MALAYSIAN JOURNAL OF SCIENCE

Vol. 41 • Special Issue (1) • 2022

3rd Virtual Symposium on Multidisciplinary Science 2021 (V-SMS2021)

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

https://myjurnal.mohe.gov.my/public/browse-journal-view.php?id=194
www.mjs.um.edu.my

Selected papers from the

Virtual Symposium on Multidisciplinary Science 2021 (V-SMS2021)

Universiti Putra Malaysia, Malaysia. July 7, 2021.

Symposium on Multidisciplinary Science (SMS) is an annual symposium organized by Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia. The first symposium was held in 2019 (SMS2019), followed by a virtual symposium in 2020 (V-SMS2020) due to pandemic break. This is the third symposium which was held virtually considering the current COVID-19 situation locally and globally. V-SMS2021 was co-organize with Iraqi Association for Academic Quality and Collaboration (IAAQC). IAAQC was founded in 2019 in Iraq, under the licence of Ministry of Higher Education and Scientific Research. IAAQC cooperates with local and international academic institutions, for organizing or sponsoring international conferences inside and outside of Iraq. IAAQC also aims to develop the culture of participation among members of IAAQC in local and international conferences and to improve the quality of writing scientific research among members of IAAQC.

V-SMS2021 was held on July 7, 2021. A fruitful symposium was held where there was a fertile exchange of information on the latest findings in every changing field of multidisciplinary sciences. The symposium theme of “Converging Interdisciplinary Science: Fundamentals to Modern Applications” is aptly chosen due to the recent trend demands where scientific explorations among multidisciplinary researchers are greatly fostered by an effective synchronizing interaction and networking both local and global levels.

This symposium was attended by both national and international experts in the field of mathematics, physics, chemistry and biology to present their current research. A total of 81 papers were presented orally by delegates from every corner of the country with more than 100 participants attended the conference. We gratefully acknowledge the support and continuous encouragement from the Vice-Chancellor and Deputy Vice-Chancellor of Universiti Putra Malaysia, and Director of Centre of Foundation Studies for Agricultural Science, University Putra Malaysia. A high appreciation is given to our colleagues and all committee members that worked hard to ensure the success of this conference.

We extend our special thanks to Prof. Dr. Wan Haliza Abd Majid and the team of the Malaysian Journal of Science for accepting our request to publish selected papers presented at this symposium and ensure that the process of publishing this special issue runs smoothly.

Ts. Dr. Ikhwan Syafiq Mohd Noor
Centre of Foundation Studies for Agricultural Science
Universiti Putra Malaysia, Malaysia

Dr. Mohammad Hasan Abdul Sathar
Centre of Foundation Studies for Agricultural Science
Universiti Putra Malaysia, Malaysia

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021
Special Issue
Malaysian Journal of Science 41 (Special Issue 1): 1-8 (September 2022)
https://mjs.um.edu.my

AN UPDATED CRYPTANALYSIS ON THE BFHP-DLP SIGNING SCHEME

Amir Hamzah Abd Ghafar[1a,b*], Muhammad Rezal Kamel Ariffin[2a,b], Muhammad Asyraf Asbullah[3b,c], Idham Arif Alias[4a]

Abstract: The concept of public-key cryptography introduced the notion of a digital signature scheme. In the era of online and digital communications, a signature scheme that works perfectly to achieve the goals of cryptography- confidentiality, authentication, data integrity, and non-repudiation, is urgently needed. However, every cryptosystem, including a digital signature scheme requires a well-defined difficult mathematical problem as its fundamental security strength, as demonstrated by the Diffie-Hellman key exchange with its discrete logarithm problem (DLP). Another problem called BFHP used by the AA_β-encryption scheme, has also withstood any destructive cryptanalysis since the scheme was introduced in 2013. Later, a digital signature scheme was introduced that combines both BFHP and DLP as difficult mathematical problems. Mathematical cryptanalysis was also performed against this scheme to test its security strength. This paper presents new cryptanalysis of the signing scheme. While the previous cryptanalysis focused only on BFHP, the obtained new results showed some improvement by scrutinizing the other difficult mathematical problem, DLP. In addition, several potential attacks on the future implementation by introducing side-channel and man-in-the-middle attacks against the scheme also will be discussed in this work. The countermeasures for each attack to enable the best-practice implementation of the scheme are also presented.

Keywords: *digital signing scheme, discrete logarithm problem, number field sieve, fault analysis attack, man-in-the-middle attack*

1. Introduction

Most digital applications of today's use required a digital signature scheme embedded in their core functions. The scheme serves the cryptographic goals of verifying the authenticity, integrity, and non-repudiation of a digital document transmitted over an insecure Internet channel. Traditional signing schemes were already introduced by ElGamal (1985), Rivest et al. (1978), and Schnorr (1991). Today, various protocols of signing schemes have been derived from these schemes and refined for niche purposes, including threshold signature (Gennaro et al., 2018; Ergezer et al., 2020), group signature (Islamidina et al., 2019; Nick et al., 2020), and blind signature (Alam et al., 2016; Fuchsbauer et al., 2020;) schemes. Some of the variants have become the backbone of the latest digital technologies, including blockchain systems (Stathakopoulou & Cachin, 2017; Guo & Lan, 2020). In addition, a standard digital signature scheme that can be used by public users has been introduced, namely, Public-Key Cryptography Standard (PKCS) #1 and Elliptic Curve Digital Signature Algorithm (ECDSA), which have been documented by the Internet Engineering Task Force (IETF) (Moriarty et al., 2016; Pornin, 2013).

All of the mentioned schemes use either the Integer Factorization Problem (IFP) or the Discrete Logarithm Problem (DLP), which are considered by many to be one-way functions in the mathematical domain (Hoffstein et al., 2008). These functions ensure the previously mentioned cryptographic goals are achieved by satisfying the properties of a mathematical one-way function. The functions are also resistant to all feasible algorithms that can work with current computing power. The best algorithm for solving IFP is the quadratic sieve algorithm described by Pomerance (1984), while several algorithms, namely the index computation, Pollard's rho, and number field sieve algorithms explained by Paar and Pelzl (2009), are among the best-known algorithms for solving it. However, all of these algorithms run in subexponential time at best, which prevents any active attack in real cryptographic implementations.

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, UPM Serdang, MALAYSIA.
E-mail: amir_hamzah@upm.edu.my[1], rezal@upm.edu.my[2], idham_aa@upm.edu.my[4]
[b]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, UPM Serdang, MALAYSIA. E-mail: ma_asyraf@upm.edu.my[3]
[c]Centre of Foundation Studies for Agricultural Science. Universiti Putra Malaysia, UPM Serdang, MALAYSIA.

*Corresponding Author: amir_hamzah@upm.edu.my

Received: January 21, 2022
Accepted: April 13, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

The approach of combining two difficult problems to increase the security of a cryptosystem is not new. Smith and Lennon (1993) introduced the LUC cryptosystem based on DLP and IFP. However, the attacks conducted against this cryptosystem (Jin et al., 2013; Wong et al., 2015; Sarbini et al., 2018;) have shown that it should be carefully examined before using any implementation. In this paper, the scheme is discussed by combining the DLP with another difficult mathematical problem called the Bivariate Function Hard Problem (BFHP). The problem was introduced by Ariffin et al. (2013) and has been used previously to develop a new encryption scheme called the $\boldsymbol{AA_{\beta}}$-algorithm. The scheme relies solely on BFHP as its security strength and is suitable to be applied on an embedded system device due to its high encryption speed compared to conventional encryption schemes (Adnan et al., 2016). Its decryption algorithm has also withstood several side-channel attacks, which can be remedied by minimal additional operation (Abd Ghafar & Ariffin, 2014; Abd Ghafar & Ariffin, 2016).

1.1. Contribution of This Paper

This paper presents a new signing scheme that combines BFHP and DLP as a key security strength. The scheme, named BFHP-DLP signing scheme, was introduced by Abd Ghafar & Ariffin (2019) and is comparable in its computational operations to existing signing schemes such as RSA, ElGamal, and Schnorr. In contrast to the original paper, the scheme is presented based on its modules. This form of presentation is better suited to control access to the modules given to the intended entity. Another important contribution of this work is that three new improved attacks on the BFHP-DLP signing method being performed. The improved cryptanalysis is based on the recent results on solving DLP and techniques of side-channel attack and man-in-the-middle attack, which can be used to retrieve the values of the private keys of the scheme.

The first attack refers to the recent attempt by Boudot et al. (2020), who successfully solved DLP using the Number Field Sieve algorithm with a 795-bits prime. Hence, the obtained result proved how this recent result can affect the size criteria used in the key generation algorithm of the BFHP-DLP scheme. The second attack assumes that an adversary can perform a side-channel attack on the device that carries out the signing scheme. In the third attack, the authors showed that the adversary can successfully break the scheme using a man-in-the-middle attack method.

1.2. Outline of the Paper

The outline of methods used in this paper is as follows; number field sieve algorithm, side-channel attack, and man-in-the-middle attack are discussed in Section 2. Then, Section 3 describes the reintroduce BFHP-DLP signing scheme. The three attacks, which are the primary basis of this paper, will be presented in Section 4. Finally, the conclusion will be discussed in Section 5.

2. Preliminaries

This section describes the methods used in improved cryptanalysis. Although all methods are little known in the literature, they are widely used in attacks on public-key cryptosystems.

2.1 Number Field Sieve (NFS)

Before describing the number field sieve method, the problem of the discrete logarithm that the method attempts to solve is first defined. The problem is also used in the BFHP-DLP signing scheme.

Definition 1 (Discrete logarithm problem). Let $\boldsymbol{p}$ be a prime. Suppose $\mathbb{F}_{\boldsymbol{p}}$ is a prime-order finite field. Given $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{F}_{\boldsymbol{p}}^{*}$, discrete logarithm problem is a problem to find $\boldsymbol{x}$ such that $\boldsymbol{g}^{\boldsymbol{x}} \equiv \boldsymbol{h} \pmod{\boldsymbol{p}}$.

The goal of the NFS in the finite field of DLP is to compute a non-trivial homomorphism from $\boldsymbol{G}$ to ${}^{\mathbb{Z}}\!/_{\boldsymbol{\ell}\mathbb{Z}}$ such that $\boldsymbol{G}$ is a subgroup of prime order $\boldsymbol{\ell}$ within $\mathbb{F}_{\boldsymbol{p}}^{*}$. The strategy to achieve this goal is to find two irreducible polynomials $\boldsymbol{f_0}$ of degree $\boldsymbol{u}$ and $\boldsymbol{f_1}$ of degree $\boldsymbol{v}$ in $\mathbb{Z}_{\boldsymbol{x}}$. These polynomials should have a common root $\boldsymbol{\mu}$ modulo $\boldsymbol{p}$. Let $\mathbb{Q}(\boldsymbol{i})$ be the number field defined by $\boldsymbol{f}$ where $\boldsymbol{i} \in \mathbb{C}$ is a root of $\boldsymbol{f_1}$ such that $\boldsymbol{f_1}$ is an irreducible polynomial, then the most challenging task in NFS is to find a pair of integers $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ such that

$$\boldsymbol{\gamma} = \boldsymbol{\alpha} - \boldsymbol{\beta\mu} \text{ and } \boldsymbol{\delta} = \boldsymbol{\alpha} - \boldsymbol{\beta i}$$

are both decomposable into small factors, i.e. smooth numbers. Many papers in the literature are devoted to finding the relation between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, since this step takes up most of the computations (computational power and computational storage. In this case, the result from this method is applied to fit into our key generation algorithm; as described in detail by Boudot et al. (2019)

2.2 Side-channel attack

This attack focuses on the implementation of cryptosystems in electronic devices. It relies on observable outputs such as computing time, power consumption, acoustic form and many more during cryptographic processes. The adversary can collect these outputs because the computation takes place in a 'black box' system, i.e. the adversary can only examine the functionality of the devices but has no access to the private functioning. The attack introduced by Kocher (1996) typically examines the private computations of the signing scheme. In this paper, the signing algorithm of the BFHP-DLP scheme is specifically become the main focus.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

2.2.1 Fault Analysis

By the definition of a side-channel attack, an attacker cannot determine the internal states of the attacked cryptographic devices. However, by introducing unexpected environmental conditions that can lead to data corruption into a specific part of the processor executed by the devices, the attacker can cause errors in the targeted cryptographic computations. By neglecting the error, the attacker can then isolate the instructions executed by the devices and eventually determine the internal workings of computations.

In a seminal work by Bao et al. (1997), $\boldsymbol{p}$ is the public key of the ElGamal signature scheme and *M* is the message to be signed. This showed that an attacker can obtain the actual signature by flipping one bit of the private signing key, $\boldsymbol{d}$ at the $\boldsymbol{i}$-th bit position, thus forming an erroneous $\boldsymbol{d}'$, then

$$\boldsymbol{S} \equiv \boldsymbol{M}^{\boldsymbol{d}} (\text{mod } \boldsymbol{p})$$

and the faulty signature,

$$\boldsymbol{S}' \equiv \boldsymbol{M}^{\boldsymbol{d}'} (\text{mod } \boldsymbol{p}).$$

Both signatures then can be used to determine the bit of $\boldsymbol{d}$ at ***the*** $\boldsymbol{i}$-th position by computing the function

$$\frac{\boldsymbol{S}'}{\boldsymbol{S}} \equiv \boldsymbol{M}^{\boldsymbol{d}'-\boldsymbol{d}} \equiv \begin{cases} \boldsymbol{M}^{2\boldsymbol{i}} \ (\text{mod } \boldsymbol{p}) \text{ if the } \boldsymbol{i} - \text{th bit of } \boldsymbol{d} = \boldsymbol{0} \\ \dfrac{\boldsymbol{1}}{\boldsymbol{M}^{2\boldsymbol{i}}} (\text{mod } \boldsymbol{p}) \text{ if the } \boldsymbol{i} - \text{th bit of } \boldsymbol{d} = \boldsymbol{1} \end{cases}.$$

To extend the attack and determine the entire bits of the private key, each bit with $\boldsymbol{i} = \boldsymbol{1}, \boldsymbol{2}, \boldsymbol{3}, \dots, \boldsymbol{n}$ should be examined and a subexponential algorithm is needed. The attack shows the significance of thorough cryptanalysis to ensure that the signature cannot be compromised to obtain information about the private keys.

2.3 Man-in-the-middle attack

If the communication between two units is secretly intercepted by an adversary, the immediate consequence depends on whether the adversary is actively involved in the communication. For example, if the adversary surreptitiously forwards and modifies the communication, there is a man-in-the-middle attack on the communication.

A suitable authentication mechanism is required to prevent this attack. The standard mechanism currently used is the exchange of digital certificates issued and verified by a trusted Certificate Authority (CA). However, this CA can also be a target of a man-in-the-middle attack. Therefore, CA must be subjected to proper evaluation and security verification at regular intervals.

In this paper, a man-in-the-middle attack is constructed against the BFHP-DLP signature procedure. The existence of such an attack shows that it is necessary to first develop a suitable cryptographic protocol before this system can be used in an application.

3. BFHP-DLP Signing Scheme

In this study, our scheme is rewritten and compared to the original paper by (Abd Ghafar & Ariffin, 2019) in our to separate our schemes into their purported modules. This form is more suitable for cryptanalysis of our scheme, especially when the modules may have different access controls even though they are included in the same algorithm. It also reflects the actual use of a cryptographic scheme in a real scenario.

The initialisation and key generation algorithms of the scheme, as shown in Figure 1.

```
$\mathcal{I}$: Initialization algorithm → $(\boldsymbol{p}, \boldsymbol{g})$
Select $\boldsymbol{p}$ randomly from $\mathbb{Z}_{2^{\boldsymbol{m}}}$
        where $\boldsymbol{m}$ is a large integer
Select $\boldsymbol{g}$ from $\mathbb{Z}_{\boldsymbol{p}}^*$ where $\boldsymbol{g}$ is a primitive root of group $\mathbb{Z}_{\boldsymbol{p}}^*$
```

```
$\mathcal{K}$: Key Generation algorithm → $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{A}, \boldsymbol{B})$
Private key
        Given $\boldsymbol{n} > \boldsymbol{m}$.
        select $\boldsymbol{a}$ randomly from $\mathbb{Z}_{2^{\boldsymbol{n}}}$
        select $\boldsymbol{b}$ randomly from $\mathbb{Z}_{2^{\boldsymbol{n}}}$
Public key
        compute $\boldsymbol{A} \equiv \boldsymbol{g}^{\boldsymbol{a}} (\text{mod } \boldsymbol{p})$
        compute $\boldsymbol{B} \equiv \boldsymbol{g}^{\boldsymbol{b}} (\text{mod } \boldsymbol{p})$
```

Figure 1. Initialization and key generation algorithms of BFHP-DLP signing scheme

As in Figure 1, the algorithms are typically computed by isolated devices controlled by a Trusted Third Party (TTP). An example of such a TTP practice is CA (as referred to in Section 2.3), which is validated by government agencies. This approach ensures that only the authorised body can monitor the process. After the keys are generated, the private keys are securely stored in a tampered-resistant device, such as chips on a smartcard or a secure token carried by the authenticated owners.

Next, the algorithms for signing and verification of the scheme are shown in Figure 2.

In the signature algorithm, a hash function $\boldsymbol{H}$ creates a digital fingerprint of $\boldsymbol{M}||\boldsymbol{r}$, which is the concatenation of the original message, $\boldsymbol{M}$ with the private parameter, $\boldsymbol{r}$. The standard hash function used today is SHA-256 and its variants.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

```
$\boldsymbol{\mathcal{S}}$: Signature algorithm of $\boldsymbol{M \to (M, \sigma, e)}$
Public ephemeral key
        select $\boldsymbol{x}$ randomly from $\mathbb{Z}_{2^m}$
        select $\boldsymbol{y}$ randomly from $\mathbb{Z}_{2^m}$
Private session key
        compute $\boldsymbol{c = ax + by}$
        select $\boldsymbol{k}$ randomly from $\mathbb{Z}_{2^n}$ such that
        $\boldsymbol{c - k > 2^m}$ and $\boldsymbol{n > m}$.
Private computation of signing $\boldsymbol{M}$
        compute $\boldsymbol{s = c - k}$
        compute $\boldsymbol{r \equiv g^k (\text{mod } p)}$
        $\boldsymbol{e = H(M \| r)}$ where $\boldsymbol{H}$ is a hash function
Output public signature $\boldsymbol{\sigma = (x, y, s, e)}$
```

```
$\boldsymbol{\mathcal{V}}$: Verification algorithm of $\boldsymbol{(M, \sigma)}$
Verification key
        compute $\boldsymbol{r' \equiv A^x \cdot B^y \cdot g^{-s} (\text{mod } p)}$
Check whether
        $\boldsymbol{H(M \| r') = e}$ → Yes/No
```

Figure 2. Signing and verification algorithms of BFHP-DLP signing scheme

Proof of Correctness. It is easy to see that

$$\boldsymbol{A^x B^y \equiv g^{ax} g^{by} \equiv g^{ax+by} \equiv g^c (\text{mod } p)}. \qquad (\mathbf{14})$$

If the correct $\boldsymbol{c}$ is obtained, $\boldsymbol{r'}$ will produce $\boldsymbol{H(M \| r') = e}$.

4. The Updated Cryptanalysis

This section presents the updated cryptanalysis of BFHP-DLP discovered based on the new techniques described in Section 2. The cryptanalysis can be categorized into three different attacks. The first attack focuses solely on solving DLP, while the second and third attacks are based on the assumption of the complexity of the scheme's key generation algorithm is reduced.

4.1 First Attack: Number Field Sieve

Boudot et al. (2019) showed that a DLP over a 795-bit prime field can be computed in 18-days using the latest computational technologies, well-chosen parameters and suitable algorithmic variants. In this attack, the assumption is made that their result affects our signing scheme, especially the parameters selection criterion in algorithms $\boldsymbol{\mathcal{I}}, \boldsymbol{\mathcal{K}}$ and $\boldsymbol{\mathcal{S}}$.

In the BFHP-DLP signing scheme, there are three instances of DLP, namely $\boldsymbol{A \equiv g^a (\text{mod } p)}$ and $\boldsymbol{B \equiv g^b (\text{mod } p)}$ of algorithm $\boldsymbol{\mathcal{K}}$ and $\boldsymbol{r \equiv g^k (\text{mod } p)}$ of algorithm $\boldsymbol{\mathcal{S}}$. Although $\boldsymbol{a, b > k}$, since $\boldsymbol{a, b \in \mathbb{Z}_{2^n}}$ and $\boldsymbol{k \in \mathbb{Z}_{2^m}}$, where $\boldsymbol{n > m}$, but all computations of DLP take place in an $\boldsymbol{m}$-bit prime field $\boldsymbol{p}$, so that $\boldsymbol{p \in \mathbb{Z}_{2^m}}$. From this observation with the results of Boudot et al. (2019), it can be noticed that those private keys $\boldsymbol{a, b}$ can be retrieved when $\boldsymbol{m \leq 795}$. So, a larger $\boldsymbol{m}$ is required to ensure that the scheme can exploit the security strength of DLP.

Since the original work by (Abd Ghafar & Ariffin, 2019) did not mention the appropriate size of $\boldsymbol{m}$ and $\boldsymbol{n}$, so it can be proposed that $\boldsymbol{m}$ is at least $\mathbf{2048}$ and $\boldsymbol{n = 2m = 4096}$. This recommendation follows the NIST standard for cryptographic keys using DLP (Barker & Dang, 2015).

4.2 Second Attack: Fault Analysis

Every implementation of a cryptosystem attempts to reduce the complexity of the cryptographic algorithms. Reduced complexity leads to reduce computational time, power consumption, or memory capacity, making it attractive to be implemented in a smaller device. Based on this motivation, it assumed that the possibility to fix the value of the parameter $\boldsymbol{k}$ is an attractive solution. The fixed values result in a fixed $\boldsymbol{r}$, since $\boldsymbol{r \equiv g^k (\text{mod } p)}$. Furthermore, random selection can be omitted so less power and memory can be fixed for $\boldsymbol{r}$. However, it can be seen that this approach can be advantageous for the adversary to determine the bits of $\boldsymbol{k}$ using the method described in Section 2.2.1.

Definition 2 (Fault analysis adversary, $\boldsymbol{\mathcal{A}_1}$). $\boldsymbol{\mathcal{A}_1}$ is defined as an adversary that is able to inject a faulty environment into the Algorithm $\boldsymbol{\mathcal{S}}$ that can invert a bit of $\boldsymbol{k}$ at $\boldsymbol{i}$th position (from the right), $\boldsymbol{k_i}$ to its complement bit, $\boldsymbol{k'_i}$.

Example 1. Let $\boldsymbol{k = 3787}$ with bits 111011001011. Given $\boldsymbol{i = 8}$, then $\boldsymbol{A_1}$can flip $\boldsymbol{k_5 = 1}$ to $\boldsymbol{k'_5 = 0}$, which produces $\boldsymbol{k' = 3659}$ with bits 111001001011.Noted that $\boldsymbol{|k - k'| = |3787 - 3659| = 128 = 2^7}$.

The attack is stated in the following theorem.

Proposition 1. Let $\boldsymbol{k}$ be the private session key generated in algorithm $\boldsymbol{\mathcal{S}}$. Let $\boldsymbol{\mathcal{A}_1}$ be defined in Definition 2. If $\boldsymbol{k}$ is used more than $\boldsymbol{n - 1}$ times, then the entire bits of $\boldsymbol{k}$ can be known.

Proof. Assume that $\boldsymbol{\mathcal{A}_1}$ can change $\boldsymbol{k_i}$ in $\boldsymbol{k}$ is to its complement $\boldsymbol{k'_i}$ which produces $\boldsymbol{k'}$ during the signing process in Algorithm $\boldsymbol{\mathcal{S}}$ as defined in Definition 2. Since the value of $\boldsymbol{k}$ differs from $\boldsymbol{k'}$ at $\boldsymbol{i}$-th bit position, then $\boldsymbol{|k - k'| = 2^{i-1}}$ or

$$\boldsymbol{k = \begin{cases} k' - 2^{i-1} \text{ if the } i - \text{th bit of } k = 0 \\ k' + 2^{i-1} \text{ if the } i - \text{th bit of } k = 1 \end{cases}}$$

Observe that

$$\boldsymbol{s = \begin{cases} c - (k' - 2^{i-1}) \text{ if the } i - \text{th bit of } k = 0 \\ c - (k' + 2^{i-1}) \text{ if the } i - \text{th bit of } k = 1 \end{cases}}. \qquad (\mathbf{1})$$

Algorithm $\mathcal{S}$ computed that

$$\tilde{r} \equiv g^{k'} (\text{mod } p) \qquad (2)$$

and output

$$e' = H(M \| \tilde{r})$$

to be included in the signature σ. Let

$$\begin{aligned} \tilde{s}_1 &= s - 2^{i-1} \\ \tilde{s}_2 &= s - 2^{i-1} \end{aligned} \qquad (3)$$

then $\mathcal{A}_1$ can obtain the potential candidates for $\tilde{r}$ based on (1), (2), and (3) by computing

$$\begin{aligned} A^x \cdot B^y \cdot g^{-\tilde{s}_1} &\equiv g^{ax+by-(s-2^{i-1})} \\ &\equiv g^{ax+by-(c-(k'-2^{i-1})-2^{i-1})} \\ &\equiv g^{k'} \equiv \widetilde{r_1} (\text{mod } p) \end{aligned} \qquad (4)$$

or

$$\begin{aligned} A^x \cdot B^y \cdot g^{-\tilde{s}_2} &\equiv g^{ax+by-(s+2^{i-1})} \\ \equiv g^{ax+by-(c-(k'+2^{i-1})+2^{i-1})} &\equiv g^{k'} \equiv \widetilde{r_2} (\text{mod } p) \end{aligned} \qquad (5)$$

if the $i -$ th bit of $k = 1$. Noted that both (4) and (5) should be executed by $\mathcal{A}_1$ since, at this point, $\mathcal{A}_1$ still does not know if the $i -$ th bit of k is 0 or 1. By using the outputs from (4) and (5), now $\mathcal{A}_1$ can determine the original bits of k_i by checking whether

$$e' = \begin{cases} H(M \| \widetilde{r_1}) & \text{if the } i - \text{th bit of } k = 0 \\ H(M \| \widetilde{r_2}) & \text{if the } i - \text{th bit of } k = 1 \end{cases}$$

It can be shown how $\mathcal{A}_1$ can determine one bit of k at position i. If $\mathcal{A}_1$ repeats the same process for $n - 1$ times, then $\mathcal{A}_1$ has the total bits of k since $k \in \mathbb{Z}_{2^n}$ or has n-bit size. This terminates the proof.

■

Theorem 1. Let (a, b) be the private keys generated from algorithm $\mathcal{K}$. Suppose (x, y) and k are randomized values from algorithm $\mathcal{S}$ and $s = c - k$ is one of the signature parameters from σ defined in algorithm $\mathcal{S}$. If full bits of k are retrieved from Proposition 1, then (a, b) can be known.

Proof. By knowing the entire bits of k, an adversary can compute $c = s + k$ since s is a public parameter obtained from σ. By knowing c, the adversary can retrieve (a, b) values using the Extended Euclidean algorithm since $ax + by = c$ and values of (x, y) are known from σ. This terminates the proof.

■

4.2.1 Countermeasures of the Second Attack

The attacks presented in Proposition 1 and Theorem 1 proved that it is possible for an adversary satisfying Definition 2 to retrieve the private keys of the BFHP-DLP signing scheme. Therefore, the apparent approach to avoid the attack is to never set k to a static value. Although this approach may be counterproductive to the implementation, exposing arbitrary bits of k can lead to a specified attack called a partial key exposure attack.

4.3 Third Attack: Man-in-the-Middle

Definition 3 (Active adversary, $\mathcal{A}_2$). Let $\sigma = (x, y, s, e)$ be defined as in Figures 1 and 2. An active adversary $\mathcal{A}_2$ is defined as a man-in-the-middle adversary who intercepts σ and then modifies it before sending it back to the intended recipient of σ.

The attack is described in the following theorem.

Theorem 2. Assume that (a, b) are the private keys generated from algorithm $\mathcal{K}$. Assume that (x, y) are random values from algorithm $\mathcal{S}$ and that signature $\sigma = (x, y, s, e)$ was computed using the same algorithm. If there is an active adversary $\mathcal{A}_2$ according to Definition 3, then $\mathcal{A}_2$ can forge a signature $\sigma' = (x, y, s', e')$, which is verified in algorithm $\mathcal{V}$.

Proof. Suppose that $\sigma = (x, y, s, e)$ was generated by Alice using algorithm $\mathcal{S}$. Assuming $\mathcal{A}_2$ is an adversary defined in Definition 3, then $\mathcal{A}_2$ can prevent σ from reaching the intended receiver, Bob. $\mathcal{A}_2$ can then compute

$$A^x \cdot B^y \cdot g^{-s} \equiv r' (\text{mod } p)$$

using algorithm $\mathcal{V}$ as in Figure 2 then modifies r' by computing

$$r' \cdot g^{\delta} \equiv g^k \cdot g^{\delta} \equiv g^{k+\delta} \equiv r'' (\text{mod } p)$$

for some $\delta \in \mathbb{Z}$. $\mathcal{A}_2$ also modifies s by computing

$$s - \delta = c - k - \delta = s'.$$

By using r' and a forged message, M', $\mathcal{A}_2$ then computes forged e' by computing

$$e' = H(M' \| r'')$$

using a hash function, H. $\mathcal{A}_2$ then sends $\sigma' = (x, y, s', e')$ and M' to Bob, acting like they are from Alice, the original sender. Then, Bob compute

$$\begin{aligned} A^x \cdot B^y \cdot g^{-s'} \equiv g^{ax} \cdot g^{by} \cdot g^{-s'} \equiv g^{ax+by-(c-k-\delta)} \equiv g^{k+\delta} \\ \equiv r'' (\text{mod } p) \end{aligned}$$

using algorithm $\mathcal{V}$ and verifies r'' by computing $H(M' \| r'')$ equal to e' sent along with the forged σ. It is shown that $\mathcal{A}_2$ has forged Alice's signature, σ, by converting it to σ' and then

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

sending it to Bob. Bob has also verified $\boldsymbol{\sigma}'$, without knowing $\boldsymbol{\sigma}'$ is a forgery signature. This terminates the proof.

■

4.3.1 Countermeasures of the Third Attack

The third attack is considered the most devastating attack on the BFHP-DLP signing scheme because it occurs during the most important process of the scheme, which is sending the signature to the intended recipient. The attack occurs because $\mathcal{A}_2$ can obtain $\boldsymbol{r}$ by computing $A^x \cdot B^y \cdot g^{-s} (\text{mod } \boldsymbol{p})$ and then modifying it. By depriving $\mathcal{A}_2$ of access to the values of $\boldsymbol{x}$ and $\boldsymbol{y}$, it can be noticed that the modification can be prevented. Therefore, the modified signature scheme is proposed, which uses an encryption function $\boldsymbol{Enc}_{K_1}$ with the encryption key, $\boldsymbol{K_1}$, and a decryption function $\boldsymbol{Dec}_{K_2}$ with the decryption key, $\boldsymbol{K_2}$. The modified signature algorithms with their corresponding verification algorithms are shown in Figure 3.

```
$\mathcal{S}'$: Modified signature algorithm of $M \rightarrow (M, \sigma, e)$
Public ephemeral key
        select $x$ randomly from $\mathbb{Z}_{2^m}$
        select $y$ randomly from $\mathbb{Z}_{2^m}$
Private session key
        compute $c = ax + by$
        select $k$ randomly from $\mathbb{Z}_{2^n}$ such that
        $c - k > 2^m$ and $n > m$.
Encrypt verification key using Bob's public key, $i$
        compute $X = Enc_{K_1}(x)$ and $Y = Enc_i(y)$
Private computation of signing $M$
        compute $s = c - k$
        compute $r \equiv g^k (\text{mod } p)$
        $e = H(M \| r)$ where $H$ is a hash function
Output public signature $\sigma = (X, Y, s, e)$
```

```
$\mathcal{V}'$: Modified verification algorithm of $(M, \sigma)$
Decrypt verification key using Bob's private key, $j$
        compute $x = Dec_{K_2}(X)$ and y= $Dec_j(Y)$
Verification key
        compute $r' \equiv A^x \cdot B^y \cdot g^{-s} (\text{mod } p)$
Check whether
        $H(M \| r') = e \rightarrow$ Yes/No
```

Figure 3. Modified signing and verification algorithms of BFHP-DLP signing scheme

5. Conclusion

Three novel cryptanalyses against the BFHP-DLP signing scheme are presented in this study. The first attack applies the latest result that successfully solves DLP. This countermeasure sets the parameter size of $\boldsymbol{n}$ and $\boldsymbol{m}$ larger than the values attacked by the previous result. This countermeasure will not affect the efficiency of the scheme because the size of $\boldsymbol{n}$ and $\boldsymbol{m}$ is the appropriate cryptographic size specified in the NIST standard. Then, the second attack highlights the danger of specifying the values of $\boldsymbol{k}$ to be used multiple times, as this can expose the signing scheme to a side-channel method called fault analysis. To prevent this attack, the signing key algorithm must use an efficient pseudorandom number generator to ensure that $\boldsymbol{k}$ is generated randomly and not static. Finally, the last attack is considered the most devastating attack. It requires an active adversary to perform a man-in-the-middle method by modifying the transmitted signature $\boldsymbol{\sigma}$ to solve the private values of the scheme. The countermeasure to this attack introduces an encryption scheme that allows a seamless signing and verification process without intervention by the man-in-the-middle. Although the process can be redundant, it can be skipped once a shared private key is created, hence increasing its efficiency. These cryptanalyses not only focus on the hardness of BFHP, as in the existing cryptanalysis against the scheme but also cover the computational complexity of DLP and possible attacks against the real implementation of the scheme. The countermeasures presented will be of great use for the future deployment of the scheme.

6. Acknowledgment

The research was supported by the Ministry of Higher Education of Malaysia with the Fundamental Research Grant Scheme (FRGS/1/2020/STG06/UPM/02/2).

7. References

Abd Ghafar, A. H., & Ariffin, M. R. K (2014). Timing Attack Analysis on $\boldsymbol{AA_\beta}$ Cryptosystem. *Journal of Computer and Communications*, *2*(4), 1-9.

Abd Ghafar, A. H., & Ariffin, M. R. K. (2016). SPA on Rabin variant with public key $\boldsymbol{N = p^2q}$. *Journal of Cryptographic Engineering*, *6*(4), 339-346.

Abd Ghafar, A. H., & Ariffin, M. R. K. (2019). A New Signing Scheme Based on BFHP and DLP. *International Journal of Cryptology Research*, *9*(2), 31-44.

Adnan, S. F. S., Isa, M. A. M., & Hashim, H. (2016). Implementation of the Aa-Beta (AAβ) lightweight asymmetric encryption scheme on an embedded system device. *Advanced Science Letters*, *22*(10), 2910-2913.

Alam, K., Alam, K. R., Faruq, O., & Morimoto, Y. (2016, January). A comparison between RSA and ElGamal based untraceable blind signature schemes. In *2016*

International Conference on Networking Systems and Security (NSysS) (pp. 1-4). IEEE.

Ariffin, M. R. K., Asbullah, M. A., Abu, N. A., & Mahad, Z. (2013). A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $= \boldsymbol{p^2q}$. Malaysian Journal of Mathematical Sciences, 7, 19-37.

Bao, F., Deng, R. H., Han, Y., Jeng, A., Narasimhalu, A. D., & Ngair, T. (1997, April). Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. In *International Workshop on Security Protocols* (pp. 115-124). Springer, Berlin, Heidelberg.

Barker, E., & Dang, Q. (2015). NIST special publication 800–57 part 3: Application-specific key management guidance. *NIST Special Publication*, *800*, 57.

Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. (2020, August). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *Annual International Cryptology Conference* (pp. 62-91). Springer, Cham.

Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

Ergezer, S., Kinkelin, H., & Rezabek, F. (2020). A Survey on Threshold Signature Schemes. *Network*, *49*.

Fleischhacker, N., Jager, T., & Schröder, D. (2019). On tight security proofs for Schnorr signatures. *Journal of Cryptology*, *32*(2), 566-599.

Fuchsbauer, G., Plouviez, A., & Seurin, Y. (2020, May). Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 63-95). Springer, Cham.

Gennaro, R., & Goldfeder, S. (2018, October). Fast multiparty threshold ECDSA with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1179-1194).

Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on computing, 17(2), 281-308.

Guo, L., & Lan, C. (2020, December). A New Signature Based on Blockchain. In *2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS)* (pp. 349-353). IEEE.

Herrmann, M., & May, A. (2008, December). Solving linear equations modulo divisors: On factoring given any bits. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 406-424). Springer, Berlin, Heidelberg.

Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H. (2008). *An introduction to mathematical cryptography* (Vol. 1). New York: Springer.

Islamidina, A. D. P., Sudarsono, A., & Dutono, T. (2019, September). Security System for Data Location of Travelling User using RSA based on Group Signature. In *2019 International Electronics Symposium (IES)* (pp. 88-93). IEEE.

Jin, W. T., Kamarulhaili, H., Said, M. R. M., Ariffin, M. R. K., Asbullah, M. A., Abu, N. A., ... & Jahani, S. (2013). On the Hastad's Attack to LUC4, 6 Cryptosystem and compared with Other RSA-Type Cryptosystem. *Malaysian Journal of Mathematical Sciences*, *7*, 1-17.

Joux, A. (2013, August). A new index calculus algorithm with complexity $$ l (1/4+ o (1)) $$ in small characteristic. In International Conference on Selected Areas in Cryptography (pp. 355-379). Springer, Berlin, Heidelberg.

Karatsuba, A. (1963). Multiplication of multidigit numbers on automata. In Soviet physics doklady (Vol. 7, pp. 595-596).

Kim, S., Kim, J., Cheon, J. H., & Ju, S. H. (2011). Threshold signature schemes for ElGamal variants. *Computer Standards & Interfaces*, *33*(4), 432-437.

Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference* (pp. 104-113). Springer, Berlin, Heidelberg.

Kravitz, D. W. (1993). Digital signature algorithm. US Patent, 5(231), 668.

Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. (1993). The number field sieve. In *The development of the number field sieve* (pp. 11-42). Springer, Berlin, Heidelberg.

Montgomery, P. L. (1985). Modular multiplication without trial division. Mathematics of computation, 44(170), 519-521.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

Moriarty, K., Kaliski, B., Jonsson, J., & Rusch, A. (2016). PKCS# 1: RSA cryptography specifications version 2.2. Internet Engineering Task Force, Request for Comments, 8017.

Nick, J., Ruffing, T., & Seurin, Y. (2020). *MuSig2: Simple Two-Round Schnorr Multi-Signatures*. Cryptology ePrint Archive, Report 2020/1261, 2020. https://eprint. iacr. org/2020/1261.

Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

Pomerance, C. (1984, April). The quadratic sieve factoring algorithm. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 169-182). Springer, Berlin, Heidelberg.

Pornin, T. (2013). Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). *Internet Engineering Task Force RFC*, *6979*, 1-79.

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

Sarbini, I. N., Jin, W. T., Feng, K. L., Othman, M., Said, M. R. M., & Hung, Y. P. Garbage-man-in-the-middle (type 2) Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field. In *Cryptology and Information Security Conference 2018* (p. 35).

Schnorr, C. P. (1991). Efficient signature generation by smart cards. Journal of cryptology, 4(3), 161-174.

Seurin, Y. (2012, April). On the exact security of Schnorr-type signatures in the random oracle model. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 554-571). Springer, Berlin, Heidelberg.

Smith, P. J., & Lennon, M. J. (1993, May). LUC: A New Public Key System. In *SEC* (pp. 103-117).

Stathakopoulou, C., & Cachin, C. (2017). Threshold signatures for blockchain systems. *Swiss Federal Institute of Technology*.

Wong, T. J., Said, M. R. M., Othman, M., & Koo, L. F. (2015, May). On the common modulus attack into the LUC4, 6 cryptosystem. In *AIP Conference Proceedings* (Vol. 1660, No. 1, p. 090052). AIP Publishing LLC.

DOI: https://doi.org/10.22452/mjs.sp2022no1.1

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021 Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022) https://mjs.um.edu.my

ON SOME PATTERNS OF TNAF FOR SCALAR MULTIPLICATION OVER KOBLITZ CURVE

Faridah Yunos [1ac*], Rosimah Rosli[2b], and Norliana Muslim[3cd]

Abstract: A τ-adic non-adjacent form (TNAF) of an element α of the ring $\mathbb{Z}(\tau)$ is an expansion whereby the digits are generated by iteratively dividing α by τ, allowing the remainders of $-1, 0$ or 1. The application of TNAF as a multiplier of scalar multiplication (SM) on the Koblitz curve plays a key role in Elliptical Curve Cryptography (ECC). There are several patterns of TNAF (α) expansion in the form of $[c_0, 0, \dots, 0, c_{l-1}]$, $[c_0, 0, \dots, c_{\frac{l-1}{2}}, \dots, 0, c_{l-1}]$, $2+2k$, $3+4k$, $5+4k$ and $8k_1+8k_2$ that have been produced in prior work in the literature. However, the construction of their properties based upon pyramid number formulas such as Nichomacus's theorem and Faulhaber's formula remains to be rather complex. In this work, we derive such types of TNAF in a more concise manner by applying the power of Frobenius map (τ^m) based on *v*-simplex and arithmetic sequences.

Keywords: *Non adjacent form, Koblitz curve, scalar multiplication.*

1. Introduction

Koblitz curves are a special type of curve for which the Frobenius endomorphism can be applied to enhance its performance of computing SM (Koblitz, 1992) in ECC. It is defined over $\boldsymbol{F_{2^m}}$ as $\boldsymbol{E_a: y^2 + xy = x^3 + ax^2 + 1}$. The Frobenius map $\boldsymbol{\tau: E_a(F_{2^m}) \rightarrow E_a(F_{2^m})}$ is defined by $\boldsymbol{\tau(x, y) = (x^2, y^2)}$ **and** $\boldsymbol{\tau(\infty) = \infty}$, where ∞ represents a point at infinity. Therefore, it satisfies the roots of the polynomial $\boldsymbol{\tau^2 - t\tau + 2}$. Since $\boldsymbol{\tau} \ = \frac{t+\sqrt{-7}}{2}$ is a quadratic integer, the set $\mathbb{Z}(\boldsymbol{\tau}) = \{\boldsymbol{r + s\tau} \mid \ \boldsymbol{r, s} \in \mathbb{Z}\}$ forms a ring (Heuberger & Krenn, 2013b). Suppose *P* and *Q* are points on a Koblitz curve. SM is $\boldsymbol{n}$ multiple repetitions of a point on the curve, and is denoted as $\boldsymbol{nP = P + P + \cdots + P}$, such that $\boldsymbol{nP = Q}$.

Solinas (1997) introduced a multiplier of SM in the form of TNAF on a Koblitz curve to reduce SM costs. TNAF of nonzero $\boldsymbol{\alpha = r + s\tau}$ in $\mathbb{Z}(\boldsymbol{\tau})$ can be written as TNAF $(\boldsymbol{\alpha}) = \sum_{i=0}^{l-1} \boldsymbol{c_i \tau^i}$ where $\boldsymbol{c_i} \in \{\boldsymbol{-1, 0, 1}\}$ and $\boldsymbol{c_i c_{i+1} = 0}$. If $\boldsymbol{c_{l-1} \neq 0}$, then $\boldsymbol{l}$ is assumed to be the length of TNAF. This $\boldsymbol{\alpha}$ is divisible by $\boldsymbol{\tau}$ *iff r* is even. That is, $\frac{\boldsymbol{\alpha}}{\boldsymbol{\tau}} = \left(\boldsymbol{s} + \frac{\boldsymbol{tr}}{\boldsymbol{2}}\right) - \frac{\boldsymbol{r}}{\boldsymbol{2}}\boldsymbol{\tau}$, where $\boldsymbol{t} = (\boldsymbol{-1})^{\boldsymbol{1-a}}$ for $\boldsymbol{a} \in \{\boldsymbol{0, 1}\}$. If $\boldsymbol{\alpha}$ is not divisible by $\boldsymbol{\tau}$ (i.e., *r* is odd), then the remainder is chosen to be either $\boldsymbol{1}$ or $\boldsymbol{-1}$. The coefficients $\boldsymbol{c_i}$ of TNAF are generated successively by dividing $\boldsymbol{\alpha}$ with $\boldsymbol{\tau}$ until $\boldsymbol{r}$ and $\boldsymbol{s}$ are equal to 0. Since $\boldsymbol{c_i \, c_{i+1} = 0}$, the next coefficient ($\boldsymbol{c_{i+1}}$) of TNAF expansion after $\boldsymbol{c_i}$ must be 0. Furthermore, it has a unique digit representation and the average density of nonzero digits in the expansion is approximately $\frac{\boldsymbol{1}}{\boldsymbol{3}}$. The following examples describe the division process of TNAF ($\boldsymbol{1 - 2\tau}$).

Example 1.

Here we consider $\boldsymbol{n = 1 - 2\tau}$ and $\boldsymbol{\bar{\tau} = 1 - \tau}$ represent the conjugate of $\boldsymbol{\tau}$. Firstly, consider the elliptic curve $\boldsymbol{E_1}$ where $\boldsymbol{a = 1}$. Therefore, $\boldsymbol{\tau \cdot \bar{\tau} = -\tau^2 + \tau \ = (-\tau + 2) + \tau = 2}$ is shown. Next, the following steps are applied for finding TNAF ($\boldsymbol{n}$).

Step 1: Since $\boldsymbol{1 - 2\tau}$ is indivisible by $\boldsymbol{\tau}$, we choose $\boldsymbol{c_0 = 1}$. That is, $\frac{\boldsymbol{1-2\tau-1}}{\boldsymbol{\tau}} = \boldsymbol{-2}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, c_1, c_2, \dots, c_{l-2}, c_{l-1}}]$. The next coefficient ($\boldsymbol{c_1}$) must be 0.

Step 2: Since $\boldsymbol{-2}$ is divisible by $\boldsymbol{\tau}$, then $\mathbf{c_1 = 0}$. That is, $\frac{\boldsymbol{-2}}{\boldsymbol{\tau}} = \frac{\boldsymbol{-2}}{\boldsymbol{\tau}} \cdot \frac{\boldsymbol{\bar{\tau}}}{\boldsymbol{\bar{\tau}}} = \boldsymbol{-1 + 1\tau}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, c_2, \dots, c_{l-2}, c_{l-1}}]$.

Step 3: Since $\boldsymbol{-1 + \tau}$ is indivisible by $\boldsymbol{\tau}$, we choose $\boldsymbol{c_2 = 1}$. That is, $\frac{\boldsymbol{-1+1\tau-1}}{\boldsymbol{\tau}} = \boldsymbol{\tau}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, 1, c_3, c_4, \dots, c_{l-2}, c_{l-1}}]$.

Step 4: Since $\boldsymbol{\tau}$ is divisible by $\boldsymbol{\tau}$ (i.e., $\frac{\boldsymbol{\tau}}{\boldsymbol{\tau}} = \boldsymbol{1}$), then $\boldsymbol{c_3}$ is $\boldsymbol{0}$ and TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, 1, 0, c_4, \dots, c_{l-2}, c_{l-1}}]$.

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia. Email: faridahy@upm.edu.my[1]
[b]Department of Mathematics, Faculty of Science, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Johor, Malaysia. E-mail: cymaroslee@gmail.com[2]
[c]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, 43400 Universiti Putra Malaysia, Serdang, Selangor, Malaysia.
[d]Department of Engineering, Faculty of Engineering and Life Sciences, Universiti Selangor, Jalan Timur Tambahan 45600, Bestari Jaya, Selangor, Malaysia. E-mail: norliana_muslim@unisel.edu.my[3]

*Corresponding Author: faridahy@upm.edu.my

Received: January 21, 2022
Accepted: June 4, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.2

Step 5: Since $\mathbf{1}$ is indivisible by , we choose $c_4 = 1$. That is, $\frac{0}{\tau} = 0$.
Lastly, TNAF$(n) = [1,0,1,0,1] = 1 + \tau^2 + \tau^4$.

For this example, we utilized a point P in the form of polynomial basis which satisfies E_1. By choosing a certain irreducible polynomial, we can obtain the output of SM in the form of Q.

Solinas (2000) also considered other properties of TNAF. That is, α is divisible by τ^2 *iff* $r \equiv 2s \ (mod\ 4)$. For length $l(\alpha) > 30$ then $log_2 N(\alpha) - 0.55 < l(\alpha) < log_2 N(\alpha) + 3.52$, where $N(\alpha) = r^2 + trs + 2s^2$ is denoted as a norm of α. Besides that, he developed among the most efficient algorithms for converting TNAF in the form of $r + s\tau$ into $\sum_{i=0}^{l-1} c_i \tau^i$ as follows. This can eliminate the elliptic doublings in SM, and increase the number of addition operations.

Algorithm 1.1. (Converting $r + s\tau$ to $\sum_{i=0}^{l-1} c_i \tau^i$)
Input: integers r, s
Output: TNAF $(r + s\tau)$
Computation:

```
$c_0 \leftarrow r,\ c_1 \leftarrow s$
$S \leftarrow [\,]$
While $c_0 \neq 0$ or $c_1 \neq 0$
    If $c_0$ odd then
        $u \leftarrow 2 - (c_0 - 2c_1 \ mod\ 4)$
        $c_0 \leftarrow c_0 - u$
    Else
        $u \leftarrow 0$
    Prepend $u$ to $S$
    $(c_0, c_1) \leftarrow (c_1 + \frac{tc_0}{2} - \frac{c_0}{2})$
End While
Output $S$
```

The detailed algorithm for SM of nP where n is in the form of TNAF $(r + s\tau)$ can be referred to in Algorithm 3 (see Solinas, 2000). Other concepts of TNAF for SM have also been investigated in prior research (Avanzi et al., 2007, 2011; Blake et al., 2008; Heuberger, 2010; Hakuta et al., 2010; Heuberger & Krenn, 2013a; Yunos & Atan, 2016; Yunos & Suberi, 2018.) on Koblitz curves as well as the other types of curves.

Yunos et al. (2014) introduced τ in the expression in the form of $\tau^i = b_i\, t^i + a_i t^{i+1}\, \tau$, where $a_0 = 0,\ b_0 = 1,\ a_i = a_{i-1} + b_{i-1}$ and $b_i = -2a_{i-1}$ for $i > 0$. It is based on the Lucas sequence and is useful to accelerate the process of transforming TNAF in the form of $\sum_{i=0}^{l-1} c_i \tau^i$ into $r + s\tau$ with $r = \sum_{i=0}^{l-1} c_i\ b_i\ t^i$ and $s = \sum_{i=0}^{l-1} c_i\, a_i\, t^{i+1}$ (Yunos et al., 2015a, b, c).

Based on their theory, we rewrite the conversion process developed by Suberi et al. (2018) as follows: List all the patterns of $\mathbf{TNAF}(A) = [c_0, 0, \dots, 0, c_{l-1}]$ (see Tables 1 and 2) and $\mathbf{TNAF}(B) = [c_0, 0, \dots, c_{\frac{l-1}{2}}, \dots, 0, c_{l-1}]$ for $c_0, c_{\frac{l-1}{2}}, c_{l-1} \in \{-1, 1\}$ **(see Table 3)** and describe the properties of TNAF with the least number of nonzero coefficients, as in Proposition 1.1.

Algorithm 1.2. (Converting $\sum_{i=0}^{l-1} c_i \tau^i$ to $r + s\tau$)
Input: coefficient c_i *for* $i = 0, 1, 2, \dots, l-1$ *and trace* $t = (-1)^{1-a}$ *for* $a \in \{0, 1\}$.
Output: $r + s\tau$
Computation:

```
$a_0 \leftarrow 0,\ b_0 \leftarrow 1$
For i from 1 to $l - 1$ do
    $a_i \leftarrow a_{i-1} + b_{i-1}$
    $b_i \leftarrow -2a_{i-1}$
    $g_i \leftarrow a_i t^i$
    $h_i \leftarrow b_i t^{i+1}$
End do
$r \leftarrow \sum_{i=0}^{l-1} c_i h_i$
$s \leftarrow \sum_{i=0}^{l-1} c_i\, g_i$
Return to (r,s)
```

Proposition 1.1. *Let,* $a_0 = 0$ *and* $b_0 = 1$. *If* $\tau^i = b_i\, t^i + a_i\, t^{i+1}\tau$ *for* $a_i = a_{i-1} + b_{i-1}$, $b_i = -2a_{i-1}$ *and* $t \in \{-1, 1\}$ *then*

(i) $$TNAF(c_0 + c_{l-1}\ \tau^{l-1}) = (c_0 + c_{l-1}\, b_{l-1}\, t^{l-1}) + (c_{l-1}\, a_{l-1}\, t^l)\tau$$

for $c_0, c_{l-1} \in \{-1, 1\}$ *and* $l \geq 3$.

(ii) $$TNAF(\pm\left(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1}\right)) = \pm\left(\left(1 + b_{\frac{l-1}{2}}\ t^{\frac{l-1}{2}} + b_{l-1}\, t^{l-1}\right) + \left(a_{\frac{l-1}{2}}\ t^{\frac{l-1}{2}+1} + a_{l-1}\ t^l\right)\tau\right)$$

for $l = 3 + 2\eta$ *with* $\eta \in \mathbb{N}$.

The following is an example for Proposition 1.1.

Example 2.
TNAF $([1,0,0,0,0,0,1]) = \tau^6 + 1$ in Table 1 and $\mathbf{TNAF}\ ([-1,0,0,0,0,0,1]) = -\tau^6 + 1$ in Table 2 can be written as $3 + 5\tau$ and $1 + 5\tau$ respectively. The converting process uses Proposition 1.1 (i) and each expansion has a density of 2/7. Meanwhile, $\mathbf{TNAF}([1,0,0,1,0,0,1]) = \tau^6 + \tau^3 + 1$ in Table 3 can be transformed into $1 + 4\tau$ by using Proposition 1.1 (ii) and its density 3/7.
Yunos et al. (2019) proposes other patterns of TNAF expression (see Table 4) in the form of $\mathbf{TNAF}(C) = [0, c_1, \dots, c_{l-1}]$, $\mathbf{TNAF}(D) = [-1, c_1, \dots, c_{l-1}]$, $\mathbf{TNAF}(E) = [1, c_1, \dots, c_{l-1}]$ and $\mathbf{TNAF}(F) = [0, 0, 0, c_3, c_4, \dots, c_{l-1}]$, which occur between integer γ from 1 to 21, which use Algorithm 1.1 for converting γ into TNAF(γ) (or alternatively, use Algorithm 1.2 for converting TNAF(γ) into γ).

DOI: https://doi.org/10.22452/mjs.sp2022no1.2

Table 1. TNAF(A) with $c_0, c_{l-1} = \pm 1$ and $c_{\mathrm{i}} = 0$ for $i = 1,2,\ldots,l-2$ with its $r + s\tau$ and length, $3 \le l \le 15$.

TNAF(A)	$r + s\tau$	l	TNAF(A)	$r + s\tau$	l
$\pm[1,0,1]$	$\pm(-1+\tau)$	3	$\pm[1,0,0,0,0,0,0,0,0,1]$	$\pm(7-17\tau)$	10
$\pm[1,0,0,1]$	$\pm(-1-\tau)$	4	$\pm[1,0,0,0,0,0,0,0,0,0,1]$	$\pm(35-11\tau)$	11
$\pm[1,0,0,0,1]$	$\pm(3-3\tau)$	5	$\pm[1,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(23+23\tau)$	12
$\pm[1,0,0,0,0,1]$	$\pm(7-\tau)$	6	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-45 + 45\tau)$	13
$\pm[1,0,0,0,0,0,1]$	$\pm(3+5\tau)$	7	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-89-\tau)$	14
$\pm[1,0,0,0,0,0,0,1$	$\pm(-9+7\tau)$	8	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(3-91\tau)$	15
$\pm[1,0,0,0,0,0,0,0,1]$	$\pm(-13-3\tau)$	9			

Table 2. TNAF(A) with $c_0 = \mp 1, c_{l-1} = \pm 1$ and $c_{\mathrm{i}} = 0$ for $i = 1,2,\ldots,l-2$ with its $r + s\tau$ and length, $3 \le l \le 15$.

TNAF(A)	$r + s\tau$	l	TNAF(A)	$r + s\tau$	l
$\pm[-1,0,1]$	$\pm(-3+\tau)$	3	$\pm[-1,0,0,0,0,0,0,0,0,1]$	$\pm(5 - 17\tau)$	10
$\pm[-1,0,0,1]$	$\pm(-3-\tau)$	4	$\pm[-1,0,0,0,0,0,0,0,0,0,1]$	$\pm(33 - 11\tau)$	11
$\pm[-1,0,0,0,1]$	$\pm(1-3\tau)$	5	$\pm[-1,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(21 + 23\tau)$	12
$\pm[-1,0,0,0,0,1]$	$\pm(5-\tau)$	6	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-47 + 45\tau)$	13
$\pm[-1,0,0,0,0,0,1]$	$\pm(1+5\tau)$	7	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-91 - \tau)$	14
$\pm[-1,0,0,0,0,0,0,1]$	$\pm(-11 + 7\tau)$	8	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(181 - 89\tau)$	15
$\pm[-1,0,0,0,0,0,0,0,1]$	$\pm(-15 - 3\tau)$	9			

Table 3. TNAF(B) with $c_0, c_{\frac{l-1}{2}}, c_{l-1} = \pm 1$ and $c_i = 0\ , i = 1,2,\ldots,l-2$ with its $r + s\tau$ and length, $l = 5, 7, 9, \ldots, 21$.

TNAF(B)	$r + s\tau$	l
$\pm[1, 0, 1, 0, 1]$	$\pm(1-2\tau)$	5
$\pm[1, 0, 0,1, 0, 0, 1]$	$\pm(1+4\tau)$	7
$\pm[1, 0, 0, 0, 1, 0, 0, 0, 1]$	$\pm(-11-6\tau)$	9
$\pm[1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1]$	$\pm(41-12\tau)$	11
$\pm[1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1]$	$\pm(-43+50\tau)$	13
$\pm[1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1]$	$\pm(-7-84\tau)$	15
$\pm[1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1]$	$\pm(165+90\tau)$	17
$\pm[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]$	$\pm(-535+\ 68\tau)$	19
$\pm[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$	$\pm(949-636\tau)$	21

Table 4. TNAF($\boldsymbol{\gamma}$) for integer $\mathbf{1} \le \boldsymbol{\gamma} \le \mathbf{21}$ and its HW and length ($\boldsymbol{l}$).

$\boldsymbol{\gamma}$	TNAF($\boldsymbol{\gamma}$)	HW	$\boldsymbol{l}$	$\boldsymbol{\gamma}$	TNAF($\boldsymbol{\gamma}$)	HW	$\boldsymbol{l}$
1	$[\mathbf{1}]$	1	1	12	$[\mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	4	9
2	$[\mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	2	4	13	$[\mathbf{1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	5	9
3	$[\mathbf{-1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}]$	3	6	14	$[\mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	4	9
4	$[\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	2	6	15	$[\mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{-1}]$	3	9
5	$[\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	3	6	16	$[\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{-1}]$	2	9
6	$[\mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	2	6	17	$[\mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{-1}]$	3	9
7	$[\mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{1}]$	3	6	18	$[\mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}]$	4	9
8	$[\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{1}]$	2	6	19	$[\mathbf{-1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	5	11
9	$[\mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{1}]$	3	6	20	$[\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	4	11
10	$[\mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	4	9	21	$[\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}]$	5	11
11	$[\mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}, \mathbf{0}, \mathbf{-1}]$	5	9				

DOI: https://doi.org/10.22452/mjs.sp2022no1.2

Hamming Weight (HW) in Table 4 is defined as the number of nonzero coefficients in the expression of an element in $\mathbb{Z}(\tau)$ (Solinas, 2000; Yunos & Atan, 2013). The following proposition illustrates the pattern of all TNAF (γ) in this table, where γ in terms of $2+2k$, $3+4k$, $5+4k$ and $8k_1+8k_2$.

Proposition 1.2.
Let k be any integer, $k_1, k_2 \in \mathbb{N}$ *and* $c_i \in \{-1,0,1\}$. *Then,*

(i) $TNAF(2+2k) = \sum_{i=1}^{l-1} c_i \tau^i$.

(ii) $TNAF(3+4k) = -1 + \sum_{i=1}^{l-1} c_i \tau^i$.

(iii) $TNAF(5+4k) = 1 + \sum_{i=1}^{l-1} c_i \tau^i$.

(iv) $TNAF(8k_1+8k_2) = \sum_{i=3}^{l-1} c_i \tau^i$.

This study then determines the actual formula for TNAF of A-F in the form of $r + s\tau$. Hadani et al. (2019a, b) resolved this issue by applying $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1}t^{m-2i+1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ as follows.

Proposition 1.3.
If $\tau^m = -2s_{m-1} + s_m\tau$ *for* $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1}t^{m-2i+1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ *and* $t \in \{-1,1\}$, *then*

(i) $TNAF(c_0 + c_{l-1}\tau^{l-1}) = \left(c_0 - 2c_{l-1}\left(1 + \sum_{i=2}^{l-2} \frac{(-2)^{i-1}t^{l-1}}{(i-1)!}\prod_{j=i}^{2i-2}(l-2-j)\right)\right) + c_{l-1}\tau\left(t + \sum_{i=2}^{l-1} \frac{(-2)^{i-1}t^{l}}{(i-1)!}\prod_{j=i}^{2i-2}(l-1-j)\right)$
for $c_0, c_{l-1} \in \{-1,1\}$ *and* $l \geq 3$.

(ii) $TNAF(\pm\left(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1}\right)) = \pm\left[1 - 2\left(t^{\eta+1} + \sum_{i=2}^{\eta} \frac{(-2)^{i-1}t^{\eta+1}}{(i-1)!}\prod_{j=i}^{2i-2}(\eta-j)\right) - 2\left(1 + \sum_{i=2}^{2\eta+1} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(2\eta+1-j)\right) + \left(t^{\eta} + \sum_{i=2}^{1+\eta} \frac{(-2)^{i-1}t^{\eta}}{(i-1)!}\prod_{j=i}^{2i-2}(1+\eta-j) + t + \sum_{i=2}^{2+2\eta} \frac{(-2)^{i-1}t}{(i-1)!}\prod_{j=i}^{2i-2}(2+2\eta-j)\right)\tau\right]$
for $l = 3 + 2\eta$ *with integer* $\eta \geq 2$.

Proposition 1.4.
Let k *be any integer,* k_1, $k_2 \in \mathbb{N}$ *and* $c_m \in \{-1,0,1\}$. *If* $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1}t^{m-2i+1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$, *then*

(i) $TNAF(2+2k) = -2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)\right) + \tau\sum_{m=1}^{l-1} c_m t^{m+1}\left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)\right)$
.

(ii) $TNAF(3+4k) = -1 - 2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)\right) + \tau\sum_{m=1}^{l-1} c_m t^{m+1}\left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)\right)$.

(iii) $TNAF(5+4k) = 1 - 2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)\right) + t\tau\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)\right)$.

(iv) $TNAF(8k_1+8k_2) = -2\sum_{m=3}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)\right) + t\tau\sum_{m=3}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)\right)$.

However, the construction of s_m in Propositions 1.3 and 1.4 are still rather complex. They are based upon the pyramid number formula, Nichomacus's theorem and Faulhaber's formula, as described by Hadani and Yunos (2018). The primary objective of this research is to derive TNAF of A-F in a more concise form by applying $\tau^m = -2s_{m-1} + s_m\tau$, where $s_m = t^{m+1}\sum_{i=1}^{\left\lfloor\frac{m+1}{2}\right\rfloor} (-2)^{i-1}\binom{m-i}{i-1}$, which is based on *v*-simplex and arithmetic sequences. The detailed development of s_m can be obtained in Yunos et al. (2021).

This paper is structured as follows. In this section, we give some properties describing the patterns for TNAF of A - F (see Propositions 1.1-1.4) produced by previous researchers. In the next section, we describe the preliminaries of this study. In Section 3, we discuss how to improve Propositions 1.3 and 1.4 using a new approach, which is the main objective of this research, and describe its advantages in cryptosystems. The final chapter concludes.

2. Preliminaries

The following are propositions and algorithms that were used throughout this study.

Proposition 2.1. (Hadani et al., 2019a)
Given $\tau^m = r_m + s_m\tau$ *an element of* $\mathbb{Z}(\tau)$ *for* $m \in \mathbb{Z}^+$. *Let* $s_1 = 1$ *and* $s_2 = t$. *If* $f_{i_m} = \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ *for* $2 \leq i \leq \frac{m+1}{2}$ *and* $m \geq 2i-1$, *then* $s_m = \sum_{i=1}^{\left\lfloor\frac{m+1}{2}\right\rfloor} f_{i_m} t^{m-2i+1}$ *with* $f_{1_m} = 1$ *and* $m \geq 3$. *Subsequently,* $r_m = -2s_{m-1}$.

Yunos et al. (2021) described an argument that $f_{i_m} = \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ is equal to $\beta_{k_m} = (-2)^{k-1}\binom{m-k}{k-1}$ for $m \geq 2$. This new approach reduced the complexity of formula s_m in Proposition 2.1, and obtained a more practical formula for τ^m. That is,

$$\tau^m = -2s_{m-1} + s_m\tau = -2\sum_{k=1}^{\left\lfloor\frac{m}{2}\right\rfloor} \beta_{k_{m-1}} t^m + \tau\sum_{k=1}^{\left\lfloor\frac{m+1}{2}\right\rfloor} \beta_{k_m} t^{m+1} \qquad (1)$$

The first application of using this result is TNAF ($\boldsymbol{\alpha}$) in the form of $\boldsymbol{r+s\tau}$ can be obtained from $\sum_{m=0}^{l-1} c_m\,\tau^m$, and its algorithm is developed as follows:

Algorithm 2.2. Converting $\sum_{m=0}^{l-1} c_m\,\tau^m$ to $\boldsymbol{r+s\tau}$ (Yunos et al., 2021)

Input: $t \leftarrow (-1)^{1-a}$ *for* $a \in \{0,1\}$, *all coefficients* $c_m \in \{-1,0,1\}$ *for* $m = 0,1,\dots,l-1.$

Output: $r+s\tau$

Computation:

```
1. For m from 0 to 1 do
2.     $d_m \leftarrow \tau^m$
3. End do
4. For m from 2 to $l-1$ do
5.     $h_m \leftarrow \lfloor\frac{m}{2}\rfloor,\ \ g_m \leftarrow \lfloor\frac{m+1}{2}\rfloor$
6.     $r_m \leftarrow t^m \sum_{k=1}^{h_m} \frac{(-2)^k\,(m-1-k)!}{(k-1)!\,(m-2k)!}$
7.     $s_m \leftarrow t^{m+1} \sum_{k=1}^{g_m} \frac{(-2)^{k-1}\,(m-k)!}{(k-1)!(m-2k+1)!}$
8.     $d_m \leftarrow r_m + s_m\tau$
9. End do
10. $r+s\tau \leftarrow \sum_{m=1}^{l-1}\ c_m d_m$
```

Therefore, it is easy to get back, for example: $\boldsymbol{1-2\tau}$ from $\boldsymbol{1+\tau^2+\tau^4}$ (refer to the reverse calculation in Example 1). Besides that, transforming $(\rho_0+\rho_1\tau)\ \frac{\tau^m-1}{\tau-1}$ to $r+s\tau$ where τ^m, based on Equation (1), is more efficient than applying the Lucas sequence. Therefore, this can enhance the performance of the conversion process as required in TNAF of *n* modulo $(\rho_0+\rho_1\tau)\ \frac{\tau^m-1}{\tau-1}$ prior to doing SM. Meanwhile, the second advantage of using Equation (1) is given in the following section.

3. Result

The following theorems improve the formulas for TNAF expansions of type A-F that were mentioned in Propositions 1.3 and 1.4.

Theorem 3.1. *If* $\tau^m = -2s_{m-1} + s_m\tau$ *for* $s_m = \sum_{k=1}^{\lfloor\frac{m+1}{2}\rfloor}\ \beta_{k_m}\,t^{m+1}$, *then*

(i) $\boldsymbol{TNAF}(c_0 + c_{l-1}\tau^{l-1}) = (c_0 - 2c_{l-1}s_{l-2}) + c_{l-1}s_{l-1}\tau$

for $c_0, c_{l-1} \in \{-1,1\}$ **and** $l \geq 3.$

(ii) TNAF $(\pm\left(1+\tau^{\frac{l-1}{2}}+\tau^{l-1}\right)) = \pm\left[\left(1-2(s_\eta + s_{2\eta+1}\right)\right) + \left(s_{\eta+1}+s_{2\eta+2}\right)\tau\right]$

for $l = 3+2\eta$ *with integer* $\eta \geq 2.$

Proof.

Let $\tau^m = -2s_{m-1} + s_m\tau$ with $s_m = \sum_{k=1}^{\lfloor\frac{m+1}{2}\rfloor}\ \beta_{k_m}\,t^{m+1}.$

(i) By considering $m = l-1$ for $l \geq 3$, we obtain $c_0 + c_{l-1}\tau^{l-1} = c_0 + c_{l-1}(-2s_{l-2} + s_{l-1}\tau) = (c_0 - 2c_{l-1}s_{l-2}) + c_{l-1}s_{l-1}\tau.$

(ii) Suppose $l = 3+2\eta$ for integer $\eta \geq 2,$ thus $l-1 = 2+2\eta$ *and* $\frac{l-1}{2} = 1+\eta.$

Now, $\pm\left(1+\tau^{\frac{l-1}{2}}+\tau^{l-1}\right) = \pm[1+\tau^{1+\eta}+\tau^{2+2\eta}]$

$= \pm\left[\left(1 + \left(-2s_\eta + s_{1+\eta}\tau\right) + \left(-2s_{2\eta+1} + s_{2+2\eta}\tau\right)\right)\right]$

$= \pm\left[(1 - 2s_\eta - 2s_{2\eta+1}) + (s_{1+\eta} + s_{2+2\eta})\tau\right].$

This completes the proof.

Theorem 3.2. *Let* k *be any integer,* $k_1,\ k_2 \in \mathbb{N}$, *and* $c_m \in \{-1,0,1\}.$ *If* $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{k=1}^{\lfloor\frac{m+1}{2}\rfloor}\ \beta_{k_m}\,t^{m+1}$, *then*

(i) *TNAF* $(2+2k) = -2\sum_{m=1}^{l-1} c_m\,s_{m-1} + \tau\sum_{m=1}^{l-1} c_m\,s_m.$

(ii) *TNAF* $(3+4k) = -1 - 2\sum_{m=1}^{l-1} c_m\,s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m.$

(iii) *TNAF* $(5+4k) = 1 - 2\sum_{m=1}^{l-1} c_m\,s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m.$

(iv) *TNAF*$(8k_1 + 8k_2) = -2\sum_{m=3}^{l-1} c_m\,s_{m-1} + \tau\sum_{m=3}^{l-1} c_m\,s_m.$

Proof.

Let $\tau^m = -2s_{m-1} + s_m\tau$ with $s_m = \sum_{k=1}^{\lfloor\frac{m+1}{2}\rfloor}\ \beta_{k_m}\,t^{m+1}.$

(i) By using Proposition 1.2 (i), we have

$\mathbf{TNAF}(2+2k) = \sum_{m=1}^{l-1} c_m\,\tau^m = -2\sum_{m=1}^{l-1} c_m s_{m-1} + \tau\sum_{m=1}^{l-1} c_m\,s_m.$

(ii) By using Proposition 1.2 (ii), we have

$\mathbf{TNAF}(3+4k) = -1 + \sum_{m=1}^{l-1} c_m\,\tau^m$

$= \left(-1 - 2\sum_{m=1}^{l-1} c_m s_{m-1}\right) + \tau\sum_{m=1}^{l-1} c_m\,s_m.$

(iii) By using Proposition 1.2 (iii), we have

$\mathbf{TNAF}(5+4k) = 1 + \sum_{m=1}^{l-1} c_m\,\tau^m$

$= \left(1 - 2\sum_{m=1}^{l-1} c_m s_{m-1}\right) + \tau\sum_{m=1}^{l-1} c_m\,s_m.$

(iv) By using Proposition 1.2 (iv), we have

TNAF$(8k_1 + 8k_2) = \sum_{m=3}^{l-1} c_m\,\tau^m = -2\sum_{m=3}^{l-1} c_m s_{m-1} + \tau\sum_{m=3}^{l-1} c_m\,s_m$.

This completes the proof.

Consequently, we can create another algorithm that has a similar performance to the running process with Algorithm 2.2 for converting TNAF (for example of types A and E) in the form of $\sum_{m=1}^{l-1} c_m\,\tau^m$ to $\boldsymbol{r+s\tau}$ (refer to the formulas of *r* and *s* in Theorem 3.1 part (i) and Theorem 3.2 part (iii)) as follows:

Algorithm 3.1.

Input: $t \leftarrow (-1)^{1-a}$ *for* $a \in \{0,1\}$, *all coefficients* $c_m \in \{-1,0,1\}$ *for* $m = 1,\dots,l-1.$

Output: $r+s\tau$

Computation:

```
1. For m from 1 to $l-1$ do
2.     $h_m \leftarrow \lfloor\frac{m}{2}\rfloor,\ \ g_m \leftarrow \lfloor\frac{m+1}{2}\rfloor$
3.     $r_m \leftarrow t^m \sum_{k=1}^{h_m} \frac{(-2)^k\,(m-1-k)!}{(k-1)!\,(m-2k)!}$
4.     $s_m \leftarrow t^{m+1} \sum_{k=1}^{g_m} \frac{(-2)^{k-1}\,(m-k)!}{(k-1)!(m-2k+1)!}$
5. End do
6. $r \leftarrow 1 - 2\sum_{m=1}^{l-1}\ c_m s_{m-1}$
7. $s \leftarrow \sum_{m=1}^{l-1}\ c_m s_m$
```

8. *Return*$(\boldsymbol{r}, \boldsymbol{s})$

Besides, Figure A1 illustrates this algorithm by applying Maple programming with a computer with an Intel(R) Core (TM) i7 processor, 8 GB RAM and a 64-bit operating system. This result is also an extension of a prior study (Suberi et al., 2016; Yunos & Suberi, 2018) to scrutinize the property of unsecure keys prior to doing SM on Koblitz Curves. Algorithm 3.1 helps Alice to list down some patterns of unsecure keys and acts as a multiplier of SM before sending a cypher text $(\boldsymbol{Q})$ to Bob. The following example is an impact of being able to identify a plain text $(\boldsymbol{P})$ by choosing some value of $\boldsymbol{r}+\boldsymbol{s\tau}$ and their TNAF and $\boldsymbol{Q}$.

TNAF	$\boldsymbol{r}+\boldsymbol{s\tau}$	$\boldsymbol{Q}=\boldsymbol{nP}$
$[\mathbf{1},\mathbf{0},\mathbf{1}]$	$-\mathbf{1}+\boldsymbol{\tau}$	$(\boldsymbol{x}^{\mathbf{2}}+\boldsymbol{x}+\mathbf{1},\mathbf{0})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1}]$	$-\mathbf{1}-\boldsymbol{\tau}$	$(\boldsymbol{x}+\mathbf{1},\boldsymbol{x}+\mathbf{1})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}]$	$\mathbf{3}-\mathbf{3}\boldsymbol{\tau}$	$(\boldsymbol{x}+\mathbf{1},\mathbf{0})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}]$	$\mathbf{7}-\boldsymbol{\tau}$	$(\boldsymbol{x}^{\mathbf{2}}+\boldsymbol{x}+\mathbf{1},\mathbf{0})$

Although Alice sends different values of $\boldsymbol{Q}$ to Bob with different multipliers of *P*, the third parties can attack $\boldsymbol{P}=(\boldsymbol{x},\boldsymbol{x}^{\mathbf{2}}+\mathbf{1})$ easily. Therefore, such keys need to be avoided in real-world scenarios of cryptosystems.

5. Conclusion

In this work, we derive TNAF of types A-F in more concise forms by applying Equation (1), which is based on *v*-simplex and arithmetic sequences. This research can be extended by looking at the nature of such patterns such that TNAF has a low-density. Besides, their possible attacks by third parties need to be explored when implementing such kinds of expansions as secret keys.

6. Acknowledgements

This work was supported by Universiti Putra Malaysia with Putra Grants GP/ 2018/9595400 so that the study has a significant impact on the environment of ECC cryptography systems based on $\boldsymbol{\tau}$ -adic non adjacent.

7. References

Avanzi R M., Heuberger C., Prodinger H. (2007). On redundant τ-adic expansions and non-adjacent digit sets, Proceeding of the 13th International Workshop on Selected Areas in Cryptography, SAC 2006, Lecture Notes in Computer Science, Springer-Verlag 4356: 285-301.

Avanzi R M., Heuberger C., Prodinger H. (2011). Redundant τ-adic expansions I: Non-adjacent digit sets and their applications to scalar multiplication, Des. Codes Cryptography 58 (2): 173-202.

Blake I F V., Murty K., Xu G. (2008). Nonadjacent Radix-τ expansions of integers in euclidean imaginary quadratic number fields, Canadian Journal of Mathematics 60(6): 1267-1282.

Hadani N H., Yunos F. (2018). Alternative formula of τ^m in scalar multiplication on Koblitz curve, Proceeding of the 25th National Symposium on Mathematical Sciences (Sksm25), AIP Publishing, AIP Conference Proceedings 1974(1): 1-9.

Hadani N H., Yunos F., Suberi S. (2019a). On some specific patterns of τ -adic non-adjacent form expansion over ring Z (τ): An alternative formula. In AIP Conference Proceedings 2138 Issue 1; Ibrahim, H., Zulkepli J., Yaakub, A M.; AIP Publishing: 1-10.

Hadani N H., Yunos F., Kamel Arifin M R., Sapar S H. and Rahman N N A. (2019b). Alternative method to find the number of points on Koblitz curve, Malaysian Journal of Science. 13(S) August, Special Issue: The 6th International Cryptology and Information Security Conference: 13-30.

Hankerson D., Menzenes A J., Venstone S. (2006). Guide to elliptic curve cryptography, Springer Science & Business Media.

Heuberger C. (2010). Redundant τ-adic expansions II: non-optimality and chaotic behaviour, Mathematics in Computer Science 3(2):141-157.

Heuberger C., Krenn D. (2013a). Existence and optimality of w-non-adjacent forms with an algebraic integer base, Acta Mathematica Hungarica 140: 90-104.

Heuberger C., Krenn D. (2013b). Analysis of width-w non-adjacent forms to imaginary quadratic, Journal of Number Theory 133(5): 1752-1808.

Hakuta K., Sato H., Takagi T., Jarvinen K. (2010). Explicit lower bound for the length of minimal weight τ-adic expansions on Koblitz curves, Journal of Math-for-Industry 2 (2010A-7): 75-83.

Koblitz N. (1987). Elliptic curve cryptosystem, Mathematics Computation 48 (177): 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

Koblitz N. (1992). CM curves with good cryptographic properties. In Advances in cryptology CRYPTO 91: Proceedings 576; Feigenbaum J.; Springer: Berlin, Heidelberg: 279-287. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.137.6778

Solinas J A. (1997). An improved algorithm for arithmetic on a family of elliptic curves, Advance in Cryptology-CRYPTO'97, 1294, Burton S., and Kaliski Jr.; Springer: Berlin, Heidelberg: 357-371.

Solinas J A. (2000). Efficient arithmetic on Koblitz curves, Kluwer Academic Publishers, Design, Codes, and Cryptography, J.A.; Springer: Boston, Massachusetts 19:

DOI: https://doi.org/10.22452/mjs.sp2022no1.2

195-249. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.157.2469

Suberi S., Yunos F., Md Said M R. (2016). An even and odd situation for the multiplier of scalar multiplication with pseudo τ -adic non-adjacent form. In AIP Conference Proceedings 1750, AIP Publishing: 1-9. https://doi.org/10.1063/1.4954597

Suberi S., Yunos F., Md Said M R., Sapar S H., Said Husain Sh K. (2018). Formula of τ-adic nonadjacent form with the least number of non-zero coefficients, Jurnal Karya Asli Lorekan Ahli Matematik 11(1): 23-30.

Yunos F., Atan M K A. (2013). An average density of τ-adic naf (τ-NAF) representation: An alternative proof, Malaysian Journal of Mathematical Sciences *7*(1): 111-123.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2014). A reduced τ-NAF (RTNAF) representation for scalar multiplication on anomalous binary curves (ABC), Pertanika Journal of Science and Technology 22(2): 489-506.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015a). Pseudo T-Adic nonadjacent form for scalar multiplication on Koblitz curves, Malaysian Journal of Mathematical Sciences 9(S) (Special Issue: The 4th International Cryptology and Information Security Conference 2014): 71-88.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015b). Pseudo T-adic nonadjacent form for scalar multiplication on Koblitz curves, Conference Proceeding of the 4th International Cryptology and Information Security Conference 2014: 120-130.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015c). Kembangan Pseudotnaf bagi pendaraban skalar ke atas lengkuk Koblitz, Ph.D. thesis, Universiti Putra Malaysia.

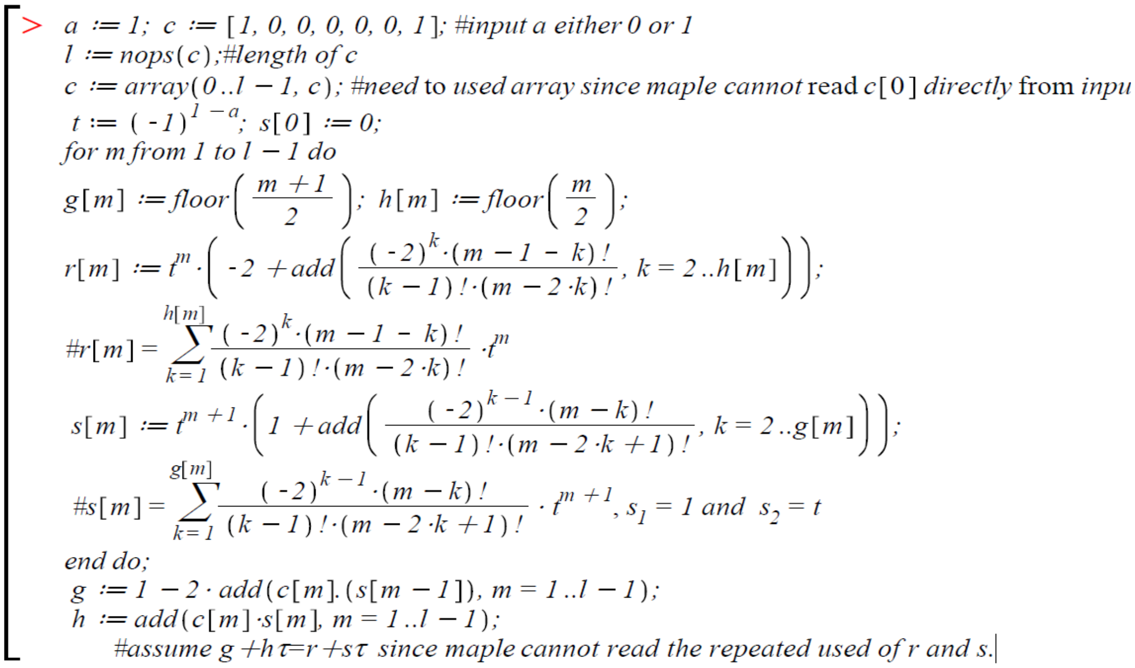
Yunos F., Atan M K A. (2016). Improvement to scalar multiplication on Koblitz curves by using Pseudo τ-adic non-adjacent form, Advances in Industrial and Applied Mathematics, Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences (SKSM23), AIP Publishing 1750: 050006.

Yunos F., Suberi S. (2018). Even and odd nature for pseudo τ-adic non-adjacent form, Malaysian Journal of Science 37(2): 94-102.

Yunos F., Suberi S., Said Husain Sh K., Ariffin M R K., Asbullah M A. (2019). On some specific patterns of τ -adic non-adjacent form expansion over ring Z (τ), Journal of Engineering and Applied Sciences.

Yunos F., Mohd Yusof A., Hadani N H., Kamel Arifin M R., Sapar S H. (2021). Power of frobenius endomorphism and its performance on PseudoTNAF system, new ideas in Cryptology in Malaysian Journal of Mathematical Sciences 15(S) December: 105-121.

Appendix



> $a := 1;\ c := [1, 0, 0, 0, 0, 0, 1];$ *#input a either 0 or 1*

$l := nops(c);$*#length of c*

$c := array(0..l-1, c);$ *#need* to *used array since maple cannot* read $c[0]$ *directly* from *inpu*

$t := (-1)^{1-a};\ s[0] := 0;$

for m from 1 to l − 1 do

$g[m] := floor\left(\frac{m+1}{2}\right);\ h[m] := floor\left(\frac{m}{2}\right);$

$r[m] := t^{m}\cdot\left(-2 + add\left(\frac{(-2)^{k}\cdot(m-1-k)!}{(k-1)!\cdot(m-2\cdot k)!}, k = 2..h[m]\right)\right);$

$\#r[m] = \sum_{k=1}^{h[m]}\frac{(-2)^{k}\cdot(m-1-k)!}{(k-1)!\cdot(m-2\cdot k)!}\cdot t^{m}$

$s[m] := t^{m+1}\cdot\left(1 + add\left(\frac{(-2)^{k-1}\cdot(m-k)!}{(k-1)!\cdot(m-2\cdot k+1)!}, k = 2..g[m]\right)\right);$

$\#s[m] = \sum_{k=1}^{g[m]}\frac{(-2)^{k-1}\cdot(m-k)!}{(k-1)!\cdot(m-2\cdot k+1)!}\cdot t^{m+1}, s_1 = 1 \text{ and } s_2 = t$

end do;

$g := 1 - 2\cdot add(c[m].(s[m-1]), m = 1..l-1);$

$h := add(c[m]\cdot s[m], m = 1..l-1);$

#assume g + hτ = r + sτ since maple cannot read the repeated used of r and s.

Figure A1. Programming for Algorithm 3.1 by Using Maple

DOI: https://doi.org/10.22452/mjs.sp2022no1.2

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021
Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 17-22 (September 2022) https://mjs.um.edu.my

EX VIVO TERAHERTZ IMAGING REFLECTION OF MALIGNANT AND BENIGN HUMAN BREAST TUMORS

Amel Al-Ibadi*

Abstract: This study evaluated the effectiveness of spectroscopy and imaging tools, using a previously-unexplored (0.2- 1.4) terahertz range, for investigating tumors in human tissue and distinguishing between malignant and benign cancer cells. One advantage of this technique is that terahertz radiation in this frequency range passes through human tissue without causing ionization or any negative effects To assess the effectiveness of this band of frequencies, THz data were collected from 10 different fresh breast tissue samples, extracted directly after excision. The optical properties were investigated at a range of low frequencies and THz imaging revealed good contrast between the different types of fresh tissue. Observations indicated that the optical and electrical properties in the low-frequency (0.3-0.5) range provided accurate information about breast cancer tissue. These results demonstrated the effectiveness of the technique up to 0.5 THz for ex vivo studies in medical applications.

Keywords: *Terahertz imaging, terahertz radiation, medical & biological tissues and tissue characterizations.*

1. Introduction

This Terahertz spectroscopy and imaging technique was used to produce two- or three-dimensional images of an object, using THz radiation (0.1 to 10THz) beamed directly or reflected through the samples, thus providing highly accurate information about tissues inaccessible to other technologies (Gong et al., 2020). Terahertz radiation is non-ionized (Peter et al., 2013) and harmless to the objects tested (Yu et al., 2012). Terahertz radiation, in the low-millimeter waveband, is highly absorbed in the water in living tissues (Wilmink & Grundt, 2011). The Terahertz team used a terahertz technique to visualize and analyze human tissue, with the aim of detecting and identifying different types of cancer tumors and comparing these images with the results of laboratory analysis by a medical oncology team. Previous studies asserted that terahertz imaging facilitated early cancer detection in tissues, before it became visible, widespread, or sensitive to any other technique. Moreover, in samples exposed to terahertz radiation, diseased tissues were readily distinguished from healthy tissues, making this technique an effective tool for future medical applications (Cassar et al., 2018). In particular, the absorption and refraction coefficients of tumor tissues were higher than those of healthy tissues (Wahaia et al., 2020). Differences between tissue regions had previously been studied between 500 and 600 GHz (Al-Ibadi et al., 2017). The distinction, variation, and differences in physical characteristics between tissues are due to the presence of water and changes in the composition of the infected tissue, such as higher cell and protein density and increased water content (Sun et al., 2013). Access to all information relating to the tissue is through exposure to terahertz radiation within a specified range of frequencies and the formation of adequate images of areas with confirmed or suspected tumors that distinguish them from healthy regions (Cassar et al., 2018). Previous research confirmed that cancer tumors had higher absorption and refraction factors than healthy tissues within a given frequency range (Fan et al., 2014). Terahertz spectroscopy is highly effective at distinguishing tumors from healthy tissues (El-Shenawee et al., 2019), thus helping surgeons remove tumors more precisely and avoid cutting out too much healthy tissue. The assurance of leaving no cancerous tissue in the patient's body minimizes the need for extensive removal of healthy tissue around the tumor, which is considered a safety precaution, but is prejudicial to patients and significantly extends recovery time, as well as avoiding repeated operations in the future. Recent research and studies suggest that the terahertz imaging technique is capable of distinguishing between infected and healthy tissue and provides valuable tissue-related diagnostic information that cannot be obtained using currently-available imaging techniques (Al-Ibadi et al., 2017).

Cancer is the second leading cause of death in the world, with outcomes exacerbated by late onset of symptoms and widespread lack of diagnostic and therapeutic services. Cells in malignant tumors (cancer) grow and divide rapidly and uncontrollably, leading to invasion and damage of natural

Authors information:
Biomedical physics department, College of medicine, University of Al-Qadisiyah, Iraq.

*Corresponding Author: Ml_absq@yahoo.com

Received: January 22, 2022
Accepted: April 22, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.3

tissue (WHO, 2017). The main diagnostic steps of examining tissue from the patient, identifying infected cells, distinguishing them from healthy tissue, and delivering the result may take at least 10 days. The diagnosis may be inaccurate, potentially leading to repeated excisions of infected tissue surrounded by insufficient amounts of intact tissue, which has not only physical, but also psychological and financial implications for the patient.

Cancer is not defined by one type or specific, persistent symptoms, since cancer cells continue unlimited division, accompanied by changes in their synthesis, functional and behavioral characteristics (Wang et al., 2014). Terahertz rays used to detect cancer and determine the degree of proliferation penetrate the tissue without causing any biological changes (Hejmadi, 2010).

The aim of this study on breast cancer was to identify the different regions in excised biological tissue and examine their physical properties, especially their dielectric properties, using terahertz imaging and spectroscopy to discriminate between tumors and normal tissue. THz radiation is produced by centering ultrafast (100fs) laser light on the space between the electrodes at near infrared wavelengths (a Ti:Sapphire laser with a central wavelength of 800 nm). Free-carrier acceleration results in the figuration of the transverse photoreceptor connected with an antenna, producing a wide band of frequencies between 100 GHz and 3 THz. Coherent photoconductor detection is achieved using a photonic antenna similar to the emitter. The signal-to-noise ratio is around 4000: 1, limited by the thermal noise of the antenna.

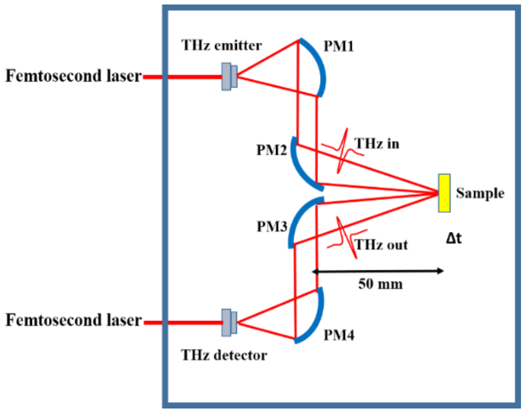


Figure 1. Schematic of Teraview system

2. Experimental Method

These experiments were conducted using a commercially-available TeraView 3000 (Teraview Ltd, Cambridge, UK, 2001) with a reflection system (Figure.1) to determine the complex dielectric properties of fresh tissues, initially to qualify the setup and data processing. A set of 10 fresh tissue samples were surgically removed from women's breasts (age range: 40-60 years) for cancer analysis. The standard operating procedure was followed at the Bergonié Institute in Bordeaux (France) to obtain human tissue sections containing breast cancer. The sapphire substrate was chosen to avoid bio-impact. The sample was fixed on the motor to scan THz pulse reflectivity. Step size and acquisition time depended on sample size. The system was purged of water particles by injecting dry air. Spatial resolution was determined by our system setup and the frequency used in this work. The samples were fixed between two 1 mm-thick quartz plates with slight pressure to avoid air gaps between the tissue and the quartz surface (Figure 2). The reflected THz pulse was measured with and without the sample to extract data on the frequency-dependent physical properties of the sample, detected by the second reflected pulse (from the sapphire-sample interface). The optical properties of these samples in the 0.2-1.4 THz range are presented in Figure 4. THz spectroscopy was also used in reflective mode, focusing on the acquisition of images to determine breast cancer. Analysis of processed THz images in the time and frequency domain presented in Figure 3 and their optical properties were used to distinguish between tumors and healthy tissues with high accuracy. These THz images were highly correlated with the histopathological images.

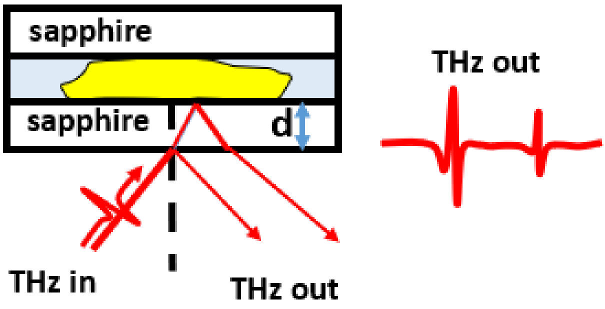


Figure 2. Schematic of the study sample (yellow) between two sapphire (white) windows with thickness (d). The two main reflex peaks. The bottom peak (THz out) reflected from the sapphire-air interface (without sample) and from the sapphire-sample interface (with sample).

2.1 Breast tissue sample preparation

After surgery, the tissues were prepared in accordance with standard laboratory methods for tissue collection, preparation, and fixation, for examination by pathologists at the Bergonié institute in Bordeaux (France). All samples were taken during breast surgery and all studies were histologically confirmed by a pathologist. Additionally, a pathologist identified diseased and healthy tissue in all samples for THz imaging. Appropriate healthy and infected tissues were determined by comparison with samples examined using the terahertz technique.

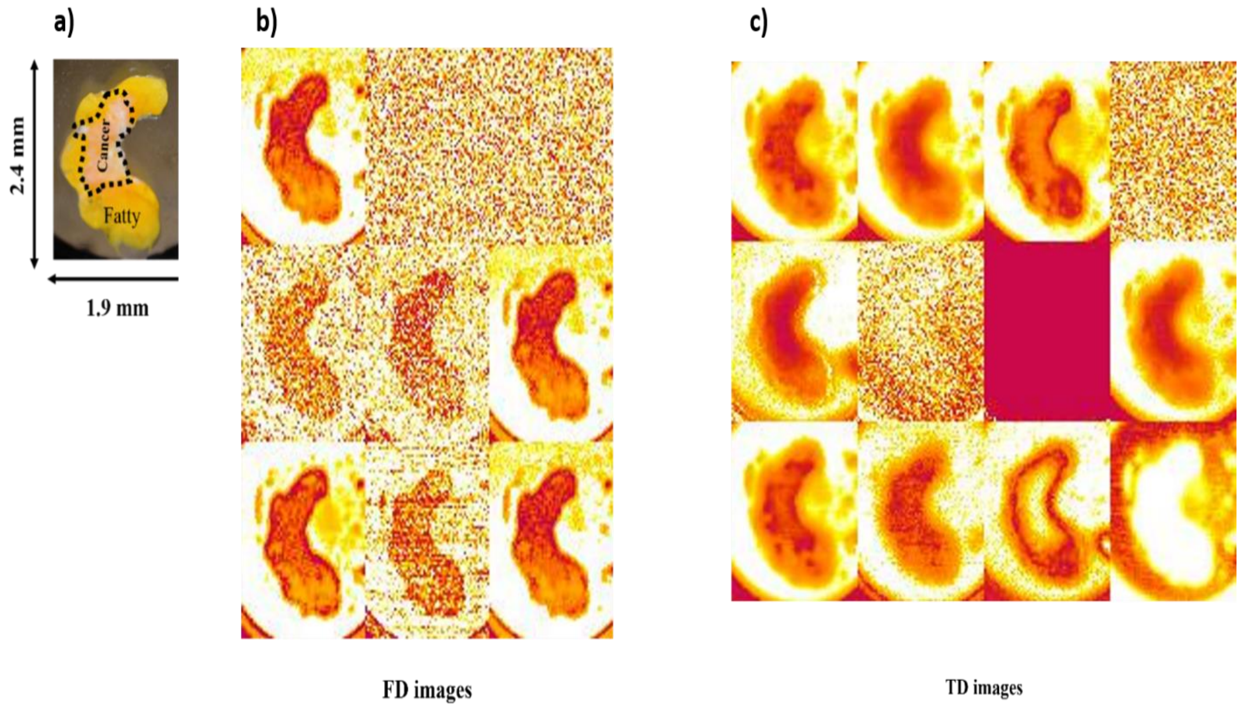


Figure 3. a) Optical image of the tissue studied, b and c) Automatic extraction of the different THz images based on the time-frequency domain, in order of mathematical operations, respectively, from left to right: Diff, Div, derivative, energy-entropy, FWHM [0-max] down, FWHM [0-max] up, FWHM [min-max] up, max, mean, min, mult, entropy-Shannon, and sum operation processes.

2.2 Data acquisition

The THz pulses were focused on a 3 mm-thick sample placed flat between the sapphire substrates at an incident angle of 10 deg. THz images were measured by a raster reflection scanning system, where the sample stage was moved two-dimensionally (2D) in an x-y plane on exposure to the THz waves with step size 0.2 mm, to measure the THz signals reflected in each pixel area. All reflection signals from the recorded samples scanned produced 4096 data points, giving a three-dimensional THz image. A two-dimensional image of the amplified signal through the THz scanning beam was created in each pixel of the image (Figure 4).

2.3 Image processing

After THz collection and processing, the data on the relevant frequency range was sufficiently accurate for feature detection. A number of challenges potentially accounted for error in our measurements, such as variations in biological tissue, including less-homogenous composition, uneven surfaces, changes through measurements, and aging. In the THz system, the curvature of the imaging window, irregular connection with the sample, and multiple reflections of THz pulses were also potential sources of error. For these reasons, mathematical operations, such as peak intensity and peak to peak intensity, were selected to obtain THz images based on the time-frequency domain (Ballacey et al., 2016). Processing thus determined the intensity level of each pixel in the image, to ensure that the THz images would provide accurate data on the amplitude of the THz signal reflected from the fresh tissue in various positions, over a range of frequencies, as shown in Figure 4a.

2.4 Data processing

Data processing was applied to the THz images and the optical properties of the samples. This involved removing background noise by averaging each pixel signal. These signals were then isolated from the dataset, using a zero-padding algorithm to improve the second peak interface of the remaining signal (Fan et al., 2016). The information related to the application of the time domain in the fast Fourier transform process (FFT) was converted to the frequency domain. Analytical data were processed using MATLAB code.

3. Results

Different THz images of the 0.2 mm-thick fresh tissue samples on a sapphire window, recorded at 0.8 THz in reflection mode, were obtained by automatic processing, using mathematical operations in both time and frequency domains, and distinguished between cancerous (abnormal) and fatty (healthy) regions, see Figure 3. The imaging results

DOI: https://doi.org/10.22452/mjs.sp2022no1.3

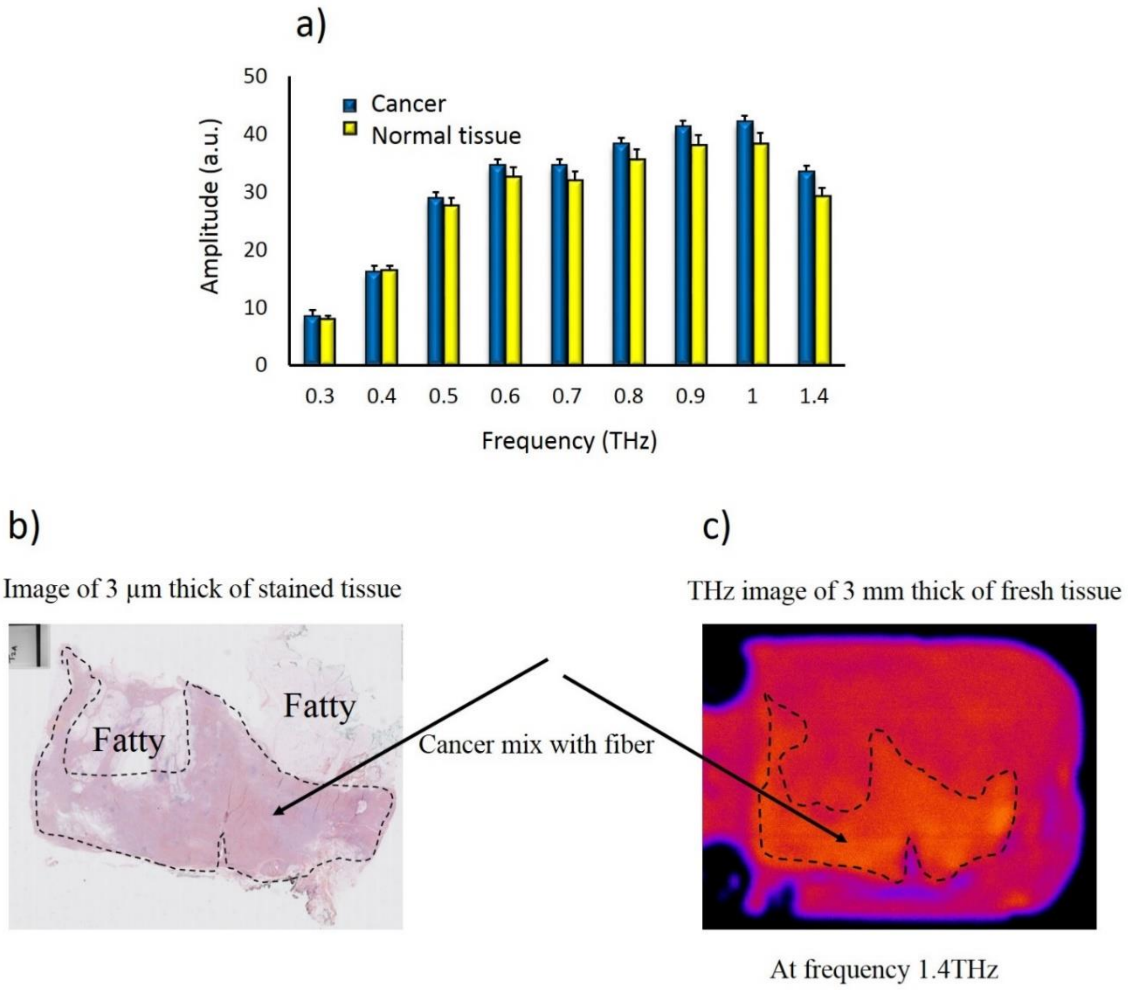


Figure 4. a) Absorption coefficients of infected (cancerous) and healthy tissue, b) Image of a 3 micrometer-thick stained tissue sample, c) image of a 3 millimeter-thick sample of the same tissue at a frequency of 1.4 THz.

varied depending on the different mathematical operations, but this method provided rapid identification of cancer tissues compared with standard clinical reports. Tumors were clearly delineated in the THz images in the frequency and time domain, compared with histopathology images, showing the distribution of cancer cells within the fatty regions. Additionally, good agreement was observed between fatty and cancer tissue in both techniques. The variation in image contrast in the time-frequency domain may be explained by differences in biological composition between fat and cancer tissues.

Figure 4 (b & c) shows the close match between the 1.4 THz image and that of the 3 µm-thick tissue sample embedded in a paraffin block, where the infected region shows more variation than the healthy region. In terms of physical analysis, the results confirmed that identification of the cancer region was more effective than the healthy region, as shown in Figure 4a, comparing the average amplitude of tumors and normal tissue. Significant differences in amplitude were clearly observed at frequencies ranging from 0.2 to 1.4 THz. Figure 4a illustrates the behavior of THz pulses progressing through each region of fresh breast tissue.

The average values for tumors and healthy tissues at 1 THz were 44.6 (a.u.) ± 0.23 and 40.3 ± 0.20, respectively. Thus, the fatty tissue exhibited less frequency-dependent amplitude, which may explain the increased THz reflection pulses on the THz detector, while the cancer tissue exhibited higher amplitude. In addition, Figure 4a shows that amplitudes for the normal and cancer tissues decreased at 1.4 THz, possibly suggesting that the THz signals reflected from the sample fell to the noise floor. Different regions of the sample are clearly distinguished and there was good correspondence between the THz images and histopathology slides.

The THz data was processed to extract refractive indices, absorption coefficients and averages of biological tissues from different regions, as reported in Table 1. The results revealed that, in the 0.3- 0.5 THz range, the optical properties (refractive indices and absorption coefficients) of normal tissue were lower than those of abnormal tissue (cancer). In addition, the dielectric properties of normal and

DOI: https://doi.org/10.22452/mjs.sp2022no1.3

Table 1. Parameters of water by the Double Debye model and measured data in the 0.3 to over 0.5 THz range. (RI, α, σ and ε) are the refractive index, absorption coefficient, conductivity, and permittivity of water and human tissue, respectively.

Material	0.3 THz				0.4 THz				0.5 THz			
	RI	α	σ	ε	RI	α	σ	ε	RI	α	σ	ε
Water-Debye model	2.7	103	4.3	6.5	2.6	118	4	6.3	2.5	136	3.2	6
Water from our measurements	2.9	129	5.8	8.6	2.7	149	5	7.7	2.6	170	4.2	6.9
Abnormal tissue	2.6±4. 9%	99±5%	4. 9	7.3	2.5±4. 8%	107±5. 4%	3.3	6.7	2.4±4. 7%	128±6%	3	6.1
Normal tissue	2.4±1. 7%	75±1. 2%	3	6.3	2.3±1. 6%	91±1. 5%	2.7	5.8	2.2±1. 5%	109±3. 3%	2.4	5.4

abnormal tissues were calculated using a Debye double-relaxation model (Pashkin et al., 2003). Furthermore, a water reference was measured before the tissue samples were processed to correct variations in data extraction using Equation 1. A detailed description of the extraction of the refractive index and absorption coefficient is given in the article cited (Pashkin et al., 2003):

$$\mathcal{E}_c = \mathcal{E}_\infty + \frac{\mathcal{E}_s - \mathcal{E}_1}{1+iwt_D} + \frac{\mathcal{E}_1 - \mathcal{E}_\infty}{1+iwt_2} \qquad (1)$$

Where ε_c is the dielectric function, $\varepsilon_{\square}$ *is* the dielectric constant at high frequencies, ε_s is the static dielectric constant, ε_1 is the dielectric function of the long and fast relaxation process, occurring over τ_1 and τ_2, respectively, at pulsation ω. These results indicated that the dielectric properties (conductivity ($\boldsymbol{\sigma}$) and permittivity ($\boldsymbol{\varepsilon}$)) (Joyce et al., 2016) of normal tissue were lower than those of abnormal tissue. The refractive index $\mathbf{n(\omega)}$ and absorption coefficient $\boldsymbol{\alpha(\omega)}$ of the sample were calculated using the equation.

For data analysis, the frequency-dependent absorption coefficient and refractive index were obtained using equations 2 and 2, respectively, giving values of $\alpha_{sample,}$ and n_{sample}. A detailed description of the extraction of the refractive index and absorption coefficient is given in the article cited (Fan et al., 2016).

$$\boldsymbol{n_s = real\left(\tilde{n}_s(\omega)\right)} \qquad (2)$$

$$\boldsymbol{\alpha_s = \frac{2\omega\,.k(\omega))}{c}} \qquad (3)$$

These results showed that the optical properties of fresh tissue, especially the refractive index (RI) and absorption coefficients (α), measured ex- vivo by spectral analysis in the 0.3-0.5 THz range, were systematically higher in tumors than in healthy tissue. In addition, the measured complex dielectric properties of the tissues increased, so we compared the conductivity and permittivity of abnormal and normal tissue with those of water. Consequently, the interaction of THz radiation with fresh tissue provided valuable information for quantifying the dielectric properties of breast tissue in the THz range. Moreover, the measured dielectric properties of the different breast tissues differed from the extracted data, depending on their optical properties. The significant difference between normal breast and cancerous tissue revealed that analysis of THz reflection parameters had the potential to differentiate between tumors and healthy tissues. Details of these THz properties are presented with average values and standard errors in Table 1. In conclusion, THz reflection spectroscopy is capable of measuring the dielectric coefficients of tumor and healthy tissue, and differentiating between them, due to their different structures. In addition, the identification of cancerous and healthy tissue in each sample was verified by a histopathologist, who provided information on the tissue types for evaluating the accuracy of the reflected THz spectroscopy measurements.

5. Conclusions

A comparison of terahertz radiation imaging with classic, slide-based tissue samples confirmed that this technique has the potential to provide reliable detection of cancer tumors. The accuracy of the THz technique varied among the different types of complex excised breast tissues and substrate materials used in this study, possibly due to scattering effects or the interaction of THz radiation with samples and substrates, as shown in Figure 3.

6. References

Al-Ibadi, A., Cassar, Q., Zimmer, T., MacGrogan, G., Mavarani, L., Hillger, P., Grzyb, J., Pfeiffer, U. R., Guillet, J. P., & Mounaix, P. (2017). THz spectroscopy and imaging for breast cancer detection in the 300-500 GHz range.

International Conference on Infrared, Millimeter, and Terahertz Waves, IRMMW-THz, *Spp 1857*, 1–1. https://doi.org/10.1109/IRMMW-THz.2017.8067037

Ballacey, H., Al-Ibadi, A., Macgrogan, G., Guillet, J. P., Macpherson, E., & Mounaix, P. (2016). Automated data and image processing for biomedical sample analysis. *International Conference on Infrared, Millimeter, and Terahertz Waves, IRMMW-THz*, *2016-Novem*, 2–3. https://doi.org/10.1109/IRMMW-THz.2016.7758882

Cassar, Q., Al-Ibadi, A., Mavarani, L., Hillger, P., Grzyb, J., MacGrogan, G., Zimmer, T., Pfeiffer, U. R., Guillet, J.-P., & Mounaix, P. (2018). Pilot study of freshly excised breast tissue response in the 300 – 600 GHz range. *Biomedical Optics Express*, *9*(7), 2930. https://doi.org/10.1364/boe.9.002930

El-Shenawee, M., Vohra, N., Bowman, T., & Bailey, K. (2019). Cancer detection in excised breast tumors using terahertz imaging and spectroscopy. *Biomedical Spectroscopy and Imaging*, *8*(1–2), 1–9. https://doi.org/10.3233/bsi-190187

Fan, S., He, Y., Ung, B. S., & Pickwell-Macpherson, E. (2014). The growth of biomedical terahertz research. *Journal of Physics D: Applied Physics*, *47*(37). https://doi.org/10.1088/0022-3727/47/37/374009

Fan, S., Parrott, E. P. J., Ung, B. S. Y., & Pickwell-MacPherson, E. (2016). Calibration method to improve the accuracy of THz imaging and spectroscopy in reflection geometry. *Photonics Research*, *4*(3), A29. https://doi.org/10.1364/prj.4.000a29

Gong, A., Qiu, Y., Chen, X., Zhao, Z., Xia, L., & Shao, Y. (2020). Biomedical applications of terahertz technology. *Applied Spectroscopy Reviews*, *55*(5), 418–438. https://doi.org/10.1080/05704928.2019.1670202

Hejmadi, M. (2010). Introduction to Cancer Biology. In *Expert Opinion on Pharmacotherapy* (2nd editio, Vol. 2, Issue 4). https://doi.org/10.1517/14656566.2.4.613

Joyce, H. J., Boland, J. L., Davies, C. L., Baig, S. A., & Johnston, M. B. (2016). A review of the electrical properties of semiconductor nanowires: Insights gained from terahertz conductivity spectroscopy. *Semiconductor Science and Technology*, *31*(10). https://doi.org/10.1088/0268-1242/31/10/103003

Pashkin, A., Kempa, M., Němec, H., Kadlec, F., & Kužel, P. (2003). Phase-sensitive time-domain terahertz reflection spectroscopy. *Review of Scientific Instruments*, *74*(11), 4711–4717. https://doi.org/10.1063/1.1614878

Peter, B. S., Yngvesson, S., Siqueira, P., Kelly, P., Khan, A., Glick, S., & Karellas, A. (2013). Development and testing of a single frequency terahertz imaging system for breast cancer detection. *IEEE Transactions on Terahertz Science and Technology*, *3*(4), 374–386. https://doi.org/10.1109/TTHZ.2013.2241429

Sun, K., Tordjman, J., Clément, K., & Scherer, P. E. (2013). Fibrosis and adipose tissue dysfunction. *Cell Metabolism*, *18*(4), 470–477. https://doi.org/10.1016/j.cmet.2013.06.016

Wahaia, F., Kašalynas, I., Minkevičius, L., Carvalho Silva, C. D., Urbanowicz, A., & Valušis, G. (2020). Terahertz spectroscopy and imaging for gastric cancer diagnosis. *Journal of Spectral Imaging*, *9*, 1–8. https://doi.org/10.1255/jsi.2020.a2

Wang, Y., Chen, D., Qian, H., Tsai, Y. S., Shao, S., Liu, Q., Dominguez, D., & Wang, Z. (2014). The Splicing Factor RBM4 Controls Apoptosis , Proliferation , and Migration to Suppress Tumor Progression. *Cancer Cell*, *26*(3), 374–389. https://doi.org/10.1016/j.ccr.2014.07.010

WHO. (2017). Guide to Cancer - Guide to cancer early diagnosis. In *World Health Organization*. https://apps.who.int/iris/bitstream/handle/10665/254500/9789241511940-eng.pdf;jsessionid=2646A3E30075DB0FCA4A703A481A5494?sequence=1

Wilmink, G. J., & Grundt, J. E. (2011). Invited Review Article : Current State of Research on Biological Effects of Terahertz Radiation. *J Infrared Milli Terahz Waves*, *32*, 1074–1122. https://doi.org/10.1007/s10762-011-9794-5

Yu, C., Fan, S., Sun, Y., & Pickwell-Macpherson, E. (2012). The potential of terahertz imaging for cancer diagnosis: A review of investigations to date. *Quantitative Imaging in Medicine and Surgery*, *2*(1), 33–45. https://doi.org/10.3978/j.issn.2223-4292.2012.01.04

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021 Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 23-33 (September 2022) https://mjs.um.edu.my

GROUP DIAGNOSTIC MEASURES OF DIFFERENT TYPES OF OUTLIERS IN MULTIPLE LINEAR REGRESSION MODEL

Hassan S. Uraibi [1a*] and Sawsan Abdul Ameer Haraj [2a]

Abstract: The topic of detection outliers is one of the crucial topics that have been of interest to researchers in many scientific fields. The presence of outliers in the dataset may lead to the breakdown of the estimator of the method in use. The statistical literature has shown that several types of outliers occur according to the type and nature of the data. Therefore, the researchers concentrated on identifying the type of outliers of statistical models by using two diagnostic procedures, individual and grouped. Unfortunately, the first procedure neglects the effect of the phenomenon of (masking and swamping). In contrast, the second procedure has not been able to eliminate this phenomenon ideally but rather reduce the rates of its appearance. This paper seeks to suggest improving one of the well-known group diagnostic methods (DRGP) by using an RMVN location and scale matrix instead of MVE to reduce the effect of (swamping). A newly proposed method denoted as DRGP(RMVN) is tested with a simulation study and real data. The results have shown that the performance of our proposed method is more efficient than (DRGP.MVE) to reduce the swamping points.

Keywords*: Masking, Swamping, Leverage Point, DRGP and RMVN*

1. Introduction

The topic of outlier detection in the samples data taken out of its statistical populations was not a topic that interested researchers in diverse scientific fields until the sixties of the last century. It also was a reason that statistical schools were divided into two schools, classical and robust. The classical school sticks to the theoretical basis to assume the normal distribution of sample data drawn randomly from its statistical population (Uraibi and Alhussieny, 2021). On the other hand, the founder Gauss had put a particular hypothesis that randomly chosen observations from its statistical population are independent and identically distributed (Huber, 1981). Most of the researchers found that one of the most important reasons behind the deviation of the specific distribution hypothesis is the presence of outliers, so it is of importance in the place of diagnosing these values that are considered far away from the centre of the gathering bulk of data (Hample et al., 1986). Apart from that, Rousseuw and Zomeren (1990) defined the outliers as being observations that lie away from most of the remaining data, which constitutes (1%) to (10%) out of any group of data in our natural world. Recently, a group of researchers showed that this ratio could be raised to more than (25%) and less than (50%), but it is inevitable even if this data is of high quality (Uraibi and Alhussieny, 2021).

Moreover, Huber (1981) pointed out that the presence of one outlier at least in the data group leads to the breakdown of the statistical estimator. Great efforts were made in the statistical literature to identify all the outliers in linear regression, such as single diagnostic methods (see, Rousseeuw and Leroy, 1987). Unfortunately, those methods did not take into consideration the phenomenon of masking and swamping, which leads to their being unable to detect all types of outliers (Vertical Outliers (VO) and High Leverage Point (HLP)) accurately in the data set. The single diagnostic conceals in its folds the wrong diagnosis when its methods detect one or more than one observation as outliers, but it's not. This phenomenon is called (swamping) (see, Maroona and Yohai, 2006).

On the other hand, may these methods suffer from the masking phenomenon in which the detected outliers probably overshadow other outliers. Therefore, the particular diagnostic method could not detect the outliers masked by other outliers (Rousseuw and Zomeren,1990). Consequently, Imon (2002) introduced a group deleted measure as a Generalize Potential (GP) measure to eliminate the effect of masking and swamping. However, Midi et al. (2009) found out that GP could not identify the exact number of leverage points and still suffer from the effect of masking and swamping. Therefore, they proposed utilizing Minimum Volume Ellipsoid (MVE) (Rousseeuw, 1984) to build a new algorithm which is a so-called Diagnostic Robust Generalized

Authors information:
[a]Department of Statistics, College of Administration and Economics, University of Al-Qadisiya, IRAQ. E-mail: hassan.uraibi@qu.edu.iq[1], stat.post22@qu.edu.iq[2]

*Corresponding Author: hassan.uraibi@qu.edu.iq

Received: January 22, 2022
Accepted: July 15, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

Potential measure (DRGP). The target of an algorithm is to the sake of accurate diagnostic and reducing the effect of masking and swamping. We noted that DRGP based on MVE (DRGP.MVE) may tackle the problem of identifying the exact number of leverage points. Still, it is not adequately effective in reducing the number of masking and swamping or getting rid of its effects.

Olive and Hawkins (2010) introduced Reweighted MultiVraite Normal (RMVN) as a robust, fast, and consistent concentration algorithm to produce a robust location and scale estimator. Due to these aspects, RMVN is more relevant to DRGP than MVE. On the other hand, it is well known that DRGP.MVE algorithm relies on Robust Mahanalobis Distance (RMD) that is integrated with MVE estimators, see (Uraibi and Midi;2009). In this paper, a slight development to the DRGP is proposed, and we call it DRGP.RMVN by incorporating RMVN with RMD instead of MVE. This paper is organized to present the DRGP(MVE) measure in Section 2. Meanwhile, Section 3 describes the DRGP(RMVN) method. Lastly, Section 4 and Section 5 illustrate simulation study and numerical examples to assess the performance of the DRGP(RMVN) method.

2. DRGP Measure

The idea of this method essentially relies on the first step in which a robust-generalized diagnostics procedure for HLP by using MD is employed with MVE location and scatter estimators. Then, the GP algorithm proposed by Imon (2002) is utilized. Suppose that $\boldsymbol{X}$ is a matrix of multivariate random varaibles. The algorithm of DRGP.MVE can be described as follows:

1. Computing the location $\widehat{\boldsymbol{\mu}}$ and scale $\boldsymbol{C_{MVE}(X)}$ estimators of MVE, denoted as.
2. Finding the mahalanobis distance $(\boldsymbol{MD})$ using Eq. (1) if the $\boldsymbol{i^{th}}$ $\boldsymbol{MD}$ $\boldsymbol{(MVE)} > \sqrt{\chi^2_{(p,0.95)}}$. Then. the $\boldsymbol{i^{th}}$ row has the suspected observations as HLP.
$$\boldsymbol{RMD_i(MVE)} = \sqrt{[\boldsymbol{X}-\widehat{\boldsymbol{\mu}}(\boldsymbol{X})]'[\boldsymbol{C_{MVE}(X)}]^{-1}[\boldsymbol{X}-\widehat{\boldsymbol{\mu}}(\boldsymbol{X})]}\ \ \boldsymbol{i} = \mathbf{1,2,\ldots,}\boldsymbol{n} \quad (\mathbf{1})$$
3. The rows are determined including HLPs, which are deleted from the design matrix $\boldsymbol{X}$ and placed as a new submatrix denoted as $\boldsymbol{X_D}$. The remaining rows that have only clean observations will be substituted as $\boldsymbol{X_R}$ matrix. In other word, $\mathbf{R}$ and $\mathbf{D}$ are sets of any arbitrary remaining and deleted cases, respectively. Hence, R consist of $(\boldsymbol{n}-\boldsymbol{d})$ cases after $\boldsymbol{d}$ cases in $\mathbf{D}$ are deleted, where $\boldsymbol{d} < (\boldsymbol{n}-\boldsymbol{p})$, $\boldsymbol{n}$ is the sample size and $\boldsymbol{p}$ is the number of variables.
4. Habshah et al. (2009) pointed out without loss of generality, those observations are assumed to be the last of d rows of X, such that the weight matrix, $\boldsymbol{H} = \boldsymbol{X}(\boldsymbol{X^t X})^{-1}\boldsymbol{X^t}$ can be decomposed as follows:
$$\mathbf{w} = \begin{bmatrix} \mathbf{U_R} & \mathbf{V} \\ \mathbf{V}' & \mathbf{U_D} \end{bmatrix},$$
where $\boldsymbol{U}_{\mathbf{R}} = \boldsymbol{X}_{\mathbf{R}}\left(\boldsymbol{X'X}\right)^{-1}\boldsymbol{X}'_{\mathbf{R}}$, $\mathbf{U_D} = \boldsymbol{X}_{\mathbf{D}}\left(\boldsymbol{X'X}\right)^{-1}\boldsymbol{X}'_{\mathbf{D}}$, are symmetric matrices of $(\boldsymbol{n}-\boldsymbol{d})$ and $\boldsymbol{d}$ cases, respectively, and $\boldsymbol{V} = \boldsymbol{X_R}\left(\boldsymbol{X'X}\right)^{-1}\boldsymbol{X}'_{\mathbf{D}}$ be an $(\boldsymbol{n}-\boldsymbol{d}) \times \boldsymbol{d}$ matrix.

When a group of observations $\mathbf{D}$ is omitted, the $\boldsymbol{W_{ii}^{(-\mathbf{D})}} = \boldsymbol{X}'_{\boldsymbol{i}}\left(\boldsymbol{X}'_{\boldsymbol{R}}\boldsymbol{X_R}\right)^{-1}\boldsymbol{X_i}$. Deletion the $\boldsymbol{i^{th}}$ diagonal element where $\mathbf{D} = \boldsymbol{i}$ result in $\boldsymbol{W_{ii}^{(-i)}} = \boldsymbol{X}'_{\boldsymbol{i}}\left(\boldsymbol{X}'_{(\boldsymbol{i})}\boldsymbol{X}_{(\boldsymbol{i})}\right)^{-1}\boldsymbol{X_i}$, which is a single diagnostic procedure equivalent to Hadi potential measure.

Finally, the group deletion measure based on MVE can be written as follows,

$$\boldsymbol{P}_{\mathbf{ii}} = \begin{cases} \boldsymbol{W}_{\mathbf{ii}}^{(-\mathbf{D})} & \forall \mathbf{i} \in \mathbf{D}, \\ \dfrac{\boldsymbol{W}_{\mathbf{ii}}^{(-\mathbf{D})}}{\mathbf{1}-\boldsymbol{W}_{\mathbf{ii}}^{(-\mathbf{D})}} & \forall \mathbf{i} \in \mathbf{R}. \end{cases}$$

Moreover, when $\boldsymbol{P}_{\mathbf{ii}} > \boldsymbol{median}(\boldsymbol{P}_{\mathbf{ii}}) + \boldsymbol{cMAD}(\boldsymbol{P}_{\mathbf{ii}})$, it is confirmed the $\boldsymbol{i^{th}}$ row has an HLP.

2.1 The DRGP(RMVN) Measure

The contribution of the suggested method is to incorporate the Reweighted Multivariate Normal estimators (RMVN) instead of (MVE) estimators within the DRGP algorithm. For example, Olive and Hawkins (2010) proposed the RMVN method to reweight multivariate standard estimators using a fast and consistent algorithm with a high breakdown point. In the first two stages, the estimators of two locations and scale have been computed, which are the DGK (Devlin et al., 1981) and Median Ball (MD) (Olive,2004). The DGK and MB are fast concentration algorithms that could converge during 5 to 10-steps.

Suppose that $(\boldsymbol{T}_{\mathbf{5},\boldsymbol{DGK}}, \boldsymbol{C}_{\mathbf{5},\boldsymbol{DGK}})$ are the DGK estimators and $(\boldsymbol{T}_{\mathbf{5},\boldsymbol{MB}}, \boldsymbol{C}_{\mathbf{5},\boldsymbol{MB}})$ are the MB estimators, then the Fast Consistence and Hgih breakdown (FCH) location and scale estimators can be obtained by

$$\boldsymbol{T_{FCH}} = \left\{\begin{matrix} \boldsymbol{T}_{\mathbf{5},\boldsymbol{DGK}} & \boldsymbol{if}\sqrt{|\boldsymbol{C}_{\mathbf{5},\boldsymbol{DGK}}|} < \sqrt{|\boldsymbol{C}_{\mathbf{5},\boldsymbol{MB}}|} \\ \boldsymbol{T}_{\mathbf{5},\boldsymbol{MB}} & \boldsymbol{Otherwise} \end{matrix}\right\},$$

and

$$\boldsymbol{C_{FCH}} = \left\{\begin{matrix} \dfrac{\boldsymbol{MED}\left(\boldsymbol{MD}_i^2\left((\boldsymbol{T}_{\mathbf{5},\boldsymbol{DGK}}, \boldsymbol{C}_{\mathbf{5},\boldsymbol{DGK}})\right)\right)}{\chi^2_{(\boldsymbol{p},\mathbf{0.5})}} \times \boldsymbol{C}_{\mathbf{5},\boldsymbol{DGK}}, & \boldsymbol{if}\sqrt{|\boldsymbol{C}_{\mathbf{5},\boldsymbol{DGK}}|} < \sqrt{|\boldsymbol{C}_{\mathbf{5},\boldsymbol{MB}}|} \\ \dfrac{\boldsymbol{MED}\left(\boldsymbol{MD}_i^2\left((\boldsymbol{T}_{\mathbf{5},\boldsymbol{MB}}, \boldsymbol{C}_{\mathbf{5},\boldsymbol{MB}})\right)\right)}{\chi^2_{(\boldsymbol{p},\mathbf{0.5})}} \times \boldsymbol{C}_{\mathbf{5},\boldsymbol{MB}} & \mathbf{Otherwise} \end{matrix}\right\}$$

where |■| stands for the determinant of scale matrix while $\boldsymbol{MD}$ is the traditional Mahalanobis Distance.

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

Let $(\widehat{T}_1, \widehat{C}_1)$ be the traditional estimator applied to n_1 cases with $MD_i^2[(\ \mathrm{T_{FCH}}, \mathrm{C_{FCH}})\ ] \leq \chi^2_{(p,0.975)}$, and let $q_1 = min\left\{\frac{(0.5\times0.975\times n)}{n_1}, 0.995\right\}$

Thus, the first standard reweighting of MVN data is given by

$$C^{(1)}_{RMVN} = \frac{MED\left(D_i^2(T_{FCH},\ C_{FCH})\right)}{\chi^2_{(p,q_1)}} \times C_{FCH}.$$

The new estimators $(T_{FCH}, C^{(1)}_{RMVN})$ are applied to n_2 case with

$$MD_i^2\left[(\ T_{FCH}, C^{(1)}_{RMVN})\ \right] \leq \chi^2_{(p,0.975)}.$$

Let $q_2 = min\left\{\frac{(0.5\times0.975\times n)}{n_2}, 0.995\right\}$, then the RMVN estimator can be found as follows

$$C^{(2)}_{RMVN} = \frac{MED\left(D_i^2\left(T_{RMVN}, C^{(1)}_{RMVN}\right)\right)}{\chi^2_{(p,q_2)}} \times C^{(1)}_{RMVN}.$$

The algorithm of DRGP (RMVN) measure can be summarized as follows

1. Computing the location T_{RMVN} and scale $C^{(2)}_{RMVN}$ estimators.
2. Calculating Mahalanobis Distance (MD) using Eq. (2). If the i^{th} $MD_i(RMVN) > \sqrt{\chi^2_{(p,0.95)}}$, then the i^{th} row has the suspected observations as HLP, given by

$$MD_i(RMVN) = \sqrt{(X - T_{RMVN}(X))' {C^{(2)}_{RMVN}}^{-1'} (X - T_{RMVN}(X))}\ .$$

3. The deletion of D rows from the matrix X of the original data where

$$D = MD\left\{(RMVN) > \sqrt{\chi^2_{(p,0.95)}}\right\}$$

   is the row's index by placing the deletion rows in X_D matrix, while the remaining rows will be in X_R matrix.
4. The last step is similar to step 4 in DRGP(MVE).

3. Simulation Study

Let's suppose the multiple linear regression be as follows:

$$y = X\beta + e, \qquad (2)$$

where X is $n \times p$ design matrix generated from a multivariate normal distribution with mean equals to zero and standard deviation equivalent to $\sigma = \rho^{|i-j|}$, implying $x \sim N(0, \rho^{|i-j|})$. Here, $p = 7$, n is the generated sample that will take a different number of observations, $n = \{45, 70, 90, 140\}$, β is the identity vector of this model

$$\beta = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}_{7x1}, \qquad (3)$$

and e is a random error term that is distributed generally with zero mean and two standard deviations. To make sure of the diagnosis efficient of comparative methods, we contaminate the simulated data with different proportions of outliers, $\alpha = (0.05, 0.10)$ as follows:

1- Contaminating the design matrix of each sample by α BLP in the presence of one HLP. By multiplying the first three rows of the second variable to the fifth variable by the number 10, multiplying the maximum value of the first variable by the number 10, and what corresponds to it in the response variable Y.

2- Contaminating both design matrix and random errors α BLP & Vertical Outliers (VO) in the presence of one HLP. The VOs are generated from a chi-square distribution with (10) degree freedom.

The main reason for including a single HLP in all cases of the simulation study is to consider the phenomenon of masking and swamping. Let λ_i be a random variable, where $i = 1, 2, \dots, n$, $O = \{\lambda_1, \dots, \lambda_\delta\}$ be the outlying observations, such that $(\delta = \alpha \times n)$, and α is the percentage of outlying observations, respectively. The clean observations would be $C = \{\lambda_{\delta+1}, \dots, \lambda_n\}$. Suppose that $\mathbf{E}_j$ is the total outlying cases detected by a specific diagnostic method, where $1 \leq j \leq \delta^*$, δ^* is then either $(\delta + b)$ or $(+b)$, such that h and b are integer numbers, $[0 \leq b < n]$ and $[0 \leq h < \delta]$. Consequently, $\lambda_b \in C$ and $\lambda_h \in O$ and we can conclude that the exact detection will happen when $(\delta^* = \delta)$ in which no swamping cases $(b = 0)$ nor masking issues $(h = 0)$ will occur. However, the particular method would have swapping cases where $(\delta^* > \delta)$ and masking where $(\delta < \delta - h)$. The performance of our proposed method is compared with another overall (1000) dataset for each simulation case. The best diagnostic method is the one that has an average of correct diagnostic closer to δ (accurate), a lower standard of b (swap).

Tables 1,2 and 3 display the results of the Hat matrix, RMD, Hadi's poteintial, DRGP.MVE and DRGP.RMVN when α={0.05,0.10,0.15 } for overall 5000 datasets are generated with two types of contamination and different samples size n={35,45,70,90,140}. The average of of $(\mathbf{E}$, correct and swap) which are the number of outlying cases (Leverage points) that identified by competiting methods, the correct number of outlying cases and the number of swamping cases, respectively. For instance, when $(n = 35, \alpha = 0.05)$, the generated dataset should be having two LP, and probably a high LP that is generated randomly be either good or bad. If it is good high LP almost should be one of two leverage points, otherwise, the total number of LP will be three. This

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

Table 1. Averages of the **correct** and **swap** diagnosis, respectively, for three cases of simulation when $\alpha = 0.05$ and different sample sizes.

			Hat	**RMD**	**Hadi**	**DRGP(MVE)**	**DRGP(RMVN)**
35	**LP**	E	11.4682	9.964	4.9952	4.2268	4.1232
		correct	2.9428	2.9428	2.9428	2.9428	2.9428
		swap	8.5254	7.0212	2.0524	1.284	1.1804
	LP & VO	E	11.4436	9.9408	5.396	4.282	4.1192
		correct	2.943	2.943	2.943	2.943	2.943
		swap	8.5006	6.9978	2.453	1.339	1.1762
45	**LP**	E	10.42	9.13	6.68	5.11	4.92
		correct	3.94	3.94	3.94	3.94	3.94
		swap	6.48	5.19	2.74	1.17	0.98
	LP & VO	E	10.41	9.18	7.27	5.05	4.98
		correct	3.93	3.93	3.93	3.93	3.93
		swap	6.48	5.25	3.34	1.12	1.05
70	**LP**	E	10.202	9.155	9.856	6.29	6.262
		correct	4.941	4.214	4.935	4.942	4.942
		swap	5.261	4.941	4.921	1.348	1.32
	LP & VO	E	10.234	9.218	10.49	6.217	6.159
		correct	4.939	4.939	4.93	4.94	4.94
		swap	5.295	4.279	5.56	1.277	1.219
90	**LP**	E	11.58	10.47	12.51	7.48	7.49
		correct	5.94	5.93	5.85	5.94	5.94
		swap	5.64	4.53	6.67	1.54	1.55
	LP & VO	E	11.54	10.53	13.21	7.46	7.49
		correct	5.95	5.95	5.88	5.95	5.95
		swap	5.60	4.58	7.33	1.51	1.54
140	**LP**	E	16.087	14.614	18.303	10.134	0.163
		correct	7.938	7.938	7.698	7.948	7.948
		swap	8.149	6.676	10.605	2.186	2.215
	LP & VO	E	16.034	14.547	19.332	10.033	10.041
		correct	7.93	7.926	7.773	7.945	7.945
		swap	8.104	6.621	11.559	2.088	2.096

Table 2. Averages of the **correct** and **swap** diagnosis, respectively, for three cases of simulation when $\alpha = 0.1$ and different sample sizes.

			Hat	**RMD**	**Hadi**	**DRGP(MVE)**	**DRGP(RMVN)**
35	**LP**	E	7.83	7.193	6.646	5.811	5.623
		correct	4.865	4.865	4.838	4.865	4.865
		swap	2.965	2.328	1.808	0.946	0.758
	LP & VO	E	7.771	7.166	7.24	5.719	5.648
		correct	4.884	4.883	4.853	4.886	4.886
		swap	2.887	2.283	2.387	0.833	0.762
45	**LP**	E	8.837	8.208	7.945	6.683	6.547
		correct	5.878	5.874	5.553	5.895	5.895
		swap	2.959	2.334	2.392	0.788	0.652
	LP & VO	E	8.857	8.172	8.911	6.682	6.606
		correct	5.87	5.868	5.627	5.886	5.886
		swap	2.987	2.304	3.284	0.796	0.72
70	**LP**	E	11.9668	11.1538	10.96	8.7822	8.7544
		correct	7.8528	7.8432	6.9832	7.9048	7.9048
		swap	4.114	3.3106	3.9768	0.8774	0.8496
	LP & VO	E	11.99	11.1872	12.515	8.746	8.7206
		correct	7.8606	7.8518	7.1938	7.907	7.907
		swap	4.1294	3.3354	5.3212	0.839	0.8136
90	**LP**	E	14.9222	13.9716	13.5374	10.8636	10.8602
		correct	9.8176	9.8018	8.3428	9.9016	9.9016
		swap	5.1046	4.1698	5.1946	0.962	0.9586
	LP & VO	E	14.9008	13.919	15.569	10.8842	10.8764
		correct	9.8174	9.7996	8.6946	9.8984	9.8984
		swap	5.0834	4.1194	6.8744	0.9858	0.978
140	**LP**	E	22.3434	20.9508	19.8194	16.2092	16.2104
		correct	14.7168	14.6814	11.6562	14.8992	14.8992
		swap	7.6266	6.2694	8.1632	1.31	1.3112
	LP & VO	E	22.3826	20.9838	19.8032	16.2218	16.23
		correct	14.7156	14.6826	11.6198	14.901	14.901
		swap	7.667	6.3012	8.1834	1.3208	1.329

Table 3. Averages of the **correct** and **swap** diagnosis, respectively, for three cases of simulation when $\alpha = 0.15$ and different sample sizes.

			Hat	RMD	Hadi	DRGP(MVE)	DRGP(RMVN)
35	**LP**	E	9.086	8.5024	6.6246	7.3208	7.2726
		correct	6.75	6.73	5.3072	6.832	6.832
		swap	2.336	1.7724	1.3174	0.4888	0.4406
	LP & VO	E	9.1104	8.5514	7.2782	7.285	7.2544
		correct	6.7526	6.7288	5.4162	6.832	6.832
		swap	2.3578	1.8226	1.862	0.453	0.4224
45	**LP**	E	10.4724	9.8478	7.8152	8.3042	8.2728
		correct	7.7378	7.713	5.9242	7.8452	7.8452
		swap	2.7346	2.1348	1.891	0.459	0.4276
	LP & VO	E	10.497	9.8884	8.8176	8.339	8.2986
		correct	7.7394	7.7162	6.0872	7.8412	7.8412
		swap	2.7576	2.1722	2.7304	0.4978	0.4574
70	**LP**	E	15.3946	14.5858	10.2204	12.3012	12.3036
		correct	11.5568	11.4976	7.2486	11.8536	11.8536
		swap	3.8378	3.0882	2.9718	0.450	0.450
	LP & VO	E	15.3966	14.5954	12.2674	12.3214	12.3102
		correct	11.5374	11.4888	7.789	11.8376	11.8376
		swap	3.8592	3.1066	4.4784	0.4838	0.4726
90	**LP**	E	19.1892	18.2664	12.2388	15.357	15.352
		correct	14.4146	14.3474	8.408	14.8388	14.8388
		swap	4.7746	3.919	3.8308	0.5182	0.5132
	LP & VO	E	19.1708	18.2016	15.1412	15.3638	15.361
		correct	14.4296	14.353	9.2282	14.8454	14.8454
		swap	4.7412	3.8486	5.913	0.5184	0.5156
140	**LP**	E	28.4406	27.054	17.7994	22.593	22.5958
		correct	21.19	21.0848	11.4674	21.851	21.851
		swap	7.2506	5.9692	6.332	0.742	0.7448
	LP & VO	E	28.4262	27.0326	22.6872	22.5732	22.577
		correct	21.1834	21.0786	13.0092	21.8482	21.8482
		swap	7.2428	5.954	9.678	0.725	0.7288

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

procedure has been done for all simulation scenarios. Each table has the results of both diagnostics single detection and group diagnostic methods. Therefore, the discussion of results would be taken the performance of single diagnostic methods first and then the dicussion the results of group diagnostic has been considered with some details.

Tables 1,2 and 3 display the results of the Hat matrix, RMD, Hadi's poteintial, DRGP.MVE and DRGP.RMVN when α={0.05,0.10,0.15 } for overall 5000 datasets are generated with two types of contamination and different samples size n={35,45,70,90,140}. The average of of ($\mathbf{E}$, correct and swap) which are the number of outlying cases (Leverage points) that identified by competiting methods, the correct number of outlying cases and the number of swamping cases, respectively. For instance, when ($\boldsymbol{n = 35, \alpha = 0.05}$), the generated dataset should be having two LP, and probably a high LP that is generated randomly be either good or bad. If it is good high LP almost should be one of two leverage points, otherwise, the total number of LP will be three. This procedure has been done for all simulation scenarios. Each table has the results of both diagnostics single detection and group diagnostic methods. Therefore, the discussion of results would be taken the performance of single diagnostic methods first and then the dicussion the results of group diagnostic has been considered with some details.

The results of single diagnostic methods (Hat,RMD, and Hadi) that presented in Table 1, Hadi's potential method has proved its ability accuracy diagnostic than Hat matrix and RMD. When ($\boldsymbol{n = 35, 45}$) the average numbers of $\boldsymbol{E}$ cases and swap of Hadi's potential method are less than Hat,RMD methods. In spite of that all the E cases of single diagnostic methods are involved the correct number of outlying cases, but Hadi's potential method reduced the swamping cases to the minimum . his superiority of Hadi's potential than other single diagnostic methods method has not held long. The signs of broken have started of this method is to be clear when ($\boldsymbol{n = 70}$) and there is vertical outliers and leverage points were present togather in the data. Table 1 has shown that RMD method is more accurate than Hadi's potential method when data are contaminated by LP & VO and ($\boldsymbol{n = 70, 90, 140}$) or in the presence of LP and ($\boldsymbol{n = 90, 140}$). We recorded that the single diagnostic methods may suffer from some masking cases particularly when the correct phases of it is more lower than their counterparts of group diagnostics. It is notable that Hadi's potential method started to be far from the correct cases gradually with the sample sizes are increased. The results that displays in Table 2 and 3 confirmed the outperforming the method of RMD than Hadi's potential and Hat matrix methods when $\{\boldsymbol{n = 45, 70, 90, 140}\}$ and where the outliers is presence in $\boldsymbol{n = 35}$ obsrvation. In another word, the Hadi's potential method are much influenced by masking cases than others as Table 2 and 3 are shown.

The performance of both group diagnostics methods DRGP.MVE and DRGP.RMVN are displayed in the Tabel 1,2, and 3. It is obvious that when 0.05, 0.10 of LP or LP and outliers together are present in the dataset, the total number of outlying cases (which is called $\boldsymbol{E}$ cases) that diagnostic by DRGP.RMVN method is less than the $\boldsymbol{E}$ cases of DRGP.MVE when ($\boldsymbol{n = 35, 45}$). However, Table 1 shows that $\boldsymbol{E}$ cases of five compared methods are 11.4682, 9.964, 4.995, 4,2268, and 4.1232, respectively. The closest number to (3) is 4.1232 which is determined by DRGP.RMVN method as the average of LP's that identified for overall 5000 iterations. The second method is DRGP.MVE which is detected 4.2268 LP's and Hadi's potential diagnosed 4.995. The Hat matrix and RMD methods are determined 11.4682 and 9.964 LP's, respectively. The good thing is that the E cases of all methods have been selected with the same number (2.9428) for the correct cases, but subtracting this number from the E cases of each method result-in the swamping cases.

Surely, the less number of (swap) will be the criterion for choosing the best method. Definitely, the results of Table 1 present that DRGP.RMVN is having a lower number of swap (1.1804) than others. in spite, of the swap of DRGP.MVE is very close to DRGP.RMVN, but the last method reduced the percentage of swap to 10%. The performance of all methods has been not changed in the second scenario of simulation (in the presence of five percent of outliers and leverage in the data) and outperforms DRGP.RMVN than DRGP.MVN and single detection methods even $\boldsymbol{n = 70}$ by two kinds from simulation scenarios are used. The DRGP.MVE method has proved its ability to compete with DRGP.RMVN method at (n=90,140) as Table 1 has been shown. That is Due to the values of the averages swamping DRGP.MVE is less than others.

The superior performance of DRGP.RMVN method has held even with increasing the sample size to (45,70) and the percentage of outlying observations increased to 10% as table 2 is showed that too. The performance of DRGP.MVE begins to get better than DRGP.RMVN when ($\boldsymbol{n = 90}$), ($\boldsymbol{\alpha = 0.05}$), but when $\boldsymbol{n = 90}$ with increasing $\boldsymbol{\alpha}$ to $\boldsymbol{0.10}$ DRGP.RMVN kept its high performance compared with other methods. Where ($\boldsymbol{n = 140}$), and ($\boldsymbol{\alpha = 0.05, 0.10}$) the DRGP.MVE shows its ability to identfy the LP's than others. But the outcomes of Table 3 confirmed the high diagnostics acuuracy of DRGP.RMVN than DRGP.MVE even though sometimes the performance of both methods are equevalant.

3.1 The Market value of Banks Iraq's Stock Market

The researchers collected these data out of the official website of the Iraqi Stock Markit after using the (SX60) system, where the annual data for market value were collected for nine of the local banks. These banks were chosen due to it the most traded than others for the period (2011-2015). The 45 samples are contained eight variables and they are (Trading Rate $\boldsymbol{x_1}$, Earning per share (EPS) $\boldsymbol{x_2}$, share turn over ratio $\boldsymbol{x_3}$, Annual Average price $\boldsymbol{x_4}$, the Assets

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

x_5, Undistributed earningsx_6, Annual Net Profit (Revenue) x_7, and market value y). We are considered seven out of those variables explain and show the size of the market value according to the multiple linear regression model that can be described as follows:

$$y = \beta_\circ + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 \qquad (4)$$

Figure 1 shows that the distribution of the residuals of model (4) is not follow normal distribution. It is clear, in the Q-Q plot, the fitted value vs residuals and scale location appear the resfigureiduals which are indexed in 25, 29,and 30 are outliers. The plot of residuals vs leverage points recorded some leverage points the indentified by Cook's distance measure.

Table 4 explains the accuracy of the correct diagnostic and the incorrect diagnostic (swamping & masking) for (Hadi, MD, Hat) methods compared with DRGP.MVE and DRGP.RMVN methods. Moreover, the DRGP.MVE and DRGP.RMVN are compared to each other.

Based on the simulation results DRGP.MVE and DRGP.RMVN methods are high efficiency and more accuarate than single diagnostic method to detect the leverage points. So, we consider it as criterion to identifying the correct and non-correct diagnostic. There is (45) samples of Banks market values probably motivate us to expect that DRGP.RMVN is more stable and accuracy diagnostics than DRGP.MVE. That is due to the simulation result shows the high performance of DRGP.RMVN with the small samples. The DRGP.MVE and DRGP.RMVN are determined (10) and (9) samples which are (1, 6, 7, 16, 23, 33, 34, 35, 36, 40) and (1, 6, 7, 13, 16, 33, 34, 35, 40) having LP's, respectively.

The Hat matrix identifies (18) samples which are (12, 13,14,16, 18, 23, 24, 25, 27, 31, 32, 33, 34, 35, 37, 38, 39, 40) are having LP's. The comparison of Hat matrix result with DRGP.MVE method, we noted that both methods are only matched to identify (6) samples that poses correct leverage points which are (16, 23, 33, 34, 35,40), while (12) samples

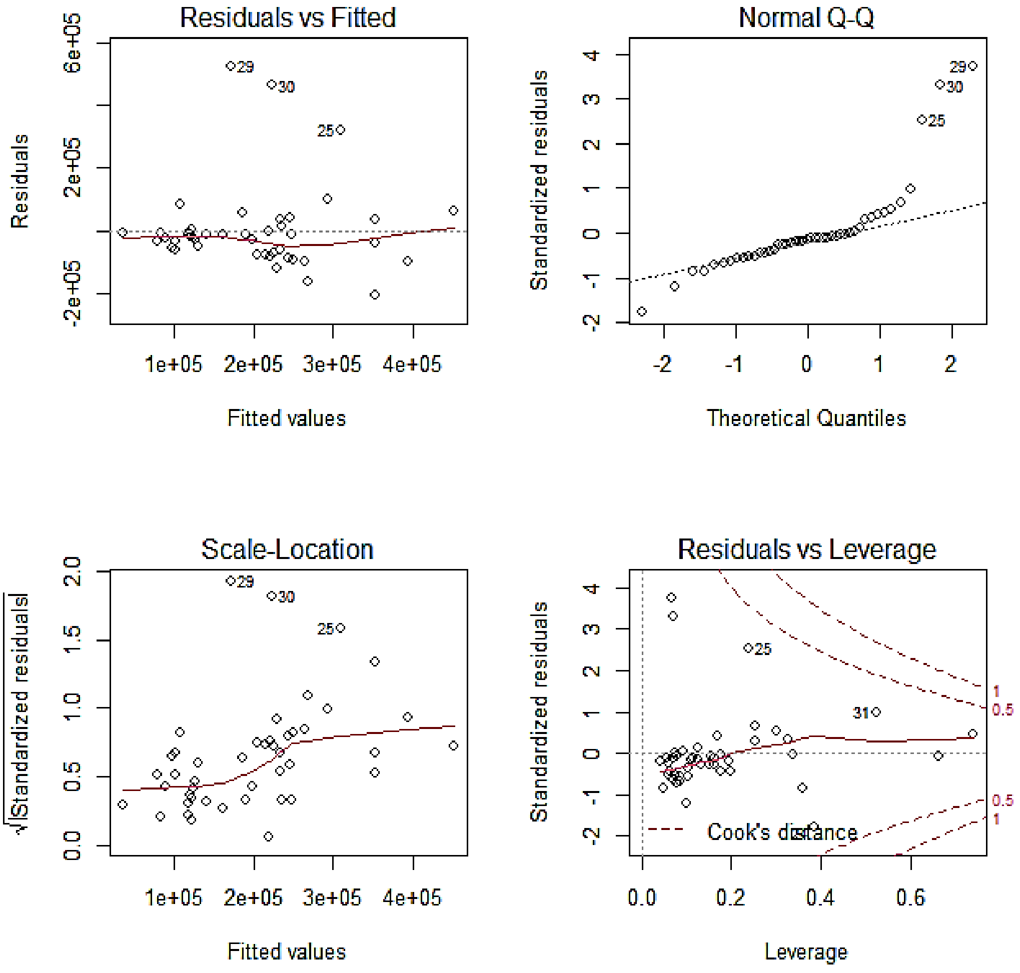


Figure 1. Initial diagnostics of outliers and leverage points for bank market value data

Table 4. Diagnostic Masking, Swamping and Correct to Hadi, MD, Hat methods in comparison with DRGP(RMVN) and DRGP(MVE) methods in terms of market value data.

Measure	Total	DRGP.MVE			DRGP.RMVN		
		Swamping	Correct	Masking	Swamping	Correct	Masking
Hat	18	12	6	4	12	6	3
MD	13	3	10	0	4	9	0
Hadi	8	5	3	7	1	3	6
DRGP.MVE	10			0	2	8	1
DRGP.RMVN	9						

are considered leverage points by Hat matrix, but are not detected by DRGP.MVE. So, this wrong diagnostics is pointed as swamping cases. On the other hand, the DRGP.MVE recorded (1,6,7,36) samples involved leverage points that are not detected by Hat matrix, therefore, we considered these as masking cases in Hat matrix. The comparison of Hat matrix with DRGP.RMVN method has not differ a lot, just it is reduced the masking cases to (3).

The MD method has reduced the total detection of leverage points from (18) case with Hat matrix to (13) case which are (1, 6, 7, 11, 13, 16, 23, 32, 33, 34, 35, 36, 40). This procedure is already would reduce the swamping cases to (3) and (4) compared with DRGP.MVE and DRGP.RMVN, respectively. So, the correct diagnostic of MD method matches with the correct diagnostics of DRGP.MVE and DRGP.RMVN without any masking cases. Unfortunately, Hadi's potaintial method detect (8) LP"s that are noted in (24, 25, 29, 30, 31, 34, 35, 40) samples, but only (3) samples are matched with DRGP.MVE and DRGP.RMVN methods {34, 35, 40} and other are swamping cases. Due to the difference in total detection of leverage points between DRGP.MVE and DRGP.RMVN methods are only one case, therefore the masking cases of Hadi's potential method are (7) and (6) compared with both of the previous methods, see Table ( ). However, DRGP.RMVN method has found that (9) samples are contained leverage points without any swamping and masking cases. This outcome is compatible with the simulation scenario where $\boldsymbol{n} = \mathbf{45}$.

Figure 2 contains (6) subgraphs, each graph shows the behavior of a certain diagnostic method against the standardized residuals measure. The vertical line represents the cutoff point of that diagnostic method, while the horizontal line represents the threshold of standardized residuals which equals 3 in this paper. It is obvious, that the developments that have happened in the detection methods of leverage points have reduced the swamping cases. The first subgraph of the Hat matrix method confirms that there are (18) leverage points and the second subgraph of MD displayed only (2) swamping cases. The third subgraph of RMD presents the high performance of RMD vs MD and has reduced the swamping cases better than Hat matrix method.

Figure 2 contains (6) subgraphs, each graph shows the behavior of a certain diagnostic method against the standardized residuals measure. The vertical line represents the cutoff point of that diagnostic method, while the horizontal line represents the threshold of standardized residuals which equals 3 in this paper. It is obvious, that the developments that have happened in the detection methods of leverage points have reduced the swamping cases. The first subgraph of the Hat matrix method confirms that there are (18) leverage points and the second subgraph of MD displayed only (2) swamping cases. The third subgraph of RMD presents the high performance of RMD vs. MD and has reduced the swamping cases better than the Hat matrix method. Hadi's potential method displayed in the subgraph fourth could not deal with these specific cases, therefore, we noted that it identified some cases that are not detected by other methods. Finally, the fifth and sixth subgraphs have related to DRGP.MVE and DRGP.RMVN methods and due to their asymptotic performances to each other, both graphs seem to be similar, but in reality, are a little bit different.

3.2 The Results

This research viewed some individual and group diagnostic methods to detect the outliers in the multivariable matrix using (Hadi Potential, RMD, Hat Matrix). However, these methods showed uneven efficiency in diagnostic accuracy, especially with the presence of the two phenomena of swamping and masking. These shortcomings led to the development of group diagnostic by some researchers like the DRGP.MVE method that relies on a robust variance and covariance matrix (MVE). Unfortunately, MVE is suffering from swamping cases, particularly with small samples. This reason led us to substitute the MVE matrix with another one called (RMVN) and proposed a new method called DRGP(RMVN). The efficiency of our proposed

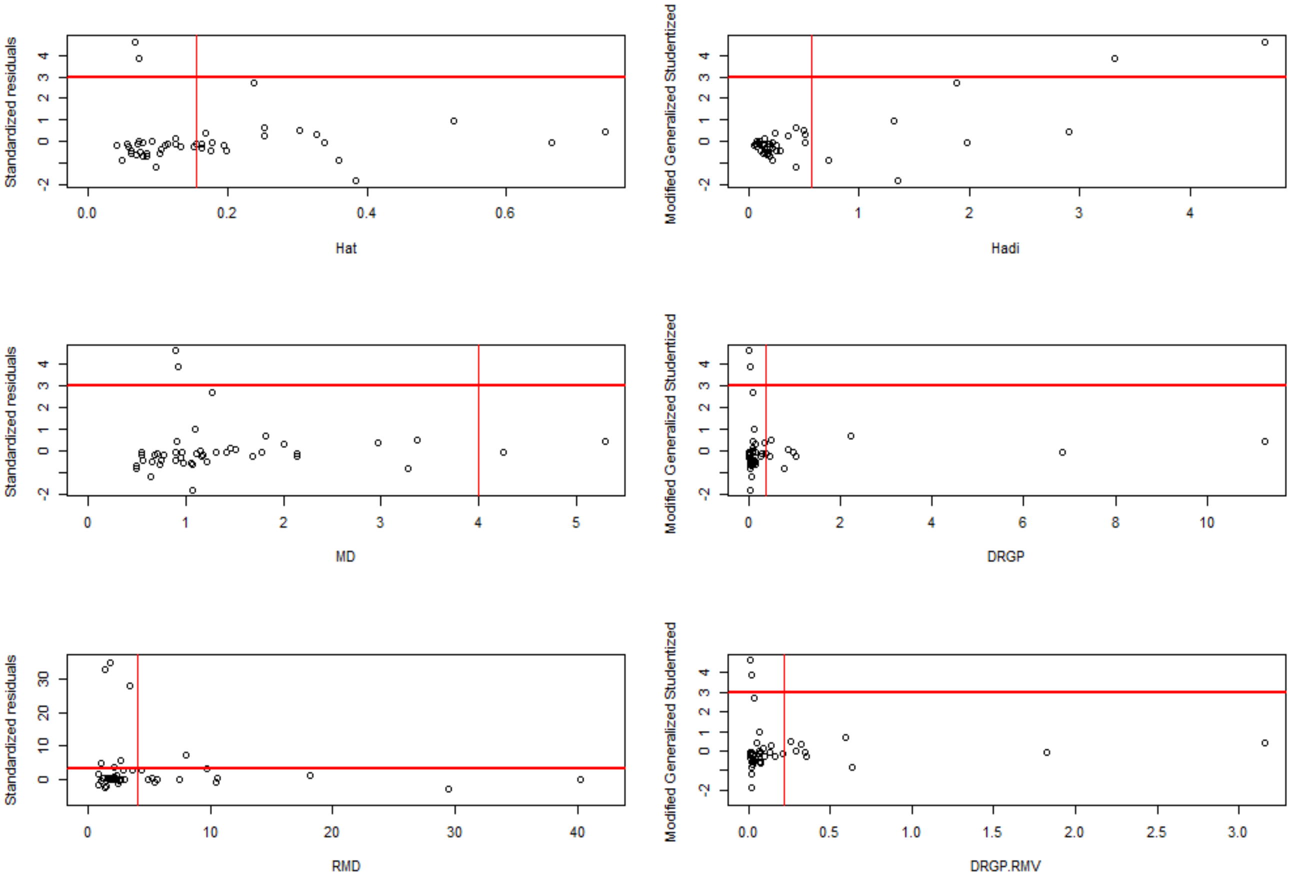


Figure 2. DRGP(RMVN), DRGP(MVE), RMD, Hadi for the banks market value data of Iraq's Stock Market

method has been tested with the previous techniques by subjecting it to many simulation studies using different sizes' samples and contaminating's different percentages of LP and (LP & VO). This is in addition to testing its efficiency on actual finance data. We can conclude from the simulation outcomes that our suggested method proved consistency and stability in the accuracy of diagnostic and the reduction of the average of the incorrect diagnostic that the previous techniques suffered from when the sizes of the samples were 35,45, and 70.

Furthermore, we noticed an enormous closeness in the correct diagnosis for LP's between our suggested method and the DRGP.MVE approach. Yet, the final form showed suffering in the problem of masking and swamping. That led to outperforming our proposed method among all the methods competing within limits, for example, the small sizes of the samples and the different rates of contamination. Thus, we recommend that the practitioners of statistics and researchers in this field use our suggested method to diagnose multivariate outliers apparent in multiple linear regression data.

4. References

A.H.M.R, Imon, Identifying multiple high leverage points in linear regression. Journal of Statistical Studies, Special Volume in Honour of Professor Mir Masoom Ali. 3(2002), 207–218.

Devlin, Susan J, Gnanadesikan, Ramanathan, & Kettenring, Jon R, Robust estimation of dispersion matrices and principal components, J J. AM. STAT. ASSOC., 76 (1981), 354-362.

F. R.Hampel, E. M. Ronchetti, P. Rousseeuw and W. A. Stahel, Robust Statistics,Wiley, New York,(1986).

H.Midi, N. Ramli, A.H.M.RImon, The performance of Diagnostic-Robust Generalized Potentials to identify multiple high leverage points in linear regression, J. APPL STAT. 36(2009): 507-520.

H. S. Uraibi, H. Midi, On Robust Bivariate and Multivariate Correlation Coefficient, Economic Computation & EconomicCybernetics Studies & Research, 53(2019), 2.

H. S. Uraibi, S. A. Alhussieny, Improvise Group Diagnostic Potential Measure for Multivariate Normal Data, Al-

DOI: https://doi.org/10.22452/mjs.sp2022no1.4

Qadisiyah Journal for Administrative and Economic Sciences, 23,(2021),2.

I-Cheng Yeh, "Modeling of strength of high performance concrete using artificial neural networks," Cement and Concrete Research, Vol. 28, No. 12, pp. 1797-1808 (1998).

Olive, David J., A resistant estimator of multivariate location and dispersion, Computational statistics & data analysis,,46,(2004), 93-102.

Olive, David J, & Hawkins, Douglas M., Robust multivariate location and dispersion. Preprint, (2010) (www. math.siu. Edu/olive/preprints. htm).

P.J. Huber, Robust Statistics, Wiley, New York, (1981).

P.j. Rousseeuw and A. M. Leroy, Robust Regression and Outlier Detection, Wiley, New York, (1987).

P. j. Rousseeuw and B. Van Zomeren, Unmasking multivariate outliers and leverage points, J. Am. STAT. ASSOC., 85(1990), 633-639

P. J., Rousseeuw, Least median of squares regression, J. AM. STAT. ASSOC., 79(1984), 871–880.

R.A. Maronna, R. D. Martin and V.J. Yohai, Robust Statistics Theory and Methods. New York: Willy and sons, (2006).

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021
Special Issue

DEGREE SUM ENERGY OF NON-COMMUTING GRAPH FOR DIHEDRAL GROUPS

Mamika Ujianita Romdhini[1ac], Athirah Nawawi[2ab]*

Abstract: For a finite group G, let $Z(G)$ be the centre of G. Then the non-commuting graph on G, denoted by Γ_G, has $G\backslash Z(G)$ as its vertex set with two distinct vertices v_p and v_q joined by an edge whenever $v_p v_q \neq v_q v_p$. The degree sum matrix of a graph is a square matrix whose (p,q)-th entry is $d_{v_p} + d_{v_q}$ whenever p is different from q, otherwise, it is zero, where d_{v_i} is the degree of the vertex v_i. This study presents the general formula for the degree sum energy, $E_{DS}(\Gamma_G)$, for the non-commuting graph of dihedral groups of order $2n$, D_{2n}, for all $n \geq 3$.

Keywords: *Non-commuting graph, dihedral group, degree sum matrix, the energy of a graph.*

1. Introduction

The non-commuting graph on $\boldsymbol{G}$, denoted by $\boldsymbol{\Gamma_G}$, has $\boldsymbol{G\backslash Z(G)}$ as its vertex set with two distinct vertices $\boldsymbol{v_p}$ and $\boldsymbol{v_q}$ joined by an edge whenever $\boldsymbol{v_p v_q \neq v_q v_p}$ (Abdollahi, 2006). In that sense, the non-commuting graph on $\boldsymbol{G}$, $\boldsymbol{\Gamma_G}$ can further be associated with the adjacency matrix. The $\boldsymbol{n \times n}$ adjacency matrix $\boldsymbol{A(\Gamma_G) = [a_{ij}]}$ of $\boldsymbol{\Gamma_G}$ has entries $\boldsymbol{a_{ij} = 1}$ if there is an edge between $\boldsymbol{v_i}$ to $\boldsymbol{v_j}$, and $\boldsymbol{a_{ij} = 0}$ otherwise. Since $\boldsymbol{\Gamma_G}$ is a simple graph, then $\boldsymbol{A(\Gamma_G)}$ is a symmetric matrix with zero diagonal entries. For a real number $\boldsymbol{\lambda}$, the characteristic polynomial $\boldsymbol{P_{A(\Gamma_G)}(\lambda)}$ of $\boldsymbol{\Gamma_G}$ is defined by $\boldsymbol{\det(\lambda I_n - A(\Gamma_G))}$, where $\boldsymbol{I_n}$ is an $\boldsymbol{n \times n}$ identity matrix. The eigenvalues of $\boldsymbol{\Gamma_G}$ are the roots of the equation $\boldsymbol{P_{A(\Gamma_G)}(\lambda) = 0}$, and they are labelled as $\boldsymbol{\lambda_1, \lambda_2, \dots, \lambda_n}$. The spectrum of $\boldsymbol{\Gamma_G}$ is given as a list of eigenvalues $\boldsymbol{\lambda_1, \lambda_2, \dots, \lambda_m}$, with their respective multiplicities $\boldsymbol{k_1, k_2, \dots, k_m}$ as exponents, denoted by $\boldsymbol{Spec(\Gamma_G) = \left\{\lambda_1^{(k_1)}, \lambda_2^{(k_2)}, \dots, \lambda_m^{(k_m)}\right\}}$. Furthermore, for all finite graphs, Gutman (1978) defined the energy of $\boldsymbol{\Gamma_G}$ as the sum of the absolute values of the eigenvalues, denoted by $\boldsymbol{E(\Gamma_G) = \sum_{i=1}^{n} |\lambda_i|}$.

There are several interesting studies regarding the non-commuting graph involving the spectrum and energy of its adjacency matrix. Mahmoud *et al.* (2017) described the adjacency energy of the non-commuting graph for dihedral groups of order $\boldsymbol{2n}$. In the same year, Dutta and Nath (2017) computed the Laplacian energy of the non-commuting graph for finite non-abelian groups, including the dihedral groups of order $\boldsymbol{2n}$. Alternatively, Fasfous and Nath (2020) computed the spectrum and energy of the non-commuting graph for certain classes of finite groups inclusive of $\boldsymbol{D_{2n}}$. They found that the adjacency energy of the non-commuting graph is not equal to the Laplacian energy for some finite groups. This refutes the conjecture by Gutman *et al.* in 2008, stating that the adjacency energy of any graph is smaller than or equal to its Laplacian energy, which holds for all graphs. However, readers can also see different perspectives of this particular graph where the discussion on the detour index, eccentric connectivity, total eccentricity polynomials, and mean distance of the non-commuting graph for the dihedral group by Khasraw *et al.* (2020).

Throughout this paper, the discussion will be directed to the degree sum energy defined by Ramane *et al.* (2013). In particular, Jog and Kotambari (2016) presented the degree sum energy of six types of simple graphs, namely, Wheel graphs, Path Tadpole graphs, Dumbbell graphs, coalescence regular graphs, complete graphs, and cycles. Apart from that, Hosamani and Ramane (2016) also discussed the degree sum energy focusing on determining the lower bounds of degree sum energy of simple graphs. However, a limited number of studies central to the degree sum matrices for non-commuting graphs have been found. Therefore, we aim to formulate the degree sum energy of the non-commuting graph for the dihedral groups.

For $\boldsymbol{n \geq 3}$, the non-abelian dihedral group $\boldsymbol{D_{2n}}$ of order $\boldsymbol{2n}$ is defined as the reflection and rotation motions that return a regular $\boldsymbol{n}$-gon to its original state, with the composition operation denoted by $\boldsymbol{D_{2n}}$. The $\boldsymbol{n}$ rotations are

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA.
[b]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA.
[c]Department of Mathematics, Faculty of Mathematics and Natural Science, Universitas Mataram, Mataram, 83125, INDONESIA. E-mail: mamika@unram.ac.id[1]

*Corresponding Author: athirah@upm.edu.my

Received: January 21, 2022
Accepted: April 9, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

$\boldsymbol{a^i}$ and the reflections are $\boldsymbol{a^ib}$, where $\boldsymbol{1 \leq i \leq n}$. Therefore, $\boldsymbol{D_{2n}}$ can be written as:

$$\boldsymbol{D_{2n} = \langle a, b : a^n = b^2 = e, bab = a^{-1} \rangle}.$$

The centre of $\boldsymbol{D_{2n}}$, $\boldsymbol{Z(D_{2n})}$ is equal to $\boldsymbol{\{e\}}$ **if $\boldsymbol{n}$ is odd** and $\boldsymbol{\{e, a^{\frac{n}{2}}\}}$ **if $\boldsymbol{n}$ is even**. The centralizer of the element $\boldsymbol{a^i}$ in the group $\boldsymbol{D_{2n}}$ is $\boldsymbol{C_{D_{2n}}(a^i) = \{a^i : 1 \leq i \leq n\}}$ and for the element $\boldsymbol{a^ib}$ is either $\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^ib\}}$, **if $\boldsymbol{n}$ is odd**, or $\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^{\frac{n}{2}}, a^ib, a^{\frac{n}{2}+i}b\}}$, **if $\boldsymbol{n}$ is even**.

2. Preliminaries

We define $\boldsymbol{d_{v_p}}$ as the degree of a vertex $\boldsymbol{v_p}$, which is the number of vertices adjacent to $\boldsymbol{v_p}$. The definition of the degree sum matrix is given as follows:

Definition 2.1. (Ramane *et al.,* 2013) The degree sum matrix of order $\boldsymbol{n \times n}$ associated with a graph $\boldsymbol{\Gamma}$ is given by $\boldsymbol{DS(\Gamma) = [ds_{pq}]}$ whose $\boldsymbol{(p, q)}$-th entry is given by

$$ds_{pq} = \begin{cases} d_{v_p} + d_{v_q}, & \text{if } p \neq q \\ 0, & \text{if } p = q \end{cases}$$

In this section, we include some previous results, which benefit the computations of our main results. Recall that, for any $\boldsymbol{n \geq 3}$, $\boldsymbol{D_{2n} = \langle a, b : a^n = b^2 = e, bab = a^{-1} \rangle}$. We define $\boldsymbol{G_1 = \{a^i : 1 \leq i \leq n\} \backslash Z(D_{2n})}$ and $\boldsymbol{G_2 = \{a^ib : 1 \leq i \leq n\}}$. The following is the result of the degree of each vertex in the non-commuting graph of $\boldsymbol{G = G_1 \cup G_2}$.

Theorem 2.1: (Khasraw *et al.*, 2020) Let $\boldsymbol{\Gamma_G}$ be the non-commuting graph on $\boldsymbol{G}$, where $\boldsymbol{G = G_1 \cup G_2}$. Then,

$$1.\ d_{a^i} = n, \text{ and}$$

$$2.\ d_{a^ib} = \begin{cases} 2n-2, & \text{if } n \text{ is odd} \\ 2n-4, & \text{if } n \text{ is even} \end{cases}.$$

A graph which has $\boldsymbol{n}$ vertices with the degree of every vertex being $\boldsymbol{n-1}$ is called a complete graph $\boldsymbol{K_n}$. Moreover, the complement of the complete graph $\boldsymbol{K_n}$ is written as $\boldsymbol{\overline{K}_n}$. Consequently, the isomorphism of the non-commuting graph with some common types of graphs can be seen in the following result:

Theorem 2.2: (Khasraw *et al.,* 2020) Let $\boldsymbol{\Gamma_G}$ be the non-commuting graph on $\boldsymbol{D_{2n}}$.

1. If $\boldsymbol{G = G_1}$, then $\boldsymbol{\Gamma_G \cong \overline{K}_m}$, where $\boldsymbol{m = |G_1|}$.
2. If $\boldsymbol{G = G_2}$, then $\boldsymbol{\Gamma_G \cong \begin{cases} K_n, & \textbf{if } n \textbf{ is odd} \\ K_n - \frac{n}{2}K_2, & \textbf{if } n \textbf{ is even} \end{cases}}$,

where $\boldsymbol{\frac{n}{2}K_2}$ denotes $\boldsymbol{\frac{n}{2}}$ copies of $\boldsymbol{K_2}$.

The following lemma helps us to compute the characteristic polynomial of the non-commuting graph of $\boldsymbol{D_{2n}}$.

Lemma 2.1: (Ramane & Shinde, 2017) If $\boldsymbol{a, b, c}$ and $\boldsymbol{d}$ are real numbers and $\boldsymbol{J_n}$ is an $\boldsymbol{n \times n}$ matrix whose entries are equal to one, then the determinant of the $\boldsymbol{(n_1 + n_2) \times (n_1 + n_2)}$ matrix of the form

$$\boldsymbol{\begin{vmatrix} (\lambda + a)I_{n_1} - aJ_{n_1} & -cJ_{n_1 \times n_2} \\ -dJ_{n_2 \times n_1} & (\lambda + b)I_{n_2} - bJ_{n_2} \end{vmatrix}},$$

can be simplified in an expression given by $\boldsymbol{(\lambda + a)^{n_1 - 1}(\lambda + b)^{n_2 - 1}\big((\lambda - (n_1 - 1)a)(\lambda - (n_2 - 1)b) - n_1n_2cd\big)}$,

where $\boldsymbol{1 \leq n_1, n_2 \leq n}$ and $\boldsymbol{n_1 + n_2 = n}$.

The following lemma is the result of the spectrum of the complete graph, which is useful for computing the energy of the non-commuting graph for $\boldsymbol{D_{2n}}$.

Lemma 2.2: (Brouwer & Haemers, 2010) If $\boldsymbol{K_n}$ is the complete graph on $\boldsymbol{n}$ vertices, then its adjacency matrix is $\boldsymbol{J_n - I_n}$ and the spectrum of $\boldsymbol{K_n}$ is $\boldsymbol{\{(n-1)^{(1)}, (-1)^{(n-1)}\}}$.

3. Main Results

This section presents several results on the degree sum energy of the non-commuting graph on the dihedral group of order $\boldsymbol{2n}$, $\boldsymbol{D_{2n}}$.

Theorem 3.1. Let $\boldsymbol{\Gamma_G}$ be the non-commuting graph on $\boldsymbol{G}$ and $\boldsymbol{E_{DS}}$ be the degree sum energy of $\boldsymbol{\Gamma_G}$.

1. If $\boldsymbol{G = G_1}$, then $\boldsymbol{E_{DS}(\Gamma_G) = 0}$.
2. If $\boldsymbol{G = G_2}$, then

$$\boldsymbol{E_{DS}(\Gamma_G) = \begin{cases} 4(n-1)^2, & \textbf{if } n \textbf{ is odd} \\ 4(n-2)(n-1), & \textbf{if } n \textbf{ is even} \end{cases}}.$$

Proof.

1. **When $\boldsymbol{n}$ is odd.** From Theorem 2.2 (1), $\boldsymbol{\Gamma_G = \overline{K}_m}$, where $\boldsymbol{G = G_1}$ and $\boldsymbol{m = |G_1| = n - 1}$. Then, every vertex of $\boldsymbol{\Gamma_G}$ has degree zero. Thus, the degree sum matrix of $\boldsymbol{\Gamma_G}$ is an $\boldsymbol{(n-1) \times (n-1)}$ zero matrix, $\boldsymbol{DS(\Gamma_G) = [0]}$. The only eigenvalue of $\boldsymbol{DS(\Gamma_G)}$ is zero with multiplicity $\boldsymbol{n-1}$. Thus, $\boldsymbol{E_{DS}(\Gamma_G) = 0}$.

   When $\boldsymbol{n}$ is even. From Theorem 2.2 (1), $\boldsymbol{\Gamma_G = \overline{K}_m}$, where $\boldsymbol{G = G_1}$ and $\boldsymbol{m = |G_1| = n - 2}$, removing $\boldsymbol{e}$ and $\boldsymbol{a^{\frac{n}{2}}}$ in $\boldsymbol{Z(D_{2n})}$. Then, every vertex of $\boldsymbol{\Gamma_G}$ has degree zero. Hence, the degree sum matrix of $\boldsymbol{\Gamma_G}$ is an $\boldsymbol{(n-2) \times (n-2)}$ zero matrix, $\boldsymbol{DS(\Gamma_G) = [0]}$. The only eigenvalue of $\boldsymbol{DS(\Gamma_G)}$ is zero with multiplicity $\boldsymbol{n-2}$. Thus, $\boldsymbol{E_{DS}(\Gamma_G) = 0}$.

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

2. When n is odd. From Theorem 2.2 (2), $\Gamma_G = K_n$, where $G = G_2$. Then, every vertex has a degree $n-1$. Thus, the

$$DS(\Gamma_G) = \begin{bmatrix} 0 & 2(n-1) & \cdots & 2(n-1) \\ 2(n-1) & 0 & \cdots & 2(n-1) \\ \vdots & \vdots & \ddots & \vdots \\ 2(n-1) & 2(n-1) & \cdots & 0 \end{bmatrix}$$
$$= 2(n-1)\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}$$

degree sum matrix of Γ_G is an $n \times n$ matrix, $DS(\Gamma_G) = [ds_{pq}]$ whose (p,q)-th entry is $ds_{pq} = (n-1)+(n-1) = 2(n-1)$ for $p \neq q$, and 0 otherwise. Hence,

In other words, the degree sum matrix of Γ_G is the product of $2(n-1)$ and the adjacency matrix of K_n. Based on Lemma 2.2, $Spec(K_n)$ is given by $\{(n-1)^{(1)}, (-1)^{(n-1)}\}$. Since the adjacency energy of K_n is $|n-1| + (n-1)|-1| = 2(n-1)$, the degree sum energy of Γ_G will be $2(n-1) \cdot 2(n-1) = 4(n-1)^2$.

When n is even. From Theorem 2.2 (2), $\Gamma_G = K_n - \frac{n}{2}K_2$, where $G = G_2$. Then, every vertex has a degree of $n-2$. We can now construct an $n \times n$ degree sum matrix of Γ_G,

$$DS(\Gamma_G) = \begin{bmatrix} 0 & 2(n-2) & \cdots & 2(n-2) \\ 2(n-2) & 0 & \cdots & 2(n-2) \\ \vdots & \vdots & \ddots & \vdots \\ 2(n-2) & 2(n-2) & \cdots & 0 \end{bmatrix}$$
$$= 2(n-2)\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}.$$

$DS(\Gamma_G) = [ds_{pq}]$ whose (p,q)-th entry is $ds_{pq} = n-2+n-2 = 2(n-2)$ for $p \neq q$, and 0 otherwise. Hence,

In other words, the degree sum matrix of Γ_G is the product of $2(n-2)$ and the adjacency matrix of K_n. Using the same argument as in the previous case, the degree sum energy of Γ_G is given by $2(n-2) \cdot 2(n-1) = 4(n-2)(n-1)$.

The illustration of Theorem 3.1 is given by the following examples for $n = 4$ and $n = 5$.

Example 1. Let Γ_G be the non-commuting graph on G, where $G \subset D_8$, $D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, $Z(D_8) = \{e, a^2\}$, $G_1 = \{a, a^3\}$, $G_2 = \{b, ab, a^2b, a^3b\}$, $C_{D_{2n}}(b) = \{e, a^2, b, a^2b\} = C_{D_{2n}}(a^2b)$, $C_{D_{2n}}(ab) = \{e, a^2, ab, a^3b\} = C_{2n}(a^3b)$. By using the information on the centralizer of each element in G, then the non-commuting graph of G is given as in Figure 1.

When $G = G_1$ from Figure 1 (i), it is clear that we only have two vertices a and a^3 and the degree of each vertex is zero. Then, the non-commuting graph of G_1 is the complement of the complete graph on two vertices, $\overline{K}_2$. This implies that we have a 2×2 degree sum matrix of Γ_G with all the entries are zero, $DS(\Gamma_G) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Furthermore, the characteristic polynomial of $DS(\Gamma_G)$ is $P_{DS(\Gamma_G)}(\lambda) = \det(\lambda I_2 - DS(\Gamma_G)) = \lambda^2$. It follows that the eigenvalues of $DS(\Gamma_G)$ is zero with multiplicity 2. Therefore, the degree sum energy of Γ_G is $E_{DS}(\Gamma_G) = 0$.

However, if $G = G_2$, then each vertex $a^i b$, where $1 \leq i \leq 4$, is of degree two, as shown in Figure 1 (ii). Then, the non-commuting graph of G_2 on four vertices is $K_4 - 2K_2$. This means that we have a 4×4 degree sum matrix of Γ_G with the non-diagonal entries are $2+2=4$, while the diagonal entries are zero. Then, we obtain

$$DS(\Gamma_G) = \begin{bmatrix} 0 & 4 & 4 & 4 \\ 4 & 0 & 4 & 4 \\ 4 & 4 & 0 & 4 \\ 4 & 4 & 4 & 0 \end{bmatrix}$$

.

Furthermore, the characteristic polynomial of $DS(\Gamma_G)$ is $P_{DS(\Gamma_G)}(\lambda) = \det(\lambda I_4 - DS(\Gamma_G)) = (\lambda+4)^3(\lambda - 12)$. This implies that the eigenvalues of $DS(\Gamma_G)$ are a single $\lambda = 12$ and $\lambda = -4$ with multiplicity 3. Therefore, $E_{DS}(\Gamma_G) = |12| + 3|-4| = 24 = 4(4-2)(4-1)$.

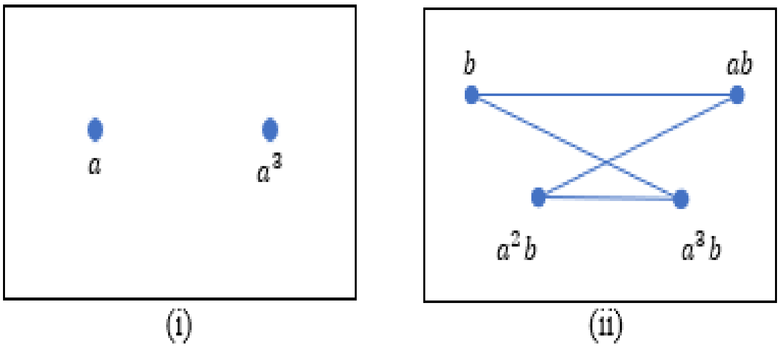


Figure 1. Non-commuting graph of G, where (i) $G = G_1$ and (ii) $G = G_2$.

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

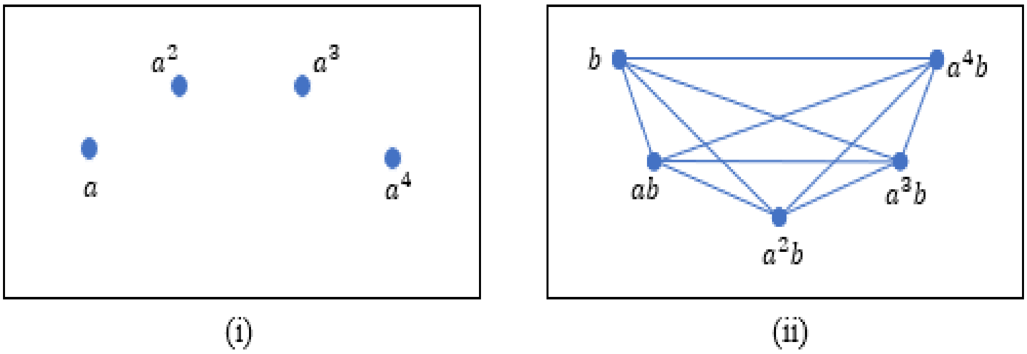


Figure 2. Non-commuting graph of G, where (i) $G = G_1$, and (ii) $G = G_2$.

Example 2. Let Γ_G be the commuting graph on G, where $G \subset D_{10}$, $D_{10} = \{e,\ a,\ a^2,\ a^3,\ a^4\ b,\ ab,\ a^2b,\ a^3b,\ a^4b\}$, $Z(D_{10}) = \{e\}$, $G_1 = \{a, a^2, a^3, a^4\}$, $G_2 = \{\ b,\ ab,\ a^2b,\ a^3b,\ a^4b\}$, $C_{D_{2n}}(a^ib) = \{e, a^ib\}$, and $C_{D_{2n}}(a^i) = \{a^i\colon 1 \le i \le n\}$. Using the information on the centralizer of each element in G, the non-commuting graph of G is given in Figure 2. When $G = G_1$, from Figure 2 (i), it is clear that we have four vertices a^i, for $1 \le i \le 4$, and the degree of each vertex is zero. Then the non-commuting graph of G_1 is the complement of the complete graph on four vertices, $\overline{K}_4$. This implies that we have a 4×4 degree sum matrix of Γ_G with all the entries are zero, $DS(\Gamma_G) = [0]$. Furthermore, the characteristic polynomial of $DS(\Gamma_G)$ is $P_{DES(\Gamma_G)}(\lambda) = \det(\lambda I_4 - DS(\Gamma_G)) = \lambda^4$. It follows that the eigenvalues of $DS(\Gamma_G)$ is zero with multiplicity 4. Therefore, the degree sum energy of Γ_G is $E_{DS}(\Gamma_G) = 0$.

In another case, if $G = G_2$, with each vertex a^ib, where $1 \le i \le 5$, is of degree four as shown in Figure 2 (ii), then the non-commuting graph of G_2 on five vertices is the complete graph, K_5. This implies that we have a 5×5 degree sum matrix of Γ_G with the non-diagonal entries are $4 + 4 = 8$, while the diagonal entries are zero. Then, we obtain

$$DS(\Gamma_G) = \begin{bmatrix} 0 & 8 & 8 & 8 & 8 \\ 8 & 0 & 8 & 8 & 8 \\ 8 & 8 & 0 & 8 & 8 \\ 8 & 8 & 8 & 0 & 8 \\ 8 & 8 & 8 & 8 & 0 \end{bmatrix}.$$

Furthermore, the characteristic polynomial of Γ_G is $P_{DS(\Gamma_G)}(\lambda) = \det(\lambda I_5 - DS(\Gamma_G)) = (\lambda + 8)^4(\lambda - 32)$. This implies that the eigenvalues of $DS(\Gamma_G)$ are a single $\lambda = 32$ and $\lambda = -8$ with multiplicity 4. Therefore, $E_{DS}(\Gamma_G) = |32| + 4|-8| = 64 = 4(5-1)^2$.

Theorem 3.2. Let Γ_G be the non-commuting graph on G, where $G = G_1 \cup G_2 \subset D_{2n}$, then the characteristic polynomial of degree sum matrices for Γ_G is given by

1. $P_{DS(\Gamma_G)}(\lambda) = (\lambda + 2n)^{n-2}(\lambda + 2(2n-2))^{n-1}(\lambda^2 - 2(3n^2 - 6n + 2)\lambda - n(n-1)(n^2 + 12n - 12)$, for n is odd, and
2. $P_{DS(\Gamma_G)}(\lambda) = (\lambda + 2n)^{n-3}(\lambda + 2(2n-4))^{n-1}(\lambda^2 - 2(3n^2 - 9n + 4)\lambda - n(n^3 + 6n^2 - 24n + 16)$, for n is even.

Proof.

1. By Theorem 2.1 for the odd n case, we have $d_{a^i} = n$ and $d_{a^ib} = 2n - 2$, for all $1 \le i \le n$. Then, using the fact that $Z(D_{2n}) = \{e\}$, we have $2n - 1$ vertices for Γ_G, where $G = G_1 \cup G_2$. The set of vertices consists of $n - 1$ vertices of a^i, for $1 \le i \le n - 1$, and n vertices of a^ib, for $1 \le i \le n$. Then, the degree sum matrix for Γ_G is a $(2n-1) \times (2n-1)$ matrix, $DS(\Gamma_G) = [ds_{pq}]$ whose (p,q)-th entries are:
   (i) $ds_{pq} = n + n = 2n$, for $p \ne q$, and $1 \le p, q \le n - 1$,
   (ii) $ds_{pq} = n + (2n - 2) = 3n - 2$, for $1 \le p \le n - 1$ and $n \le q \le 2n - 1$,
   (iii) $ds_{pq} = (2n - 2) + n = 3n - 2$, for $n \le p \le 2n - 1$ and $1 \le q \le n - 1$,
   (iv) $ds_{pq} = (2n - 2) + (2n - 2) = 2(2n - 2)$, for $p \ne q$, $n \le p, q \le 2n - 1$,
   (v) $ds_{pq} = 0$, for $p = q$.

   We can construct $DS(\Gamma_G)$ given as follows:

$$DS(\Gamma_G) = \left[\begin{array}{cccc:cccc} 0 & 2n & \cdots & 2n & 3n-2 & 3n-2 & \cdots & 3n-2 \\ 2n & 0 & \cdots & 2n & 3n-2 & 3n-2 & \cdots & 3n-2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2n & 2n & \cdots & 0 & 3n-2 & 3n-2 & \cdots & 3n-2 \\ \hdashline 3n-2 & 3n-2 & \cdots & 3n-2 & 0 & 2(2n-2) & \cdots & 2(2n-2) \\ 3n-2 & 3n-2 & \cdots & 3n-2 & 2(2n-2) & 0 & \cdots & 2(2n-2) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 3n-2 & 3n-2 & \cdots & 3n-2 & 2(2n-2) & 2(2n-2) & \cdots & 0 \end{array}\right]$$

$$= \begin{bmatrix} 2n(J_{n-1} - I_{n-1}) & (3n-2)J_{(n-1)\times n} \\ (3n-2)J_{n\times(n-1)} & 2(2n-2)(J_n - I_n) \end{bmatrix}$$

$$= \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}.$$

   In this case, $DS(\Gamma_G)$ is divided into four blocks, where the first block is B_1, which is a block of $(n-1) \times (n-1)$ matrix with zero diagonal, and every non-diagonal entry is $2n$. In the next two blocks, we have B_2 and B_3 matrices, which are of the size $(n-1) \times n$ and $n \times (n-1)$, respectively, whose entries are $3n - 2$. The last block

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

is B_4, which is an $n \times n$ matrix with zero diagonal, and every non-diagonal entry is $2(2n-2)$. Then, we obtain the characteristic polynomial of $DS(\Gamma_G)$ from the following determinant

$$P_{DS(\Gamma_G)}(\lambda) = |\lambda I_{2n-1} - DS(\Gamma_G)|$$
$$= \begin{vmatrix} (\lambda+2n)I_{n-1} - 2nJ_{n-1} & -(3n-2)J_{(n-1)\times n} \\ -(3n-2)\,J_{n\times(n-1)} & (\lambda+2(2n-2))I_n - 2(2n-2)J_n \end{vmatrix}.$$

Using Lemma 2.1, with $a = 2n$, $b = 2(2n-2)$, $c = 3n-2$, $d = 3n-2$, $n_1 = n-1$ and $n_2 = n$, we obtain the required result.

2. Again, by Theorem 2.1 for the even n case, we know that $d_{a^i} = n$ and $d_{a^ib} = 2n-4$, for all $1 \le i \le n$. Then, using the fact that $Z(D_{2n}) = \{e, a^{\frac{n}{2}}\}$, we have $2n-2$ vertices for Γ_G, where $G = G_1 \cup G_2$. The set of vertices consists of $n-2$ vertices of a^i, for $1 \le i \le n-1$, $i \ne \frac{n}{2}$, and n vertices of a^ib, for $1 \le i \le n$. Then, the degree sum matrix for Γ_G is a $(2n-2)\times(2n-2)$ matrix, $DS(\Gamma_G) = [ds_{pq}]$ whose (p,q)-th entry is
(i) $ds_{pq} = n + n = 2n$, for $p \ne q$, and $1 \le p, q \le n-2$,
(ii) $ds_{pq} = n + (2n-4) = 3n-4$, for $1 \le p \le n-2$ and $n-1 \le q \le 2n-2$,
(iii) $ds_{pq} = (2n-4) + n = 3n-4$, for $n-1 \le p \le 2n-2$ and $1 \le q \le n-2$,
(iv) $ds_{pq} = (2n-4) + (2n-4) = 2(2n-4)$, for $p \ne q$, $n-1 \le p, q \le 2n-2$,
(v) $des_{pq} = 0$, for $p = q$.

We can construct $DS(\Gamma_G)$ as follows:

$$DS(\Gamma_G)$$
$$= \left[\begin{array}{cccc:cccc} 0 & 2n & \cdots & 2n & 3n-4 & 3n-4 & \cdots & 3n-4 \\ 2n & 0 & \cdots & 2n & 3n-4 & 3n-4 & \cdots & 3n-4 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2n & 2n & \cdots & 0 & 3n-4 & 3n-4 & \cdots & 3n-4 \\ \hdashline 3n-4 & 3n-4 & \cdots & 3n-4 & 0 & 2(2n-4) & \cdots & 2(2n-4) \\ 3n-4 & 3n-4 & \cdots & 3n-4 & 2(2n-4) & 0 & \cdots & 2(2n-4) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 3n-4 & 3n-4 & \cdots & 3n-4 & 2(2n-4) & 2(2n-4) & \cdots & 0 \end{array}\right]$$
$$= \begin{bmatrix} 2n(J_{n-2} - I_{n-2}) & (3n-4)J_{(n-2)\times n} \\ (3n-4)J_{n\times(n-2)} & 2(2n-4)(J_n - I_n) \end{bmatrix}$$
$$= \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}.$$

In this case, $DS(\Gamma_G)$ is divided into four blocks, where the first block is M_1, which is a block of $(n-2)\times(n-2)$ matrix with zero diagonal, where every non-diagonal entry is $2n$. The next two blocks are M_2 and M_3, which are of the size $(n-2)\times n$ and $n \times (n-2)$, respectively, whose all entries are equal to $3n-4$. The last block is M_4, which is an $n \times n$ matrix with zero diagonal, while every non-diagonal entry is $2(2n-4)$. Then, we obtain the characteristic polynomial of $DS(\Gamma_G)$ from the following determinant

$$P_{DS(\Gamma_G)}(\lambda) = |\lambda I_{2n-2} - DS(\Gamma_G)|$$
$$= \begin{vmatrix} (\lambda+2n)I_{n-2} - 2nJ_{n-2} & -(3n-4)J_{(n-2)\times n} \\ -(3n-4)\,J_{n\times(n-2)} & (\lambda+2(2n-4))I_n - 2(2n-4)J_n \end{vmatrix}.$$

Using Lemma 2.1, with $a = 2n$, $b = 2(2n-4)$, $c = 3n-4$, $d = 3n-4$, $n_1 = n-2$ and $n_2 = n$, we obtain the required result.

Consequently, the degree sum energy of the non-commuting graph for the dihedral group of order $2n$ can be expressed in the following theorem.

Theorem 3.3: Let Γ_G be the non-commuting graph on G, where $G = G_1 \cup G_2$, then the degree sum energy for Γ_G is given by

1. for n is odd,

$$E_{DS}(\Gamma_G) = 2(3n^2 - 6n + 2) + 2\sqrt{10n^4 - 25n^3 + 24n^2 - 12n + 4},$$

2. and for n is even,

$$E_{DS}(\Gamma_G) = 2(3n^2 - 9n + 4) + 2\sqrt{10n^4 - 48n^3 + 81n^2 - 56n + 16}.$$

Proof.

1. By Theorem 3.2 (1), for the odd n, the characteristic polynomial of $DS(\Gamma_G)$ has four eigenvalues, with the first eigenvalue is $\lambda_1 = -2n$ of multiplicity $n-2$, and the second eigenvalue is $\lambda_2 = -2(2n-2)$ of multiplicity $n-1$. The quadratic formula gives the other two eigenvalues, which are $\lambda_3, \lambda_4 = (3n^2 - 6n + 2) \pm \sqrt{10n^4 - 25n^3 + 24n^2 - 12n + 4}$, where one is a positive real number, and the other is negative. Hence, the degree sum energy for Γ_G is
$$E_{DS}(\Gamma_G) = (n-2)|-2n| + (n-1)|-2(2n-2)| + \left|(3n^2 - 6n + 2) \pm \sqrt{10n^4 - 25n^3 + 24n^2 - 12n + 4}\right|$$
$$= 2(3n^2 - 6n + 2) + 2\sqrt{10n^4 - 25n^3 + 24n^2 - 12n + 4}.$$

2. For n is even and following Theorem 3.2 (2), the characteristic polynomial of $DS(\Gamma_G)$ has four eigenvalues, where the first eigenvalue is $\lambda_1 = -2n$ of multiplicity $n-3$, and the second eigenvalue is $\lambda_2 = -2(2n-4)$ of multiplicity $n-1$. The quadratic formula gives the other two eigenvalues, which are $\lambda_3, \lambda_4 = (3n^2 - 9n + 4) \pm \sqrt{10n^4 - 48n^3 + 81n^2 - 56n + 16}$. One is a positive real number for this current case, and the other is negative. Therefore, the degree sum energy for Γ_G is
$$E_{DS}(\Gamma_G) = (n-3)|-2n| + (n-1)|-2(2n-4)| + \left|(3n^2 - 9n + 4) \pm \sqrt{10n^4 - 48n^3 + 81n^2 - 56n + 16}\right|$$
$$= 2(3n^2 - 9n + 4) + 2\sqrt{10n^4 - 48n^3 + 81n^2 - 56n + 16}.$$

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

4. Conclusion

This paper has given the general formula of degree sum energy of non-commuting graph for dihedral groups of order $\boldsymbol{2n}$, $\boldsymbol{n \geq 3}$. For $\boldsymbol{n}$ is odd, $\boldsymbol{E_{DS}(\Gamma_G) = 2\left(3n^2 - 6n + 2\right) + 2\sqrt{10n^4 - 25n^3 + 24n^2 - 12n + 4}}$, while for $\boldsymbol{n}$ is even, $\boldsymbol{E_{DS}(\Gamma_G) = 2(3n^2 - 9n + 4) + 2\sqrt{10n^4 - 48n^3 + 81n^2 - 56n + 16}}$.

5. Acknowledgements

This research has been supported by the Ministry of Education (MOE) under the Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/UPM/02/9). We also wish to express our gratitude to Mataram University, Indonesia, for providing partial funding assistance.

6. References

Abdollahi, A., Akbari, S., & Maimani, H.R. (2006). Non-commuting graph of a group. *Journal of Algebra*, 298(2): 468 – 492.

Aschbacher, M. (2000). Finite Group Theory, pp. 1 – 6, Cambridge, UK: Cambridge University Press.

Brouwer, A. E., & Haemers W. H. (2012). Spectra of Graphs, pp. 1 – 19, New York, USA: Springer-Verlag.

Dutta, J. & Nath, R. K. (2018). On laplacian energy of non-commuting graphs of finite groups. *Journal of Linear and Topological Algebra*, 7(2): 121 – 132.

Fasfous, W. N. T., & Nath, R. K. (2020). Spectrum and energy of non-commuting graphs of finite groups. 1 – 22. Retrieved from *ArXiv:2002.10146v1*

Gutman, I. (1978). The energy of graph. *Ber. Math. Statist. Sekt. Forschungszenturm Graz*, 103: 1 – 22.

Gutman, I., Abreau, N. M. M. D., Vinagre, C. T. M., Bonifacio, A.S., & Radenkovic, S. (2008). Relation between energy and laplacian energy. *MATCH Communications in Mathematical and in Computer Chemistry,* 59: 343 – 354.

Hosamani, S. M., & Ramane, H. S. (2016). On degree sum energy of a graph. *European Journal of Pure and Applied Mathematics*, 9(3): 340 – 345.

Jog, S. R., & Kotambari, R. (2016). Degree sum energy of some graphs. *Annals of Pure and Applied Mathematics*, 11(1): 17-27.

Khasraw, S. M. S., Ali, I. D., & Haji, R. R. (2020). On the non-commuting graph of dihedral group, *Electronic Journal of Graph Theory and Applications*, 8(2): 233 – 239.

Mahmoud, R., Sarmin, N. H., & Erfanian, A. (2017). On the energy of non-commuting graph of dihedral groups. *AIP Conference Proceedings,* 1830: 070011.

Ramane, H. S., Revankar, D. S., & Patil, J. B. (2013). Bounds for the degree sum eigenvalues and degree sum energy of a graph. *International Journal of Pure and Applied Mathematical Sciences,* 6(2): 161-167.

Ramane, H. S., & Shinde, S. S. (2017). Degree exponent polynomial of graphs obtained by some graph operations. *Electronic Notes in Discrete Mathematics*, 63: 161 – 168.

DOI: https://doi.org/10.22452/mjs.sp2022no.1.5

MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021
Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 40-46 (September 2022)
https://mjs.um.edu.my

DEGREE EXPONENT SUM ENERGY OF COMMUTING GRAPH FOR DIHEDRAL GROUPS

Mamika Ujianita Romdhini[1ac], Athirah Nawawi[2ab]*, Chen Chuei Yee[3a]

Abstract: For a finite group G and a nonempty subset X of G, we construct a graph with a set of vertex X such that any pair of distinct vertices of X are adjacent if they are commuting elements in G. This graph is known as the commuting graph of G on X, denoted by $\Gamma_G[X]$. The degree exponent sum (DES) matrix of a graph is a square matrix whose (p, q)-th entry is $d_{v_p}{}^{d_{v_q}} + d_{v_q}{}^{d_{v_p}}$ whenever p is different from q, otherwise, it is zero, where d_{v_p} (or d_{v_q}) is the degree of the vertex v_p (or vertex, v_q) of a graph. This study presents results for the DES energy of commuting graph for dihedral groups of order $2n$, using the absolute eigenvalues of its DES matrix.

Keywords: *Commuting graph, dihedral group, degree exponent sum matrix, the energy of a graph.*

1. Introduction

A group is a set of elements associated by a binary operation, which satisfies closure property, has a unique identity element, and unique inverses for each element in the group (Aschbacher, 2000). Suppose now that G is any finite group and $Z(G)$ is the center of G. The commuting graph of G on a nonempty subset X of G, denoted by $\Gamma_G[X]$, is a graph whose vertex set is X, and two distinct vertices are adjacent if they commute in G. If $X = G \backslash Z(G)$, then we write $\Gamma_G \coloneqq \Gamma_G[X]$ and Γ_G is called the commuting graph of G. This graph is a simple undirected graph introduced by Brauer and Fowler (1955).

The commuting graph of G on X has been further associated with the spectral graph theory, where matrices are associated with a graph. The adjacency matrix $A(\Gamma_G[X]) = [a_{pq}]$ of $\Gamma_G[X]$, is an $n \times n$ matrix, defined by its entries a_{pq} are equal to 1 if there is an edge between the vertices v_p, v_q, and 0 otherwise. Clearly, $A(\Gamma_G[X])$ is a symmetric matrix with zero diagonal entries since $\Gamma_G[X]$ is a simple graph. For real numbers λ and an $n \times n$ identity matrix I_n, the characteristic polynomial of $\Gamma_G[X]$ is defined by $P_{A(\Gamma_G[X])}(\lambda) = \det(\lambda I_n - A(\Gamma_G[X]))$. The roots of $P_{A(\Gamma_G[X])}(\lambda) = 0$ are $\lambda_1, \lambda_2, \ldots, \lambda_n$ and are known as the eigenvalues of $\Gamma_G[X]$.

By the definition of adjacency matrix, the (ordinary) spectrum of the finite graph $\Gamma_G[X]$ is the list of eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$, with their respective multiplicities $k_1, k_2, \ldots, k_m$ as exponents, denoted by $Spec(\Gamma_G[X]) = \left\{\lambda_1^{(k_1)}, \lambda_2^{(k_2)}, \ldots, \lambda_m^{(k_m)}\right\}$. Furthermore, the energy of $\Gamma_G[X]$ is the sum of the absolute eigenvalues of $A(\Gamma_G[X])$, which is $E(\Gamma_G[X]) = \sum_{i=1}^{n} |\lambda_i|$. Other than that, Gutman found this definition in 1978 by considering a chemical molecule as a graph and estimating the π-electron energy.

Several studies regarding the commuting graph involve the spectrum and energy of its adjacency matrix. For finite non-abelian groups, Dutta and Nath (2017a) and Dutta and Nath (2017b) have described the formula for the spectrum of the commuting graph. Laplacian spectrum, signless Laplacian spectrum and their corresponding energies of the commuting graph of dihedral groups can be found in Dutta and Nath (2018) and Dutta and Nath (2021). Furthermore, the discussion of the adjacency energy for the subgroup graph of the dihedral group has been done by Abdussakir *et al.* (2019). In 2022, Sharafdini *et al.* discussed the commuting graph for some finite groups with abelian centralizers and found the energy for some particular families of AC groups.

Apart from the adjacency matrix, Laplacian matrix, and signless Laplacian matrix, another matrix related to the degree of vertices in a graph defined by Basavanagoud and Eshwarachandra in 2020 is the principal focus point here, called the degree exponent sum (DES) matrix. A limited number of studies central to the DES matrices for the commuting graph have been found. This fact motivates us to have a detailed description of the DES energy for the commuting graphs of G.

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA. E-mail: s57042@student.upm.edu.my[1], athirah@upm.edu.my[2], cychen@upm.edu.my[3]
[b]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA.
[c]Department of Mathematics, Faculty of Mathematics and Natural Science, Universitas Mataram, Mataram, 83125, INDONESIA. E-mail: mamika@unram.ac.id[1]

*Corresponding Author: athirah@upm.edu.my

Received: January 21, 2022
Accepted: April 13, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.6

In this paper, we focus on $\boldsymbol{\Gamma_G[X]}$ constructed on the non-abelian dihedral group of order $\boldsymbol{2n, n \geq 3}$, denoted as $\boldsymbol{D_{2n} = \langle a, b : a^n = b^2 = e, bab = a^{-1}\rangle}$. The center of $\boldsymbol{D_{2n}}$, $\boldsymbol{Z(D_{2n})}$ is either $\boldsymbol{\{e\}}$ **if n is odd** or $\boldsymbol{\{e, a^{\frac{n}{2}}\}}$ **if n is even**. The centralizer of the element $\boldsymbol{a^i}$ in the group $\boldsymbol{D_{2n}}$ is $\boldsymbol{C_{D_{2n}}(a^i) = \{a^i : 1 \leq i \leq n\}}$ and for the element $\boldsymbol{a^ib}$ is either $\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^ib\}}$, if $\boldsymbol{n}$ is odd or $\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^{\frac{n}{2}}, a^ib, a^{\frac{n}{2}+i}b\}}$, **if n is even**.

2. Preliminaries

Now, we are ready to see the definition of the degree exponent sum (DES) matrix, considering $\boldsymbol{d_{v_p}}$ as the degree of $\boldsymbol{v_p}$, which is the number of vertices adjacent to $\boldsymbol{v_p}$. Moreover, if every vertex has the same degree $\boldsymbol{r}$, then the graph is called $\boldsymbol{r}$-regular graph.

Definition 2.1. (Basavanagoud & Eshwarachandra, 2020) The DES matrix of order $\boldsymbol{n \times n}$ associated with $\boldsymbol{\Gamma_G[X]}$ is given by $\boldsymbol{DES(\Gamma_G[X]) = [des_{pq}]}$ whose $\boldsymbol{(p, q)}$-th entry is

$$\boldsymbol{des_{pq} = \begin{cases} {d_{v_p}}^{d_{v_q}} + {d_{v_q}}^{d_{v_p}}, & \text{if } p \neq q \\ 0, & \text{if } p = q \end{cases}.}$$

Therefore, the DES energy of $\boldsymbol{\Gamma_G[X]}$ can be defined as follows:

$$\boldsymbol{E_{DES}(\Gamma_G[X]) = \sum_{i=1}^{n} |\lambda_i|},$$

where $\boldsymbol{\lambda_1, \lambda_2, \cdots, \lambda_n}$ are the eigenvalues (not necessarily distinct) of $\boldsymbol{DES(\Gamma_G[X])}$.

In this section, we include some previous results beneficial for the next section. The following lemma is important for computing the characteristic polynomial of the commuting graph $\boldsymbol{\Gamma_G}$.

Lemma 2.1: (Ramane & Shinde, 2017) If $\boldsymbol{a, b, c}$ and $\boldsymbol{d}$ are real numbers, and $\boldsymbol{J_n}$ is an $\boldsymbol{n \times n}$ matrix whose all elements are equal to 1, then the determinant of the $\boldsymbol{(n_1 + n_2) \times (n_1 + n_2)}$ matrix of the form

$$\boldsymbol{\begin{vmatrix} (\lambda + a)I_{n_1} - aJ_{n_1} & -cJ_{n_1 \times n_2} \\ -dJ_{n_2 \times n_1} & (\lambda + b)I_{n_2} - bJ_{n_2} \end{vmatrix}},$$

can be simplified as given in the following expression $\boldsymbol{(\lambda + a)^{n_1 - 1}(\lambda + b)^{n_2 - 1}\big((\lambda - (n_1 - 1)a)(\lambda - (n_2 - 1)b) - n_1 n_2 cd\big)}$,
where $\boldsymbol{1 \leq n_1, n_2 \leq n}$ and $\boldsymbol{n_1 + n_2 = n}$.

A graph with $\boldsymbol{n}$ vertices, where every vertex is adjacent to all other vertices, is called a complete graph $\boldsymbol{K_n}$ and the complement of $\boldsymbol{K_n}$ is denoted by $\boldsymbol{\overline{K}_n}$. The following lemma is the result of the spectrum of $\boldsymbol{K_n}$, which is useful in computing $\boldsymbol{E_{DES}(\Gamma_G[X])}$.

Lemma 2.2: (Brouwer & Haemers, 2010) If $\boldsymbol{K_n}$ is the complete graph on $\boldsymbol{n}$ vertices, then its adjacency matrix is $\boldsymbol{J_n - I_n}$ and the spectrum of $\boldsymbol{K_n}$ is $\boldsymbol{\{(n-1)^{(1)}, (-1)^{(n-1)}\}}$.

3. Main Results

This section presents several results on the degree exponent sum (DES) energy of the commuting graph on the dihedral group of order $\boldsymbol{2n}$. We divide $\boldsymbol{n}$ into two cases, namely when $\boldsymbol{n}$ is odd and $\boldsymbol{n}$ is even. This is strictly for $\boldsymbol{n \geq 3}$ since the dihedral group is abelian for $\boldsymbol{n = 1}$ and $\boldsymbol{n = 2}$.

Recall that the dihedral group of order $\boldsymbol{2n}$ is $\boldsymbol{D_{2n} = \langle a, b : a^n = b^2 = e, bab = a^{-1}\rangle}$. Let the set of rotation elements of $\boldsymbol{D_{2n}}$, which are not members of $\boldsymbol{Z(D_{2n})}$, be written as $\boldsymbol{G_1 = \{a^i : 1 \leq i \leq n\} \backslash Z(D_{2n})}$ and $\boldsymbol{G_2 = \{a^ib : 1 \leq i \leq n\}}$ be the set of reflection elements of $\boldsymbol{D_{2n}}$. The following is the result of the degree of each vertex in the commuting graph of $\boldsymbol{D_{2n}}$.

Theorem 3.1: Let $\boldsymbol{\Gamma_{D_{2n}}}$ be the commuting graph of $\boldsymbol{D_{2n}}$. Then,

1. the degree of $\boldsymbol{a^i}$ in $\boldsymbol{\Gamma_{D_{2n}}}$, denoted as $\boldsymbol{d_{a^i}}$, is given by
$$\boldsymbol{d_{a^i} = \begin{cases} n - 2, & \text{if } n \text{ is odd} \\ n - 3, & \text{if } n \text{ is even} \end{cases}},$$
2. the degree of $\boldsymbol{a^ib}$ in $\boldsymbol{\Gamma_{D_{2n}}}$, denoted as $\boldsymbol{d_{a^ib}}$, is given by
$$\boldsymbol{d_{a^ib} = \begin{cases} 0, & \text{if } n \text{ is odd} \\ 1, & \text{if } n \text{ is even} \end{cases}}.$$

Proof.

1. If $\boldsymbol{n}$ is odd, then $\boldsymbol{Z(D_{2n}) = \{e\}}$. Since $\boldsymbol{C_{D_{2n}}(a^i) = \{a^i : 1 \leq i \leq n\}}$, then $\boldsymbol{d_{a^i} = n - 2}$, removing $\boldsymbol{e}$ and $\boldsymbol{a^i}$ itself. If $\boldsymbol{n}$ is even, then $\boldsymbol{Z(D_{2n}) = \{e, a^{\frac{n}{2}}\}}$. Consequently, we have $\boldsymbol{d_{a^i} = n - 3}$, removing $\boldsymbol{e, a^{\frac{n}{2}}}$, and $\boldsymbol{a^i}$ itself.
2. If $\boldsymbol{n}$ is odd, the element $\boldsymbol{a^ib}$, where $\boldsymbol{1 \leq i \leq n}$, has the centralizer $\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^ib\}}$ of size two, then there is no edge between any pair of vertices in $\boldsymbol{\Gamma_G}$. Therefore, $\boldsymbol{d_{a^ib} = 0}$. If $\boldsymbol{n}$ is even, the centralizer of each element $\boldsymbol{a^ib}$ is given by
$\boldsymbol{C_{D_{2n}}(a^ib) = \{e, a^{\frac{n}{2}}, a^ib, a^{\frac{n}{2}+i}b\}}$, for all $\boldsymbol{1 \leq i \leq n}$.
Then, by excluding $\boldsymbol{e}$ and $\boldsymbol{a^{\frac{n}{2}}}$, which are the central elements in $\boldsymbol{D_{2n}}$, there exists only an edge between the vertices $\boldsymbol{a^ib}$ and $\boldsymbol{a^{\frac{n}{2}+i}b}$ in $\boldsymbol{\Gamma_G}$, for all $\boldsymbol{1 \leq i \leq n}$. Hence, $\boldsymbol{d_{a^ib} = 1}$.

Consequently, the isomorphism of the commuting graph with the common type of graphs can be seen in the following result:

Theorem 3.2: Let $\boldsymbol{X}$ be any nonempty subset of $\boldsymbol{D_{2n}}$.

1. If $\boldsymbol{X = G_1}$, then
$\boldsymbol{\Gamma_{D_{2n}}[X] \cong K_m}$, where $\boldsymbol{m = |G_1|}$.

2. If $\boldsymbol{X = G_2}$, then

$$\Gamma_{D_{2n}}[X] \cong \begin{cases} \bar{K}_n, & \textbf{if } \boldsymbol{n} \textbf{ is odd} \\ \mathbf{1-regular\ graph}, & \textbf{if } \boldsymbol{n} \textbf{ is even} \end{cases}$$

Proof:

1. The centralizer of a^i, for $1 \le i \le n$, is $C_{D_{2n}}(a^i) = \{a^i : 1 \le i \le n\}$ of size n. This implies that every vertex of G_1 is adjacent to all vertices in the set itself. Thus, $\Gamma_{D_{2n}}[G_1] \cong K_m$, where $m = |G_1|$.
2. It follows from Theorem 3.1 that the degree of $a^i b$ in $\Gamma_{D_{2n}}[G_2]$ is all zero for $1 \le i \le n$, where n is odd. Hence, $\Gamma_{D_{2n}}[G_2] \cong \bar{K}_n$, a complement of the complete graph on n vertices. Now, suppose n is even. Again, by Theorem 3.1, the degree of $a^i b$ in $\Gamma_{D_{2n}}[G_2]$ is all 1. This implies that $\Gamma_{D_{2n}}[G_2]$ is disconnected, with each component isomorphic to the 1-regular graph.

We illustrate the two theorems above via the following examples for $n = 4$ and $n = 5$.

Example 1. Let Γ_{D_8} be the commuting graph of D_8, where $D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, $Z(D_8) = \{e, a^2\}$, $G_1 = \{a, a^3\}$, $G_2 = \{b, ab, a^2b, a^3b\}$, $C_{D_8}(b) = \{e, a^2, b, a^2b\} = C_{D_8}(a^2b)$, $C_{D_8}(ab) = \{e, a^2, ab, a^3b\} = C_{D_8}(a^3b)$. Using the information on the centralizer of each element in D_8, the commuting graph of D_8 is as in Figure 1.

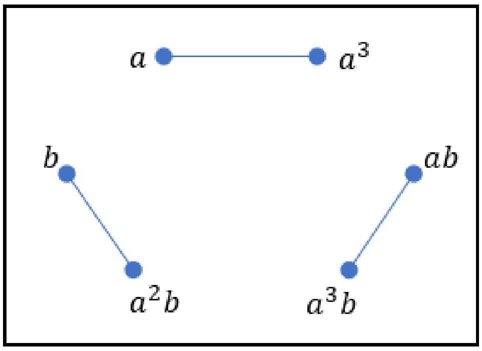


Figure 1. Commuting graph of D_8.

From Figure 1, it is clear that the degree of each vertex a and a^3 is one. In particular, if $X = G_1$, then $\Gamma_{D_8}[G_1]$ is a complete graph on two vertices, K_2. However, for each vertex $a^i b$, for $1 \le i \le 4$, its degree is also one. If $X = G_2$, then $\Gamma_{D_8}[G_2]$ is a disconnected 1-regular graph with two components isomorphic to K_2.

Example 2. Let $\Gamma_{D_{10}}$ be the commuting graph of D_{10}, where $D_{10} = \{e, a, a^2, a^3, a^4 b, ab, a^2b, a^3b, a^4b\}$, $Z(D_{10}) = \{e\}$, $G_1 = \{a, a^2, a^3, a^4\}$, $G_2 = \{b, ab, a^2b, a^3b, a^4b\}$, $C_{D_{10}}(a^ib) = \{a^ib\}$, and $C_{D_{10}}(a^i) = \{a^i : 1 \le i \le 4\}$. Using the information on the centralizer of each element in D_{10}, the commuting graph of D_{10} is as in Figure 2.

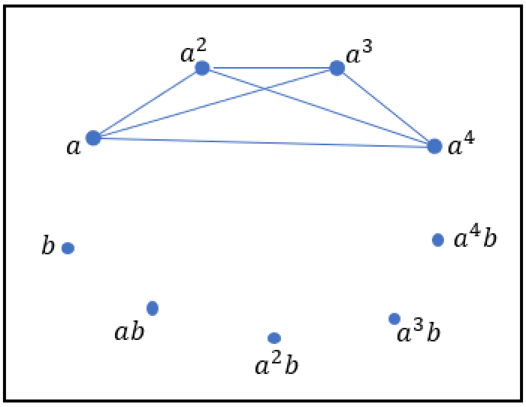


Figure 2. Commuting graph $\Gamma_{D_{10}}$.

From Figure 2, it is clear that the degree of each vertex a^i, where $1 \le i \le 4$ is three. In particular, if $X = G_1$, then $\Gamma_{D_{10}}[G_1]$ is a complete graph on four vertices, K_4. However, for each vertex a^ib, for $1 \le i \le 5$, its degree is zero. If $X = G_2$, then $\Gamma_{D_{10}}[G_2]$ is a disconnected graph with five isolated vertices and isomorphic to the complement of a complete graph on five vertices, $\bar{K}_5$.

Theorem 3.3: Let X be any nonempty subset of D_{2n}.

1. If $X = G_1$, then

$$E_{DES}(\Gamma_{D_{2n}}[X]) = \begin{cases} 4(n-2)^{n-1}, & \textbf{if } \boldsymbol{n} \textbf{ is odd} \\ 4(n-3)^{n-2}, & \textbf{if } \boldsymbol{n} \textbf{ is even} \end{cases}.$$

2. If $X = G_2$, then

$$E_{DES}(\Gamma_{D_{2n}}[X]) = 4(n-1).$$

Proof.

2. **When n is odd**. From Theorem 3.2 (1), $\Gamma_{D_{2n}}[G_1] = K_m$, where $m = |G_1| = n - 1$, removing e in $Z(D_{2n})$. Then, every vertex of $\Gamma_{D_{2n}}[G_1]$ has degree $n - 2$. Subsequently, we can construct an $(n-1) \times (n-1)$ DES matrix of $\Gamma_{D_{2n}}[G_1]$, $DES(\Gamma_{D_{2n}}[G_1]) = [des_{pq}]$ whose (p, q)-th entry is $des_{pq} = (n-2)^{n-2} + (n-2)^{n-2} = 2(n-2)^{n-2}$, for $p \ne q$, and 0 otherwise:

$$DES(\Gamma_{D_{2n}}[G_1])$$
$$= \begin{bmatrix} 0 & 2(n-2)^{n-2} & \cdots & 2(n-2)^{n-2} \\ 2(n-2)^{n-2} & 0 & \cdots & 2(n-2)^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 2(n-2)^{n-2} & 2(n-2)^{n-2} & \cdots & 0 \end{bmatrix}$$

$$= 2(n-2)^{n-2} \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}.$$

In other words, the DES matrix of $\Gamma_{D_{2n}}[G_1]$ is the product of $2(n-2)^{n-2}$ and the adjacency matrix of K_{n-1}. Based on Lemma 2.2, $\boldsymbol{Spec}(\boldsymbol{K_{n-1}})$ is given by $\{(\boldsymbol{n}-\boldsymbol{2})^{(1)}, (-\boldsymbol{1})^{(n-2)}\}$. Since the adjacency energy of $\boldsymbol{K_{n-1}}$ is $|\boldsymbol{n}-\boldsymbol{2}| + (\boldsymbol{n}-\boldsymbol{2})|-\boldsymbol{1}| = \boldsymbol{2}(\boldsymbol{n}-\boldsymbol{2})$, the DES energy of $\boldsymbol{\Gamma_{D_{2n}}[G_1]}$ will be $\boldsymbol{2(n-2)^{n-2}\cdot 2(n-2) = 4(n-2)^{n-1}}$.

When $\boldsymbol{n}$ is even. From Theorem 3.2 (1), $\boldsymbol{\Gamma_{D_{2n}}[G_1] = K_m}$, where $\boldsymbol{m = |G_1| = n-2}$, removing $\boldsymbol{e}$ and $\boldsymbol{a^{\frac{n}{2}}}$ in $\boldsymbol{Z(D_{2n})}$. Then, every vertex of $\boldsymbol{\Gamma_{D_{2n}}[G_1]}$ has degree $\boldsymbol{n-3}$. Consequently, we can construct an $(\boldsymbol{n}-\boldsymbol{2}) \times (\boldsymbol{n}-\boldsymbol{2})$ DES matrix of $\boldsymbol{\Gamma_{D_{2n}}[G_1]}$, $\boldsymbol{DES(\Gamma_{D_{2n}}[G_1]) = [des_{pq}]}$ whose $(\boldsymbol{p},\boldsymbol{q})$-th entry is $\boldsymbol{des_{pq} = (n-3)^{n-3} + (n-3)^{n-3} = 2(n-3)^{n-3}}$, for $\boldsymbol{p \neq q}$, and 0 otherwise:

$$\boldsymbol{DES(\Gamma_{D_{2n}}[G_1])}$$
$$= \begin{bmatrix} 0 & 2(n-3)^{n-3} & \cdots & 2(n-3)^{n-3} \\ 2(n-3)^{n-3} & 0 & \cdots & 2(n-3)^{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ 2(n-3)^{n-3} & 2(n-3)^{n-3} & \cdots & 0 \end{bmatrix}$$

$$= 2(n-3)^{n-3} \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}$$

Thus, the DES matrix of $\boldsymbol{\Gamma_{D_{2n}}[G_1]}$ is the product of $\boldsymbol{2(n-3)^{n-3}}$ and the adjacency matrix of $\boldsymbol{K_{n-2}}$. Based on Lemma 2.2, $\boldsymbol{Spec(K_{n-2})}$ is given by $\{(\boldsymbol{n}-\boldsymbol{3})^{(1)}, (-\boldsymbol{1})^{(n-3)}\}$. Since the adjacency energy of $\boldsymbol{K_{n-2}}$ is $|\boldsymbol{n}-\boldsymbol{3}| + (\boldsymbol{n}-\boldsymbol{3})|-\boldsymbol{1}| = \boldsymbol{2(n-3)}$, the DES energy of $\boldsymbol{\Gamma_{D_{2n}}[G_1]}$ will be $\boldsymbol{2(n-3)^{n-3}\cdot 2(n-3) = 4(n-3)^{n-2}}$.

2. **When $\boldsymbol{n}$ is odd**. From Theorem 3.2 (2), $\boldsymbol{\Gamma_{D_{2n}}[G_2] = \overline{K}_n}$, where $\boldsymbol{n = |G_2|}$. Then, all of the vertices have degree zero. Correspondingly, we can construct an $\boldsymbol{n \times n}$ DES matrix of $\boldsymbol{\Gamma_{D_{2n}}[G_2]}$, $\boldsymbol{DES(\Gamma_{D_{2n}}[G_2]) = [des_{pq}]}$ whose $(\boldsymbol{p},\boldsymbol{q})$-th entry is $\boldsymbol{des_{pq} = 0^0 + 0^0 = 2}$, for $\boldsymbol{p \neq q}$, and 0 otherwise:

$$\boldsymbol{DES(\Gamma_{D_{2n}}[G_2])} = \begin{bmatrix} \mathbf{0} & \mathbf{2} & \cdots & \mathbf{2} \\ \mathbf{2} & \mathbf{0} & \cdots & \mathbf{2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{2} & \mathbf{2} & \cdots & \mathbf{0} \end{bmatrix} = 2\begin{bmatrix} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{1} & \mathbf{1} & \cdots & \mathbf{0} \end{bmatrix}.$$

In other words, $\boldsymbol{DES(\Gamma_{D_{2n}}[G_2]) = 2A(K_n)}$ is the multiple of two adjacency matrices of $\boldsymbol{K_n}$. Thus, $\boldsymbol{E_{DES}(\Gamma_{D_{2n}}[G_2]) = 2(|n-1| + (n-1)|-1|) = 4(n-1)}$.

When $\boldsymbol{n}$ is even. From Theorem 3.2 (2), $\boldsymbol{\Gamma_{D_{2n}}[G_2]}$ is a regular graph with degree one. Then, we can construct an $\boldsymbol{n \times n}$ DES matrix of $\boldsymbol{\Gamma_{D_{2n}}[G_2]}$, $\boldsymbol{DES(\Gamma_{D_{2n}}[G_2]) = [des_{pq}]}$ whose $(\boldsymbol{p},\boldsymbol{q})$-th entry is $\boldsymbol{des_{pq} = 1^1 + 1^1 = 2}$, for $\boldsymbol{p \neq q}$, and 0 otherwise:

$$\boldsymbol{DES(\Gamma_{D_{2n}}[G_2])} = \begin{bmatrix} \mathbf{0} & \mathbf{2} & \cdots & \mathbf{2} \\ \mathbf{2} & \mathbf{0} & \cdots & \mathbf{2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{2} & \mathbf{2} & \cdots & \mathbf{0} \end{bmatrix} = 2\begin{bmatrix} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{1} & \mathbf{1} & \cdots & \mathbf{0} \end{bmatrix}.$$

It implies that $\boldsymbol{DES(\Gamma_{D_{2n}}[G_2]) = 2A(K_n)}$. Thus, $\boldsymbol{E_{DES}(\Gamma_{D_{2n}}[G_2]) = 4(n-1)}$.

The DES energy of the commuting graph $\boldsymbol{\Gamma_{D_{2n}}[X]}$ for $\boldsymbol{X = G_1, G_2}$ are given by the following examples, for $\boldsymbol{n = 4}$ and $\boldsymbol{n = 5}$.

Example 3. In Figure 1, we have shown the commuting graph of $\boldsymbol{D_8}$. When $\boldsymbol{X = G_1}$, since we only have two vertices $\boldsymbol{a}$ and $\boldsymbol{a^3}$, we have a $\boldsymbol{2 \times 2}$ DES matrix of $\boldsymbol{\Gamma_{D_8}[G_1]}$ with the non-diagonal entries are $\boldsymbol{1^1 + 1^1 = 2}$, and the diagonal entries are zero. We then obtain

$$\boldsymbol{DES(\Gamma_{D_8}[G_1])} = \begin{bmatrix} \mathbf{0} & \mathbf{2} \\ \mathbf{2} & \mathbf{0} \end{bmatrix}.$$

Furthermore, the characteristic polynomial of $\boldsymbol{DES(\Gamma_{D_8}[G_1])}$ is $\boldsymbol{P_{DES(\Gamma_{D_8}[G_1])}(\lambda) = \det\left(\lambda I_2 - DES(\Gamma_{D_8}[G_1])\right) = det\begin{bmatrix} \lambda & -2 \\ -2 & \lambda \end{bmatrix} = \lambda^2 - 4}$. It implies that the eigenvalues of $\boldsymbol{DES(\Gamma_{D_8}[G_1])}$ are $\boldsymbol{\lambda = 2}$ and $\boldsymbol{\lambda} = -2$. Therefore, the DES energy of $\boldsymbol{\Gamma_{D_8}[G_1]}$ is $\boldsymbol{E_{DES}(\Gamma_{D_8}[G_1])} = |2| + |-2| = \boldsymbol{4 = 4(4-3)^{4-2}}$.

For the case $\boldsymbol{X = G_2}$, we know that the set of vertices is $\{\boldsymbol{b},\ \boldsymbol{ab},\ \boldsymbol{a^2b},\ \boldsymbol{a^3b}\}$. Here, we have a $\boldsymbol{4 \times 4}$ DES matrix of $\boldsymbol{\Gamma_{D_8}[G_2]}$ with the non-diagonal entries are $\boldsymbol{1^1 + 1^1 = 2}$, while the diagonal entries are zero. Then, we get

$$\boldsymbol{DES(\Gamma_{D_8}[G_2])} = \begin{bmatrix} \mathbf{0} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \mathbf{2} & \mathbf{0} & \mathbf{2} & \mathbf{2} \\ \mathbf{2} & \mathbf{2} & \mathbf{0} & \mathbf{2} \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{0} \end{bmatrix}.$$

Additionally, the characteristic polynomial of $\boldsymbol{DES(\Gamma_{D_8}[G_2])}$ is $\boldsymbol{P_{DES(\Gamma_{D_8}[G_2])}(\lambda) = \det\left(\lambda I_4 - DES(\Gamma_{D_8}[G_2])\right)} = (\boldsymbol{\lambda} + \boldsymbol{2})^3(\boldsymbol{\lambda} - \boldsymbol{6})$. It implies that the eigenvalues of $\boldsymbol{DES(\Gamma_{D_8}[G_2])}$ are $\boldsymbol{\lambda = -2}$ with multiplicity 3 and a single $\boldsymbol{\lambda = 6}$. Therefore, $\boldsymbol{E_{DES}(\Gamma_{D_8}[G_2])} = 3|-2| + |6| = \boldsymbol{12 = 4(4-1)}$.

Example 4. In Figure 2, we have presented the commuting graph of $\boldsymbol{D_{10}}$. For $\boldsymbol{X = G_1}$, we have a $\boldsymbol{4 \times 4}$ DES matrix of $\boldsymbol{\Gamma_{D_{10}}[G_1]}$ with the non-diagonal entries are $\boldsymbol{3^3 + 3^3 = 54}$, while the diagonal entries are zero. We then obtain

$$\boldsymbol{DES(\Gamma_{D_{10}}[G_1]\,)} = \begin{bmatrix} \mathbf{0} & \mathbf{54} & \mathbf{54} & \mathbf{54} \\ \mathbf{54} & \mathbf{0} & \mathbf{54} & \mathbf{54} \\ \mathbf{54} & \mathbf{54} & \mathbf{0} & \mathbf{54} \\ \mathbf{54} & \mathbf{54} & \mathbf{54} & \mathbf{0} \end{bmatrix}$$

DOI: https://doi.org/10.22452/mjs.sp2022no1.6

Furthermore, the characteristic polynomial of $DES(\Gamma_{D_{10}}[G_1])$ is $P_{DES(\Gamma_{D_{10}}[G_1])}(\lambda) = \det\left(\lambda I_4 - DES(\Gamma_{D_{10}}[G_1])\right) = (\lambda+54)^3(\lambda-162)$. It implies that the eigenvalues of $DES(\Gamma_{D_{10}}[G_1])$ are $\lambda = -54$ with multiplicity 3 and a single $\lambda = 162$. Therefore, the DES energy of $\Gamma_{D_{10}}[G_1]$ is $E_{DES}(\Gamma_{D_{10}}[G_1]) = 3|-54| + |162| = 324 = 4(5-2)^{5-1}$.

Additionally, for $X = G_2$, we have a 5×5 DES matrix of $\Gamma_{D_{10}}[G_2]$ with the non-diagonal entries are $0^0 + 0^0 = 2$, and the diagonal entries are zero. We then obtain

$$DES(\Gamma_{D_{10}}[G_2]) = \begin{bmatrix} 0 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

Hence, the characteristic polynomial of $DES(\Gamma_{D_{10}}[G_2])$ is $P_{DES(\Gamma_{D_{10}}[G_2])}(\lambda) = \det\left(\lambda I_5 - DES(\Gamma_{D_{10}}[G_2])\right) = (\lambda+2)^4(\lambda-8)$. It implies that the eigenvalues of $DES(\Gamma_{D_{10}}[G_2])$ are $\lambda = -2$ with multiplicity 4 and $\lambda = 8$ with multiplicity 1. Therefore, $E_{DES}(\Gamma_{D_{10}}[G_2]) = 4|-2| + |8| = 16 = 4(5-1)$.

Theorem 3.4: Let $\Gamma_{D_{2n}}$ be the commuting graph of D_{2n}. Then, the characteristic polynomial of $DES(\Gamma_{D_{2n}})$ is

1. $P_{DES(\Gamma_{D_{2n}})}(\lambda) = \left(\lambda + 2(n-2)^{(n-2)}\right)^{n-2}(\lambda+2)^{n-1}(\lambda^2 - (2(n-1) + 2(n-2)^{n-1})\lambda + 4(n-2)^{n-1}(n-1) - n(n-1))$, for n is odd, while
2. $P_{DES(\Gamma_{D_{2n}})}(\lambda) = \left(\lambda + 2(n-3)^{(n-3)}\right)^{n-3}(\lambda+2)^{n-1}(\lambda^2 - (2(n-1) + 2(n-3)^{n-2})\lambda + 4(n-1)(n-3)^{n-2} - n(n-2)^3)$, for n is even.

Proof.

1. When n is odd, from Theorem 3.1, we have $d_{a^i} = n-2$ and $d_{a^ib} = 0$, for all $1 \le i \le n$. Then, using the fact that $Z(D_{2n}) = \{e\}$, we have $2n-1$ vertices in $\Gamma_{D_{2n}}$. The set of vertices consists of $n-1$ vertices of the form a^i, for $1 \le i \le n-1$, and n vertices of the form a^ib, for $1 \le i \le n$. Consequently, the DES matrix for $\Gamma_{D_{2n}}$ is a $(2n-1)\times(2n-1)$ matrix, $DES(\Gamma_{D_{2n}}) = [des_{pq}]$ whose entries are:
   (i) $des_{pq} = (n-2)^{n-2} + (n-2)^{n-2} = 2(n-2)^{n-2}$, for $p \ne q$, and $1 \le p, q \le n-1$,
   (ii) $des_{pq} = (n-2)^0 + (0)^{n-2} = 1$, for $1 \le p \le n-1$ and $n \le q \le 2n-1$,
   (iii) $des_{pq} = (0)^{n-2} + (n-2)^0 = 1$, for $n \le p \le 2n-1$ and $1 \le q \le n-1$,
   (iv) $des_{pq} = (0)^0 + (0)^0 = 2$, for $p \ne q$, $n \le p \le 2n-1$ and $n \le q \le 2n-1$,
   (v) $des_{pq} = 0$, for $p = q$.

We can construct $DES(\Gamma_{D_{2n}})$ as follows:

$DES(\Gamma_{D_{2n}})$

$$= \left[\begin{array}{cccc|cccc} 0 & 2(n-2)^{(n-2)} & \cdots & 2(n-2)^{(n-2)} & 1 & 1 & \cdots & 1 \\ 2(n-2)^{(n-2)} & 0 & \cdots & 2(n-2)^{(n-2)} & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2(n-2)^{(n-2)} & 2(n-2)^{(n-2)} & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & 1 & \cdots & 1 & 0 & 2 & \cdots & 2 \\ 1 & 1 & \cdots & 1 & 2 & 0 & \cdots & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 & 2 & 2 & \cdots & 0 \end{array}\right]$$

$$= \begin{bmatrix} 2(n-2)^{(n-2)}(J_{n-1} - I_{n-1}) & J_{(n-1)\times n} \\ J_{n\times(n-1)} & 2(J_n - I_n) \end{bmatrix}$$

$$= \begin{bmatrix} T_1 & T_2 \\ T_3 & T_4 \end{bmatrix}.$$

In the current case, $DES(\Gamma_{D_{2n}})$ is divided into four blocks, where the first block is T_1, which is a block of $(n-1)\times(n-1)$ matrix with zero diagonal and all non-diagonal entries as $2(n-2)^{(n-2)}$. In the next two blocks, we have T_2 and T_3 matrices, which are of the size $(n-1)\times n$ and $n\times(n-1)$, respectively, whose all entries are equal to one. The last block is T_4, which is an $n\times n$ matrix with zero diagonal, and all non-diagonal entries are equal to two. Then, we obtain the characteristic polynomial of $DES(\Gamma_{D_{2n}})$ from the following determinant

$$P_{DES(\Gamma_{D_{2n}})}(\lambda) = \left|\lambda I_{2n-1} - DES(\Gamma_{D_{2n}})\right|$$

$$= \begin{vmatrix} \left(\lambda + 2(n-2)^{(n-2)}\right)I_{n-1} - 2(n-2)^{(n-2)}J_{n-1} & -J_{(n-1)\times n} \\ -J_{n\times(n-1)} & (\lambda+2)I_n - 2J_n \end{vmatrix}$$

.

By using Lemma 2.1, with $a = 2(n-2)^{(n-2)}$, $b = 2$, $c = 1$, $d = 1$, $n_1 = n-1$ and $n_2 = n$, we get the required result.

2. When n is even, using Theorem 3.1, we know that $d_{a^i} = n-3$ and $d_{a^ib} = 1$, for all $1 \le i \le n$. Then, using the fact that $Z(D_{2n}) = \{e, a^{\frac{n}{2}}\}$, we have $2n-2$ vertices in $\Gamma_{D_{2n}}$. The set of vertices consists of $n-2$ vertices of the form a^i, with $i \ne n, \frac{n}{2}$ and n vertices of the form a^ib, for $1 \le i \le n$. Correspondingly, the DES matrix for $\Gamma_{D_{2n}}$ is a $(2n-2)\times(2n-2)$ matrix, $DES(\Gamma_{D_{2n}}) = [des_{pq}]$ whose entries are:
   (i) $des_{pq} = (n-3)^{n-3} + (n-3)^{n-3} = 2(n-3)^{n-3}$, for $p \ne q$, and $1 \le p, q \le n-2$,
   (ii) $des_{pq} = (n-3)^1 + (1)^{n-3} = n-2$, for $1 \le p \le n-2$ and $n-1 \le q \le 2n-2$,
   (iii) $des_{pq} = (1)^{n-3} + (n-3)^1 = n-2$, for $n-1 \le p \le 2n-2$ and $1 \le q \le n-2$,
   (iv) $des_{pq} = (1)^1 + (1)^1 = 2$, for $p \ne q$, $n-1 \le p \le 2n-2$ and $n-1 \le q \le 2n-2$,
   (v) $des_{pq} = 0$, for $p = q$.

We can construct $DES(\Gamma_{D_{2n}})$ as the following:

$$\left[\begin{array}{cccc:cccc} 0 & 2(n-3)^{(n-3)} & \cdots & 2(n-3)^{(n-3)} & n-2 & n-2 & \cdots & n-2 \\ 2(n-3)^{(n-3)} & 0 & \cdots & 2(n-3)^{(n-3)} & n-2 & n-2 & \cdots & n-2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2(n-3)^{(n-3)} & 2(n-3)^{(n-3)} & \cdots & 0 & n-2 & n-2 & \cdots & n-2 \\ \hdashline n-2 & n-2 & \cdots & n-2 & 0 & 2 & \cdots & 2 \\ n-2 & n-2 & \cdots & n-2 & 2 & 0 & \cdots & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n-2 & n-2 & \cdots & n-2 & 2 & 2 & \cdots & 0 \end{array}\right]$$

$$= \begin{bmatrix} 2(n-3)^{(n-3)}(J_{n-2} - I_{n-2}) & (n-2)J_{(n-2)\times n} \\ (n-2)J_{n\times(n-2)} & 2(J_n - I_n) \end{bmatrix}$$

$$= \begin{bmatrix} U_1 & U_2 \\ U_3 & U_4 \end{bmatrix}.$$

In the current case, $DES(\Gamma_{D_{2n}})$ is divided into four blocks, where the first block we have U_1 which is a block of $(n-2)\times(n-2)$ matrix with zero diagonal and all non-diagonal entries as $2(n-3)^{(n-3)}$. The next two blocks are U_2 and U_3, which are of the size $(n-2)\times n$ and $n\times(n-2)$, respectively, whose all entries are equal to $n-2$. The last block is U_4, which is an $n\times n$ matrix with zero diagonal, and all non-diagonal entries are equal to two. Then, we obtain the characteristic polynomial of $DES(\Gamma_{D_{2n}})$ from the following determinant

$$P_{DES(\Gamma_{D_{2n}})}(\lambda) = |\lambda I_{2n-2} - DES(\Gamma_{D_{2n}})|$$

$$= \begin{vmatrix} (\lambda + 2(n-3)^{(n-3)})I_{n-2} - 2(n-3)^{(n-3)}J_{n-2} & -(n-2)J_{(n-2)\times n} \\ -(n-2)J_{n\times(n-2)} & (\lambda+2)I_n - 2J_n \end{vmatrix}.$$

By using Lemma 2.1, with $a = 2(n-3)^{(n-3)}, b = 2, c = n-2,\ d = n-2,\ n_1 = n-2$ and $n_2 = n$, we obtain the result.

The illustration of the above theorem is given by the following examples for $n = 4$ and $n = 5$.

Example 5. In Example 1, we obtained the commuting graph of D_8. Since the degree of each vertex is one, then we will have a 6×6 DES matrix of Γ_{D_8} as follows:

$$DES(\Gamma_{D_8}) = \begin{bmatrix} 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}.$$

Hence, the characteristic polynomial of $DES(\Gamma_{D_8})$ is $P_{DES(\Gamma_{D_8})}(\lambda) = \det\left(\lambda I_6 - DES(\Gamma_{D_8})\right) = (\lambda+2)(\lambda+2)^3(\lambda^2 - 8\lambda - 20) = (\lambda+2)^5(\lambda - 10)$. Using Maple™, we confirmed that the eigenvalues of $DES(\Gamma_{D_8})$ are $\lambda = -2$ with multiplicity 5 and a single $\lambda = 10$. Therefore, $E_{DES}(\Gamma_{D_8}) = 5|-2| + |10| = 20$.

Example 6. In Example 2, we have presented the commuting graph of D_{10}. Then, we have a 9×9 DES matrix of $\Gamma_{D_{10}}$ as follows:

$$DES(\Gamma_{D_{10}}) = \left[\begin{array}{cccc:ccccc} 0 & 54 & 54 & 54 & 1 & 1 & 1 & 1 & 1 \\ 54 & 0 & 54 & 54 & 1 & 1 & 1 & 1 & 1 \\ 54 & 54 & 0 & 54 & 1 & 1 & 1 & 1 & 1 \\ 54 & 54 & 54 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hdashline 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 2 & 0 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 2 & 2 & 0 & 2 & 2 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 0 \end{array}\right].$$

Hence, the characteristic polynomial of $DES(\Gamma_{D_{10}})$ is $P_{DES(\Gamma_{D_{10}})}(\lambda) = \det\left(\lambda I_9 - DES(\Gamma_{D_{10}})\right) = (\lambda + 54)^3\,(\lambda+2)^4(\lambda^2 - 170\lambda + 1276)$. Using Maple™, we confirmed that the eigenvalues of $DES(\Gamma_{D_{10}})$ are $\lambda = -54$ with multiplicity 3, $\lambda = -2$ with multiplicity 4 and $\lambda = 85 \pm 3\sqrt{661}$. Thus, $E_{DES}(\Gamma_{D_{10}}) = 3|-54| + 4|-2| + |85 + 3\sqrt{661}| + |85 - 3\sqrt{661}| = 340$.

Theorem 3.5: Let $\Gamma_{D_{2n}}$ be the commuting graph of D_{2n}. Then
1. for the odd n,
$E_{DES}(\Gamma_{D_{2n}}) = 4(n-2)^{n-1} + 4(n-1)$,
2. and for the even n,

$$E_{DES}(\Gamma_{D_{2n}}) = \begin{cases} 20, & \text{if } n = 4 \\ 4(n-3)^{n-2} + 4(n-1), & \text{if } n > 4 \end{cases}.$$

Proof.

1. By Theorem 3.4 (1) for the odd n, the characteristic polynomial of $DES(\Gamma_{D_{2n}})$ has four eigenvalues, with the first eigenvalue is $\lambda_1 = -2(n-2)^{n-2}$ of multiplicity $n-2$, and the second eigenvalue is $\lambda_2 = -2$ of multiplicity $n-1$. The quadratic formula gives the other two eigenvalues, which are $\lambda_3, \lambda_4 = (n-2)^{n-1} + (n-1) \pm \sqrt{\left((n-2)^{n-1} - (n-1)\right)^2 + n(n-1)}$, and both of them are positive real numbers. Hence, the DES energy for $\Gamma_{D_{2n}}$ is
$$E_{DES}(\Gamma_{D_{2n}}) = (n-2)|-2(n-2)^{n-2}| + (n-1)|-2|$$
$$+ \left|(n-2)^{n-1} + (n-1) \pm \sqrt{\left((n-2)^{n-1} - (n-1)\right)^2 + n(n-1)}\right|$$
$$= 2(n-2)^{n-1} + 2(n-1) + 2(n-2)^{n-1} + 2(n-1)$$
$$= 4(n-2)^{n-1} + 4(n-1).$$

2. By Theorem 3.4 (2) for the even n, the characteristic polynomial of $DES(\Gamma_{D_{2n}})$ has four eigenvalues, with the first eigenvalue is $\lambda_1 = -2(n-3)^{n-3}$ of multiplicity $n-3$, and the second eigenvalue is $\lambda_2 = -2$ of multiplicity $n-1$. The quadratic formula gives the other two eigenvalues, which leads to two cases. First, when $n = 4$, they are a positive real number, and the other is negative. It is evident from Example 5 that $E_{DES}(\Gamma_{D_{2n}}) = 20$. Meanwhile, for $n > 4$, the last two eigenvalues are positive real numbers given by $\lambda_3, \lambda_4 = (n-3)^{n-2} +$

DOI: https://doi.org/10.22452/mjs.sp2022no1.6

$$(n-1) \pm \sqrt{\left((n-3)^{n-2}-(n-1)\right)^2+n(n-2)^3}.$$

Thus, the DES energy for $\Gamma_{D_{2n}}$ is

$$E_{DES}\left(\Gamma_{D_{2n}}\right) = (n-3)\left|-2(n-3)^{n-3}\right| + (n-1)|-2|$$
$$+\left|(n-3)^{n-2}+(n-1)\right.$$
$$\left.\pm\sqrt{\left((n-3)^{n-2}-(n-1)\right)^2+n(n-2)^3}\right|$$
$$= 4(n-3)^{n-2}+4(n-1).$$

4. Conclusion

This paper has given the general formula of degree exponent sum (DES) energy of commuting graphs for dihedral groups. In particular, $E_{DES}\left(\Gamma_{D_{2n}}\right) = 4(n-2)^{n-1} + 4(n-1)$ when n is odd. On the other hand, there are two cases for n is even, namely $E_{DES}\left(\Gamma_{D_{2n}}\right) = 20$ if $n = 4$ and $E_{DES}\left(\Gamma_{D_{2n}}\right) = 4(n-3)^{n-2} + 4(n-1)$ if $n > 4$. This happens as a result of the difference between the quadratic polynomial roots, which is a part of the corresponding characteristic polynomial of $DES\left(\Gamma_{D_{2n}}\right)$.

5. Acknowledgements

This research has been supported by the Ministry of Education (MOE) under the Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/UPM/02/9). We also wish to express our gratitude to Mataram University, Indonesia, for providing partial funding assistance.

6. References

Abdussakir, Akhadiyah, D. A., Layali, A., & Putra, A. T. (2019). The adjacency spectrum of subgroup graphs of dihedral group. IOP Conference Series: Earth and Environmental Science. 243 012042.

Aschbacher, M. (2000). Finite Group Theory, pp. 1 – 6, Cambridge, UK: Cambridge University Press.

Basavanagoud, B., & Eshwarachandra, C. (2020). Degree exponent sum energy of a graph. *Gulf Journal of Mathematics,* 8(1): 52 – 70.

Brauer, R., & Fowler, K.A. (1955). On groups of even order. *Annals of Mathematics*, 62(3): 565 – 583.

Brouwer, A.E., & Haemers W.H. (2012). Spectra of Graphs, pp. 1 – 19, New York, USA: Springer-Verlag.

Dutta, J. & Nath, R. K. (2017a). Spectrum of commuting graphs of some classes of finite groups. *Matematika*, 33(1): 87 – 95.

Dutta, J. & Nath, R. K. (2017b). Finite groups whose commuting graphs are integral, *Matematički Vesnik,* 69(3): 226 – 230.

Dutta, J. & Nath, R. K. (2018). Laplacian and signless Laplacian spectrum of commuting graphs of finite groups. *Khayyam Journal of Mathematics*, 4(1): 77 – 87.

Dutta, P. & Nath, R. K. (2021). Various energies of commuting graphs of some super integral groups. *Indian Journal of Pure and Applied Mathematics*, 52(1): 1 – 10.

Gutman, I. (1978). The energy of graph. *Ber. Math. Statist. Sekt. Forschungszenturm Graz*, 103: 1 – 22.

Sharafdini, R., Nath, R. K., & Darbandi, R. (2022). Energy of commuting graph of finite AC-groups. *Proyecciones Journal of Mathematics*, 41(1): 263 – 273.