., 2002) with $N - \frac{3}{\sqrt{2}}\sqrt{N} + 1$, then $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N-\frac{3}{\sqrt{2}}\sqrt{N}+1}$.

Motivated from the earlier work of (de Weger, B., 2002) and (Maitra, S. and Sarkar, S., 2008) of utilizing a good approximation of $\phi(N)$ methodology, (Asbullah, M. A. and Ariffin, M. R. K., 2015) extended such cryptanalysis technique to the RSA modulus of type $N = p^2q$. A recent survey of RSA-like cryptosystems that implement such modulus can be found in (Asbullah, M. A. and Ariffin, M. R. K., 2014; Asbullah, M. A. and Ariffin, M. R. K., 2016c). The continued fraction technique is also widely used for algebraic cryptanalysis such as in (Asbullah, M. A. and Ariffin, M. R. K., 2016a) and (Asbullah, M. A. and Ariffin, M. R. K., 2016b)

We recall that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later, Nitaj (Nitaj, A., 2013) revisited the Wiener's theorem and proof. As a result, the upper bound was improved satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof to Wiener's short secret exponent satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We remark that our result is slightly better than the previously mentioned attacks in (Wiener M., 1990) and (Nitaj, A., 2013).

This paper was written in five main sections. In Section 2 we give definitions and useful theorems that are needed in our work. Section 3 provides mathematical proof of our result. We illustrate two numerical examples to show how the attack was conducted and performance analysis by comparing with Wiener's (Wiener M., 1990) and Nitaj's (Nitaj, A., 2013) attack's, respectively in Section 4. Finally, in Section 5 we end with a conclusion of our work.

PRELIMINARIES

In this section, we state the definition of continued fraction and useful theorems that form the basis for this paper. These include the result from (Wiener M., 1990) and (Nitaj, A., 2013).

Definition 2.1 (Continued fraction) *Each rational number x can be written as an expression of the form*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}}$$

A simple way to show the above expression is by the form $x = [a_0, a_1, a_2 \dots . a_n]$. We define that the i^{th} term from the list of the continued fraction to be $[a_0, a_1, a_2, \dots, a_i]$ for $i \geq 0$.

An important result on continued fractions that will be used is the following theorem.

Theorem 2.2 (Legendre's Theorem) *Suppose x is written in its continued fraction expansion $[a_0, a_1, a_2, \dots]$ form. If $y, z \in \mathbb{Z}$ and coprime such that*

$$|x - \frac{y}{z}| < \frac{1}{2z^2}$$

then $\frac{y}{z}$ is a rational number amongst the continued fraction's convergent of x.

Suppose $N = pq$ is an RSA modulus where the bit-length of the primes p and q are in the same size (i.e. $q < p < 2q$). Such condition will be used throughout this paper.

Theorem 2.3 (Wiener's Theorem) *Let e be an RSA public exponent and d be the RSA private exponent satisfying the relation $ed - k\phi(N) = 1$. Let $d < \frac{1}{3}N^{\frac{1}{4}}$, then the integer k and d appeared the continued fraction's convergent of $\frac{e}{N}$.*

Later, Nitaj (2013) refine the bound of d as stated in the following theorem.

Theorem 2.4 (Nitaj, A., 2013). *The integer k and d can be obtained from the convergent of the continued fraction of $\frac{e}{N}$, if $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$.*

OUR RESULT

In comparison to the (Wiener M., 1990) and (Nitaj, A., 2013) bounds of which $d < \frac{1}{3}N^{1/4}$ and $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$, respectively, our bound is fixed to $d < \frac{1}{2}N^{1/4}$. We begin with the following lemma.

Lemma 3.1 *Suppose we have the prime factors p and q with $q < p < 2q$ and let $N = pq$ be the RSA modulus. Then*

$$\frac{1}{2^{1/2}}N^{1/2} < q < N^{1/2} < p < 2^{1/2}N^{1/2}$$

and

$$p + q > 2N^{1/2}$$

Proof. The first statement is straight forward. Now, we provide the proof for the second statement. Observe the relation of $(p + q)^2 = (p - q)^2 + 4N$. Thus, directly gives $p + q > 4N > 2N^{1/2}$.

We prove our main result as follows.

Theorem 3.2 *Suppose $ed - \phi(N)k = 1$ be the RSA key equation. If $d < \frac{1}{2}N^{1/4}$, then the* *secret value of k and d are easily recovered from the continued fraction's convergent of $\frac{e}{N}$.*

Proof. Let $ed - \phi(N)k = 1$ be the RSA key equation. Thus, such equation can be transformed as follows.

$$ed - k(N + 1 - p - q) = 1$$

$$ed - Nk = 1 - k(p + q - 1) \qquad (1)$$

Divides both sides of (1) by Nd and take the modulus sign, thus we have

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{1 - k(p + q - 1)}{Nd}\right| = \left|\frac{k(p + q - 1) - 1}{Nd}\right| < \frac{k(p + q - 1)}{Nd} \qquad (2)$$

Let the public RSA exponent $e < \phi(N)$, then rearranging $ed - \phi(N)k = 1$ we have

$$k = \frac{ed - 1}{\phi(N)} < \frac{ed}{\phi(N)} < d$$

Thus (2) straightforward gives

$$< \frac{p + q}{N}$$

For the Theorem 2.2 to work, it is adequate to show that $\frac{p+q}{N} < \frac{1}{2d^2}$.

Hence, by making the secret value d as the subject and plugging in the condition of Lemma 3.1, we have the following result

$$d < \left(\frac{N}{2(p + q)}\right)^{1/2} < \left(\frac{N}{2(2N^{1/2})}\right)^{1/2} = \frac{1}{2}N^{1/4}$$

COMPARATIVE ANALYSIS AND EXAMPLES

Table 1 compare our result in Section 3 with Wiener (1990) and Nitaj's (2013), respectively. The result, as shown in Table 1, indicate that regarding the attack and finding the secret parameter d, our result significantly improves the previous bound, which extends the Wiener's Theorem by 16.7%. While a comparison of with Nitaj's theorem reveals slight betterment, which is improves significantly by 1.5%.

Table 1: Comparison of the bounds on d for RSA modulo $N = pq$

Reference	Bounds for d
(Wiener M., 1990)	$d < \frac{1}{3}N^{\frac{1}{4}} \approx 0.333N^{\frac{1}{4}}$
(Nitaj, A., 2013)	$d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}} \approx 0.485N^{\frac{1}{4}}$
Our work	$d < \frac{1}{2}N^{\frac{1}{4}} \approx 0.500N^{\frac{1}{4}}$

Next, we provide algorithm workflow for factoring finding d and k based on Theorem 3.2 as follows.

Algorithm 4.1 Algorithm for factoring finding d and k based on Theorem 3.2
Input: The public key modulus (N, e) Output: The secret value d and k
1. Compute the continued fraction of $\frac{e}{N}$. 2. For each convergent $\frac{k'}{d'}$ of $\frac{e}{N}$, compute $N' = \frac{ed'-1}{k'}$. 3. For N' be an integer, proceed to Step 4. Else, repeat Step 2. 4. Compute $ed(\text{mod } N')$. 5. Output the $d = d'$ and $k = k'$ if $ed' \equiv 1(\text{mod } N')$. Else, repeat Step 2.

Turning now to the numerical examples on our result. Consider an RSA modulus N and an RSA public key e as follows.

$N = 13783853195340239094605568 58$
95128490833

$e = 11720373558924246698770660273$
5966338617

Example 4.1 *As an illustration of Theorem 3.2, suppose we find a list of the continued fraction expansion of $\frac{e}{N}$ using Algorithm 2. Let the above values of N and e satisfy all the requirements of Theorem 3.2. Hence, we will have a list of the continued fraction expansion of $\frac{e}{N}$ as follows.*

$$\left[0,1,\frac{5}{6},\frac{6}{7},\frac{142}{167},\cdots,\frac{572547398}{673349637},\frac{1438826739}{1692145429},\cdots\right]$$

We find that the secret the integer k and d are amongst the list the convergents of $\frac{e}{N}$. For each convergent $\frac{k'}{d'}$ of $\frac{e}{N}$, compute $N' = \frac{ed'-1}{k'}$. In fact, $\frac{k'}{d'} = \frac{1438826739}{1692145429}$ gives the integer

$N' = 137838531953402390922574540$
$097412197028.$

Next, since $ed' \equiv 1(\text{mod} N')$, thus according to Algorithm 2, we obtained $d = d' = 1692145429$ and $k = k' = 1438826739$.

Example 4.2 *Let we consider an RSA modulus*

$N = 13783853195340239094605568 58$
95128490833

as the same as in Example 4.1, but with different value e' as follows;

$e' = 78079823056802569754144973 50$
6355376043

Computing the continued fraction expansion of $\frac{e'}{N}$ will give the following list;

$$\left[0,1,\frac{1}{2},\frac{4}{7},\frac{13}{23},\cdots,\frac{47970613}{84685116},\frac{969859519}{1712145431},\cdots\right]$$

We find that the secret the integer k and d are amongst the list the convergents of $\frac{e'}{N}$. In fact, in this example we obtained $\frac{k}{d} = \frac{969859519}{1712145431}$. From here, one can verified that $e'd' \equiv 1(\text{mod}N')$ holds.

Let us compare the integers d and k with the upper bound of d provided by applying the Wiener's Theorem and Nitaj's Theorem attacks to the same problem. As shown in the Example 4.1, we obtained the secret parameter $d = 1692145429$, which is much larger than Wiener's upper bound (i.e. $d < 1142145426$) and Nitaj's bound (i.e. $d < 1663506620$), respectively.

Referring to the Example 4.2, the attack presented in this example use a much larger value of d yet our attack still finds such secret integer d. Note that, our attack works with the maximal value d less than 1713218139 for the respective N in both examples. Again, the secret integer d from Example 2 is much larger than Wiener's upper bound (i.e. $d < 1142145426$) and Nitaj's bound (i.e. $d < 1663506620$), respectively. Hence, this is in a good agreement with our theoretical result, which is mathematically proven in Theorem 3.2 and as reported in Table 1.

CONCLUSION

Note that Wiener's attack works efficiently on RSA with the condition that the secret exponent $d < \frac{1}{3}N^{\frac{1}{4}}$, which was using a Diophantine's method called continued fractions. Later, the upper bound was improved in Nitaj, A., 2013 satisfying $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. In this work, we present another proof of using continued fraction method that shows a way to obtain the secret exponent d efficiently, satisfying $d < \frac{1}{2}N^{\frac{1}{4}}$. We conclude that our result is slightly better than the previously mentioned attacks, in term of both theoretically and practically, via numerical examples.

ACKNOWLEDGMENT

The present research was partially supported by the Putra Grant - Putra Young Initiative (IPM) -GP-IPM-2017-9519200.

REFERENCES

Asbullah, M. A. and Ariffin, M. R. K. (2014). Comparative Analysis of Three Asymmetric Encryption Schemes Based Upon the Intractability of Square Roots Modulo $N = p^2q$. *4th International Cryptology and Information Security Conference 2014 (CRYPTOLOGY2014)* 24-26 June 2014, Putrajaya, 86-99.

Asbullah, M. A. and Ariffin, M. R. K. (2015). New Attack on RSA with Modulus $N = p^2q$ Using Continued Fractions, *Journal of Physics* **622** 191-199.

Asbullah, M. A. and Ariffin, M. R. K. (2016a) Analysis on the AA_β Cryptosystem. *5th International Cryptology and Information Security Conference 2016 (Cryptology2016),* 31 May-2 June 2016, Sabah, Malaysia, 41-48.

Asbullah, M. A. and Ariffin, M. R. K. (2016b). Analysis on the Rabin-p cryptosystem. *4th International Conference on Fundamental and Applied Sciences (ICFAS2016). AIP Conf. Proc.* **1787** 080012-1 - 080012-8

Asbullah, M. A. and Ariffin, M. R. K. (2016c). Design of Rabin-like cryptosystem without decryption failure. *Malaysian Journal of Mathematical Sciences* **10 (S)** 1 - 18.

de Weger, B. (2002). Cryptanalysis of RSA with Small Prime Difference *Applicable Algebra in Enginering, Commnication and Computing AAECC* **13** 17-28.

Maitra, S. and Sarkar, S. (2008). Revisiting Wiener's Attack- New Weak Keys in RSA. *11th International Conference on Information Security ISC* Taipei.

Nitaj, A. (2013). Diophantine and lattice cryptanalysis of the RSA cryptosystem *In Artificial Intelligence, Evolutionary Computing and Metaheuristics* Springer Berlin Heidelberg 139-168.

Rivest, R., Shamir, A. and Adleman, L. (1978). A Method for Obtaining digital signatures and public-key cryptosystems *Communications of the ACM* **21 (2)** 120-126.

Wiener M. (1990). Cryptanalysis of Short RSA Secret Exponents *IEEE Trans. Inform. Theory* 36 **3** 553-558.