

ISSN:2636-7467(Online)

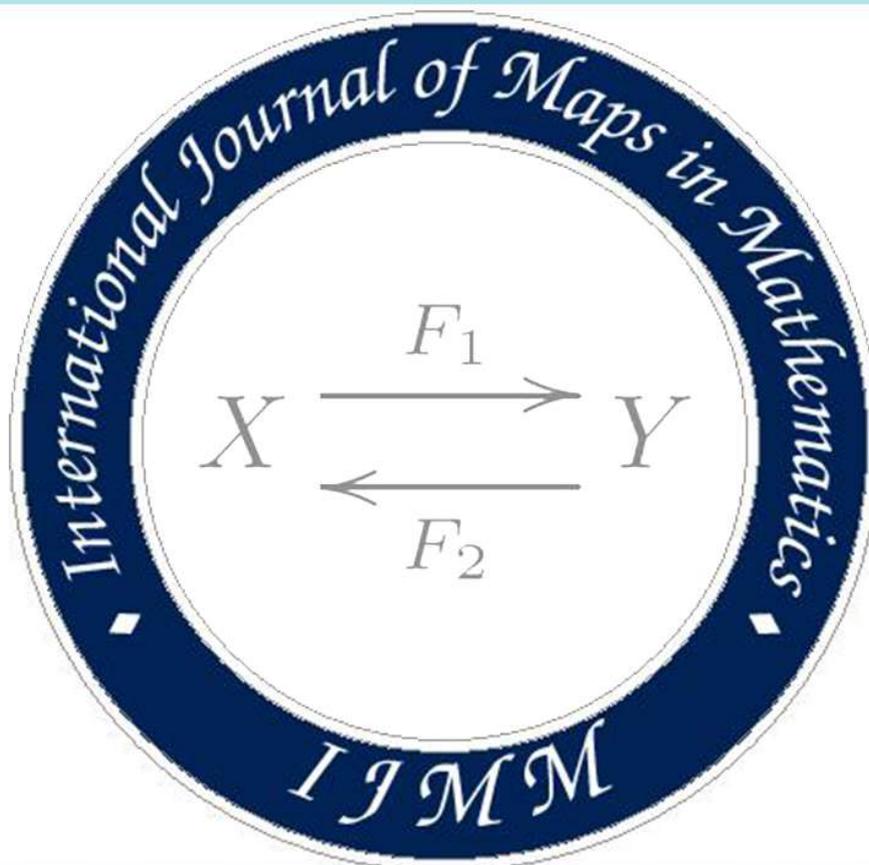
international journal of
MAPS IN MATHEMATICS

Volume 4
Issue 1
2021

Editor in chief

Bayram SAHIN

Ege University, Izmir, TURKEY



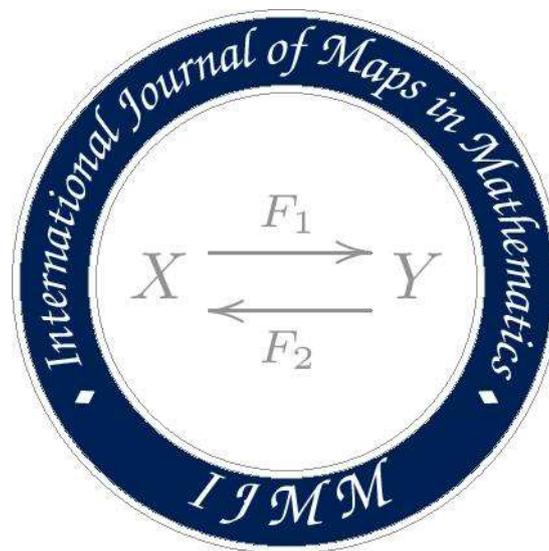
International Journal of Maps in Mathematics is a fully refereed journal devoted to publishing recent results obtained in the research areas of maps in mathematics

www.journalmim.com

VOLUME 4 ISSUE 1
ISSN 2636-7467

March 2021
<https://www.journalmim.com>

International Journal of Maps in Mathematics



Editor-in-Chief

Bayram Sahin
Department of Mathematics, Faculty of Science, Ege University, Izmir, Turkey
journalofmapsinmathematics@gmail.com

Managing Editor

Arif Gursoy
Department of Mathematics, Faculty of Science, Ege University, Izmir, Turkey
arif.gursoy@ege.edu.tr

Editorial Board

Syed Ejaz Ahmed
Brock University, Canada

Kamil Rajab Ayda-zade
Azerbaijan National Academy of Sciences, Azerbaijan

Erdal Ekici
Canakkale Onsekiz Mart University, Turkey

Arif Gursoy
Ege University, Turkey

Zulfiqar Habib
COMSATS Institute of Information Technology, Pakistan

Vatan Karakaya
Yildiz Technical University, Turkey

Andrey L. Karchevsky
Sobolev Mathematical Institute, Russia

Selcuk Kutluay
Inonu University, Turkey

Jae Won Lee
Gyeongsang National University, Republic of Korea

Jung Wook Lim
Kyungpook National University, Republic of Korea

Takashi Noiri
Yatsushiro College of Technology, Japan

Aldo Figallo Orellano
Universidad Nacional del Sur, Argentina

Bayram Sahin
Ege University, Turkey

Ali Taghavi
University of Mazandaran, Iran

Adnan Tercan
Hacettepe University, Turkey

Gabriel Eduard Vilcu
Petroleum-Gas University of Ploiesti, Romania

Technical Assistants

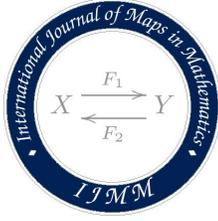
Ibrahim Senturk

Deniz Poyraz

Department of Mathematics, Faculty of Science, Ege
University, Izmir, Turkey

Department of Mathematics, Faculty of Science, Ege
University, Izmir, Turkey

This page intentionally left blank



International Journal of Maps in Mathematics

Volume 4, Issue 1, 2021, Pages:1

ISSN: 2636-7467 (Online)

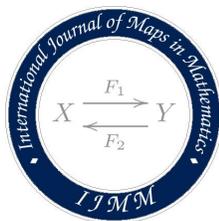
www.journalmim.com

EDITORIAL

BAYRAM ŞAHİN 

Our journal INTERNATIONAL JOURNAL OF MAPS IN MATHEMATICS (IJMM) has completed three years. The year 2020 has been a tough year for us as for everyone. Still, the year 2020 was a year of some important developments for our journal. In 2020, IJMM has been included in the lists by international important indexes MATHSCINET (Mathematical Reviews), Road, Journal Factor, World Catalog of Scientific Journal, Scientific Indexing Services, Journals Directory. IJMM will continue to be the best platform for scientists conducting research in the fields determined by the journal, with an emphasis on quality.

We would like to thank our authors, referees, editorial board, technical team and you, our readers, who contributed to our journal during this period. We wish everyone a happy and healthy new year.



WEYL CONNECTION ON TANGENT BUNDLE OF HYPERSURFACE

RABIA CAKAN AKPINAR *

ABSTRACT. In this paper, we determine the complete lift of weyl connection to tangent bundle of hypersurface. And we obtain some certain results regarding to the tangent bundle.

Keywords: Hypersurface, Weyl connection

2010 Mathematics Subject Classification: 53B25, 53B05.

1. INTRODUCTION

Let M be an m -dimensional Riemannian manifold with a linear connection $\widehat{\nabla}$. Wong obtained some properties of a recurrent tensor field K of type (r, s) on a manifold M endowed with a linear connection $\widehat{\nabla}$. A non zero tensor field K on manifold M is said to be recurrent if there exist a 1-form such that $\widehat{\nabla}K = \omega \otimes K$ [15]. An linear connection $\overline{\nabla}$ on a Riemannian manifold with Riemannian metric \widehat{g} is called a recurrent metric connection if there exist a diferentiable 1-form ω such that

$$(\overline{\nabla}_{\widehat{X}}\widehat{g})(\widehat{Y}, \widehat{Z}) = \widehat{\omega}(\widehat{X})\widehat{g}(\widehat{Y}, \widehat{Z})$$

for any vector fields $\widehat{X}, \widehat{Y}, \widehat{Z}$ in M , ω is called the 1-form of recurrence [10]. The torsion tensor \widehat{T} of $\widehat{\nabla}$ is given by

$$\widehat{T}(\widehat{X}, \widehat{Y}) = \widehat{\nabla}_{\widehat{X}}\widehat{Y} - \widehat{\nabla}_{\widehat{Y}}\widehat{X} - [\widehat{X}, \widehat{Y}] \quad (1.1)$$

Received: 2020.06.24

Accepted: 2020.08.16

* Corresponding author

Rabia Cakan Akpinar; rabiական4@gmail.com; rabiական@kafkas.edu.tr; <https://orcid.org/0000-0001-9885-6373>

for any vector fields \widehat{X} and \widehat{Y} in M . The connection $\widehat{\nabla}$ is symmetric if its torsion tensor \widehat{T} vanishes, i.e., $\widehat{T} = 0$. Then the symmetric $\overline{\nabla}$ connection is called a symmetric recurrent metric connection on M . The Weyl connection is constructed with $\widehat{\omega}$ and \widehat{P} and given by [5], [14]

$$\overline{\nabla}_{\widehat{X}}\widehat{Y} = \widehat{\nabla}_{\widehat{X}}\widehat{Y} - \frac{1}{2} \left(\widehat{\omega}(\widehat{X})\widehat{Y} + \widehat{\omega}(\widehat{Y})\widehat{X} - \widehat{g}(\widehat{X}, \widehat{Y})\widehat{P} \right) \quad (1.2)$$

which satisfies

$$(\overline{\nabla}_{\widehat{X}}\widehat{g})(\widehat{Y}, \widehat{Z}) = \widehat{\omega}(\widehat{X})\widehat{g}(\widehat{Y}, \widehat{Z}) \quad (1.3)$$

for any vector fields \widehat{X} and \widehat{Y} in (M, \widehat{g}) , where $\widehat{\nabla}$ is a Riemannian connection in (M, \widehat{g}) and \widehat{P} is a vector field defined by $\widehat{g}(\widehat{P}, \widehat{X}) = \widehat{\omega}(\widehat{X})$. The Weyl connection is a symmetric recurrent metric connection. The Weyl connection have been studied many authors [2], [6], [12].

The study of differential geometry of tangent bundles was started in the early 1960s. The prolongations called complete, vertical and horizontal lifts of tensor field and connection to tangent bundle have been studied by Yano and Ishihara [17]. The tangent bundle have been studied many authors [3], [9], [13], [16]. Tani [11] improved the theory of hypersurfaces prolonged to tangent bundle with respect to the complete lift of metric tensor of Riemannian manifold. Gözütok and Esin [4] have studied the complete lift of semi-symmetric metric connection to tangent bundle of the hypersurfaces. Khan and his collaborators [7], [8] have studied lifts of quarter-symmetric semi-metric and semi-symmetric semi-metric connections to tangent bundle of the hypersurfaces. This paper is devoted to the study the complete lift of Weyl connection to tangent bundle of the hypersurfaces. And we find certain results on totally umbilical and geodesic to the tangent bundle.

2. PRELIMINARIES

Let M be a Riemannian manifold and we denote by $T(M)$ it is tangent bundle with the projection $\pi_M : T(M) \rightarrow M$ and by $T_p(M)$ its tangent space at a point p of M . $\mathfrak{S}_s^r(M)$ is the set of all tensor fields of type (r, s) in M .

Let $f, t \in \mathfrak{S}_0^0(M)$, $X \in \mathfrak{S}_1^0(M)$, $\omega \in \mathfrak{S}_1^0(M)$, $\varphi \in \mathfrak{S}_1^1(M)$, $g \in \mathfrak{S}_2^0(M)$, $T \in \mathfrak{S}_2^1(M)$ be a function, a vector field, a 1-form, type- (1, 1), type-(0, 2), type-(1, 2) tensor field, respectively. We denote, respectively, by ${}^V f, {}^V X, {}^V \omega, {}^V \varphi, {}^V g, {}^V T$ their vertical lifts and by ${}^C f, {}^C X, {}^C \omega,$

${}^c\varphi, {}^c g, {}^c T$ their complete lifts. This lifts have the properties [17]:

$$\begin{aligned}
[{}^c\hat{X}, {}^c\hat{Y}] &= {}^c [\hat{X}, \hat{Y}] \\
{}^c\hat{\varphi}({}^c\hat{X}) &= {}^c(\hat{\varphi}(\hat{X})) \\
{}^v\hat{\omega}({}^c\hat{X}) &= {}^v(\hat{\omega}(\hat{X})) \\
{}^c\hat{\omega}({}^c\hat{X}) &= {}^c(\hat{\omega}(\hat{X})) \\
{}^c\hat{g}({}^v\hat{X}, {}^c\hat{Y}) &= {}^c\hat{g}({}^c\hat{X}, {}^v\hat{Y}) = {}^v(\hat{g}(\hat{X}, \hat{Y})) \\
{}^c\hat{g}({}^c\hat{X}, {}^c\hat{Y}) &= {}^c(\hat{g}(\hat{X}, \hat{Y})) \\
{}^c\hat{\nabla}_{{}^c\hat{X}} {}^c\hat{Y} &= {}^c(\hat{\nabla}_{\hat{X}}\hat{Y}) \\
{}^c\hat{\nabla}_{{}^c\hat{X}} {}^v\hat{Y} &= {}^v(\hat{\nabla}_{\hat{X}}\hat{Y}) \\
{}^c\hat{T}({}^c\hat{X}, {}^c\hat{Y}) &= {}^c(\hat{T}(\hat{X}, \hat{Y})) \\
{}^c f \quad {}^v t + \quad {}^v f \quad {}^c t &= {}^c(ft).
\end{aligned} \tag{2.4}$$

Let S be an manifold with dimension $(m - 1)$ imbedded differentially as a submanifold in (M, \hat{g}) and denote by $\iota : S \rightarrow M$ its imbedding [11]. The differential mapping $d\iota$ is a mapping from TS into TM , which is called the tangent map of ι , where TS and TM are the tangent bundles of S and M , respectively. The tangent map $d\iota$ is denoted by B . The tangent map of B is denoted by $\tilde{B} : T(TS) \rightarrow T(TM)$.

The hypersurface S is also a Riemannian manifold with the induced metric g defined by $g(X, Y) = \hat{g}(BX, BY)$ for arbitrary $X, Y \in \mathfrak{S}_0^1(S)$. Thus, ∇ is Riemannian connection with the induced connection on (S, g) from $\hat{\nabla}$ defined by

$$\hat{\nabla}_{BX} BY = B(\nabla_X Y) + h(X, Y)N \tag{2.5}$$

for any $X, Y \in \mathfrak{S}_0^1(S)$, where N is unit normal vector field on (S, g) and h is the second fundamental tensor field of (S, g) [11]. Also, the following equality

$$h(X, Y) = g(HX, Y)$$

for any $X, Y \in \mathfrak{S}_0^1(S)$, where $H \in \mathfrak{S}_1^1(S)$.

If h is equal to zero, S is called totally geodesic with respect to ∇ and if h is proportional to g , then S is called totally umbilical with respect to ∇ [11].

3. WEYL CONNECTION ON TANGENT BUNDLE OF HYPERSURFACE

$\overset{\circ}{\nabla}$ is a Weyl connection induced on the hypersurface S from $\overline{\nabla}$, which satisfies the equation

$$\overline{\nabla}_{BX} BY = B\left(\overset{\circ}{\nabla}_X Y\right) + m(X, Y)N \tag{3.6}$$

for $X, Y \in \mathfrak{S}_0^1(S)$, where m is a type-(0, 2) tensor field in S . Defining $M = H - \eta I$, we obtain the equality

$$m(X, Y) = g(MX, Y) \quad (3.7)$$

for any $X, Y \in \mathfrak{S}_0^1(S)$, where I is the unit type-(1, 1) tensor field in S .

If m is equal to zero, then S is called totally geodesic with respect to $\overset{\circ}{\nabla}$ and if m is proportional to g , then S is called totally umbilical with respect to $\overset{\circ}{\nabla}$.

Theorem 3.1. *The connection induced on a hypersurface S of a Riemannian manifold with a Weyl connection with respect to the unit normal is also a Weyl connection.*

Proof. From (1.2) we obtain

$$\bar{\nabla}_{BX} BY = \hat{\nabla}_{BX} BY - \frac{1}{2} \left(\hat{\omega}(BX) BY + \hat{\omega}(BY) BX - \hat{g}(BX, BY) \hat{P} \right) \quad (3.8)$$

for arbitrary vector fields $X, Y \in S$. From equations (2.5), (3.6), (3.8),

$$\begin{aligned} B \left(\overset{\circ}{\nabla}_X Y \right) + m(X, Y) N &= B(\nabla_X Y) + h(X, Y) N - \frac{1}{2} \hat{\omega}(BX) BY \\ &\quad - \frac{1}{2} \hat{\omega}(BY) BX + \frac{1}{2} \hat{g}(BX, BY) (BP + \eta N) \end{aligned} \quad (3.9)$$

where we put $\hat{P} = BP + \eta N$, where η is a function, P is a vector field and ω is a 1-form in S determined by $\omega(X) = \hat{\omega}(BX)$.

By taking the tangential and normal parts from both the sides, we get, respectively,

$$\begin{aligned} \overset{\circ}{\nabla}_X Y &= \nabla_X Y - \frac{1}{2} (\omega(X) Y + \omega(Y) X - g(X, Y) P), \\ m(X, Y) &= h(X, Y) + \frac{1}{2} \eta g(X, Y). \end{aligned}$$

The complete lift ${}^C\hat{g}$ of Riemannian metric \hat{g} is the pseudo-Riemannian metric in TM . Therefore, if we denote by \tilde{g} the induced metric on TS from ${}^C\hat{g}$, then

$$\tilde{g}({}^C X, {}^C Y) = {}^C\hat{g}(\tilde{B} {}^C X, \tilde{B} {}^C Y)$$

for arbitrary vector fields $X, Y \in \mathfrak{S}_0^1(S)$.

Thus, the complete lift ${}^C\hat{\nabla}$ of the Riemannian connection $\hat{\nabla}$ in (M, \hat{g}) is the Riemannian connection in the pseudo-Riemannian manifold $(TM, {}^C\hat{g})$. The complete lift ${}^C\nabla$ of the induced connection ∇ on (S, g) is also the Riemannian connection in $(T(S), \tilde{g})$.

Theorem 3.2. *If \hat{T} is torsion tensor of $\hat{\nabla}$ in (M, \hat{g}) , then ${}^C\hat{T}$ is torsion tensor of ${}^C\hat{\nabla}$ in $(TM, {}^C\hat{g})$ [17].*

Now we obtain the main theorem of this study.

Theorem 3.3. *Let $\bar{\nabla}$ a Weyl connection with respect to $\widehat{\nabla}$ Riemannian connection in (M, \widehat{g}) . Then, ${}^C\bar{\nabla}$ is also a Weyl connection with respect to ${}^C\widehat{\nabla}$ Riemannian connection in $(TM, {}^C\widehat{g})$.*

Proof. Firstly, let's show that ${}^V\widehat{\omega}(\widetilde{B}{}^CX) = \bar{\nabla}(\widehat{\omega}(BX))$ and ${}^C\widehat{\omega}(\widetilde{B}{}^CX) = \bar{C}(\widehat{\omega}(BX))$. In [11], using $\bar{\nabla}(BX) = \widetilde{B}{}^VX$ and $\bar{C}(BX) = \widetilde{B}{}^CX$ for $X \in \mathfrak{S}_0^1(S)$ we get

$$\begin{aligned} {}^V\widehat{\omega}(\widetilde{B}{}^CX) &= {}^V\widehat{\omega}\bar{C}(BX) = \sharp({}^V\widehat{\omega}({}^C\widehat{X})) = \sharp{}^V(\widehat{\omega}(\widehat{X})) = \bar{\nabla}(\widehat{\omega}(BX)), \\ {}^C\widehat{\omega}(\widetilde{B}{}^CX) &= {}^C\widehat{\omega}\bar{C}(BX) = \sharp({}^C\widehat{\omega}({}^C\widehat{X})) = \sharp{}^C(\widehat{\omega}(\widehat{X})) = \bar{C}(\widehat{\omega}(BX)) \end{aligned}$$

for arbitrary $X, Y \in \mathfrak{S}_0^1(S)$. Here, we denote the operation of restriction to $\pi_M^{-1}(\iota(S))$ by \sharp . Also, we denote the vertical and complete lift operations on $\pi_M^{-1}(\iota(S))$ by $\bar{\nabla}$ and \bar{C} , respectively. Now taking the complete lift of both sides of the equation (1.2) and using the equations (2.4) we get

$$\begin{aligned} \bar{C}(\bar{\nabla}_{BX}BY) &= \bar{C}(\widehat{\nabla}_{BX}BY) - \frac{1}{2}\bar{C}(\widehat{\omega}(BX)(BY)) - \frac{1}{2}\bar{C}(\widehat{\omega}(BY)(BX)) \\ &\quad + \frac{1}{2}\bar{C}(\widehat{g}(BX, BY)\widehat{P}) \end{aligned}$$

$$\begin{aligned} \bar{C}(\bar{\nabla}_{BX}BY) &= \bar{C}(\widehat{\nabla}_{BX}BY) - \frac{1}{2}\bar{C}(\widehat{\omega}(BX))\bar{\nabla}(BY) - \frac{1}{2}\bar{\nabla}(\widehat{\omega}(BX))\bar{C}(BY) \\ &\quad - \frac{1}{2}\bar{C}(\widehat{\omega}(BY))\bar{\nabla}(BX) - \frac{1}{2}\bar{\nabla}(\widehat{\omega}(BY))\bar{C}(BX) \\ &\quad + \frac{1}{2}\bar{C}(\widehat{g}(BX, BY))\bar{\nabla}\widehat{P} + \frac{1}{2}\bar{\nabla}(\widehat{g}(BX, BY))\bar{C}\widehat{P} \end{aligned}$$

$$\begin{aligned} {}^C\bar{\nabla}_{\widetilde{B}{}^CX}\widetilde{B}{}^CY &= {}^C\widehat{\nabla}_{\widetilde{B}{}^CX}\widetilde{B}{}^CY - \frac{1}{2}{}^C\widehat{\omega}(\widetilde{B}{}^CX)(\widetilde{B}{}^VY) - \frac{1}{2}{}^V\widehat{\omega}(\widetilde{B}{}^CX)(\widetilde{B}{}^CY) \\ &\quad - \frac{1}{2}{}^C\widehat{\omega}(\widetilde{B}{}^CY)(\widetilde{B}{}^VX) - \frac{1}{2}{}^V\widehat{\omega}(\widetilde{B}{}^CY)(\widetilde{B}{}^CX) \\ &\quad + \frac{1}{2}{}^C\widehat{g}(\widetilde{B}{}^CX, \widetilde{B}{}^CY)\bar{\nabla}\widehat{P} + \frac{1}{2}{}^C\widehat{g}(\widetilde{B}{}^VX, \widetilde{B}{}^CY)\bar{C}\widehat{P} \end{aligned}$$

and

$$\begin{aligned} {}^C\bar{\nabla}_{\widetilde{B}{}^CY}\widetilde{B}{}^CX &= {}^C\widehat{\nabla}_{\widetilde{B}{}^CY}\widetilde{B}{}^CX - \frac{1}{2}{}^C\widehat{\omega}(\widetilde{B}{}^CY)(\widetilde{B}{}^VX) - \frac{1}{2}{}^V\widehat{\omega}(\widetilde{B}{}^CY)(\widetilde{B}{}^CX) \\ &\quad - \frac{1}{2}{}^C\widehat{\omega}(\widetilde{B}{}^CX)(\widetilde{B}{}^VY) - \frac{1}{2}{}^V\widehat{\omega}(\widetilde{B}{}^CX)(\widetilde{B}{}^CY) \\ &\quad + \frac{1}{2}{}^C\widehat{g}(\widetilde{B}{}^CY, \widetilde{B}{}^CX)\bar{\nabla}\widehat{P} + \frac{1}{2}{}^C\widehat{g}(\widetilde{B}{}^VY, \widetilde{B}{}^CX)\bar{C}\widehat{P}. \end{aligned}$$

Then, we have

$$\begin{aligned}
 {}^c\bar{T}(\tilde{B}^cX, \tilde{B}^cY) &= {}^c\nabla_{\tilde{B}^cX} \tilde{B}^cY - {}^c\nabla_{\tilde{B}^cY} \tilde{B}^cX - [\tilde{B}^cX, \tilde{B}^cY] \\
 &= {}^c\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY - {}^c\hat{\nabla}_{\tilde{B}^cY} \tilde{B}^cX - [\tilde{B}^cX, \tilde{B}^cY] \\
 &= {}^c\hat{T}(\tilde{B}^cX, \tilde{B}^cY) \\
 &= \bar{c}(\hat{T}(BX, BY)) \\
 &= 0.
 \end{aligned}$$

By computing

$$\begin{aligned}
 &{}^c\hat{g}({}^c\nabla_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ) + {}^c\hat{g}(\tilde{B}^cY, {}^c\nabla_{\tilde{B}^cX} \tilde{B}^cZ) \\
 &= {}^c\hat{g}({}^c\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY - \frac{1}{2} {}^c\hat{\omega}(\tilde{B}^cX)(\tilde{B}^vY) - \frac{1}{2} {}^v\hat{\omega}(\tilde{B}^cX)(\tilde{B}^cY) \\
 &\quad - \frac{1}{2} {}^c\hat{\omega}(\tilde{B}^cY)(\tilde{B}^vX) - \frac{1}{2} {}^v\hat{\omega}(\tilde{B}^cY)(\tilde{B}^cX) \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^cX, \tilde{B}^cY) \bar{v}\hat{P} + \frac{1}{2} {}^c\hat{g}(\tilde{B}^vX, \tilde{B}^cY) \bar{c}\hat{P}, \tilde{B}^cZ) \\
 &\quad + {}^c\hat{g}(\tilde{B}^cY, {}^c\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ - \frac{1}{2} {}^c\hat{\omega}(\tilde{B}^cX)(\tilde{B}^vZ) \\
 &\quad - \frac{1}{2} {}^v\hat{\omega}(\tilde{B}^cX)(\tilde{B}^cZ) - \frac{1}{2} {}^c\hat{\omega}(\tilde{B}^cZ)(\tilde{B}^vX) \\
 &\quad - \frac{1}{2} {}^v\hat{\omega}(\tilde{B}^cZ)(\tilde{B}^cX) + \frac{1}{2} {}^c\hat{g}(\tilde{B}^cX, \tilde{B}^cZ) \bar{v}\hat{P} \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^vX, \tilde{B}^cZ) \bar{c}\hat{P}) \\
 &= {}^c\hat{g}({}^c\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ) + {}^c\hat{g}(\tilde{B}^cY, {}^c\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ) \\
 &\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BX)) {}^c\hat{g}(\tilde{B}^vY, \tilde{B}^cZ) - \frac{1}{2} \bar{v}(\hat{\omega}(BX)) {}^c\hat{g}(\tilde{B}^cY, \tilde{B}^cZ) \\
 &\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BY)) {}^c\hat{g}(\tilde{B}^vX, \tilde{B}^cZ) - \frac{1}{2} \bar{v}(\hat{\omega}(BY)) {}^c\hat{g}(\tilde{B}^cX, \tilde{B}^cZ) \\
 &\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BX)) {}^c\hat{g}(\tilde{B}^cY, \tilde{B}^vZ) - \frac{1}{2} \bar{v}(\hat{\omega}(BX)) {}^c\hat{g}(\tilde{B}^cY, \tilde{B}^cZ) \\
 &\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BZ)) {}^c\hat{g}(\tilde{B}^cY, \tilde{B}^vX) - \frac{1}{2} \bar{v}(\hat{\omega}(BZ)) {}^c\hat{g}(\tilde{B}^cY, \tilde{B}^cX) \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^cX, \tilde{B}^cY) {}^c\hat{g}(\bar{v}\hat{P}, \tilde{B}^cZ) \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^vX, \tilde{B}^cY) {}^c\hat{g}(\bar{c}\hat{P}, \tilde{B}^cZ) \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^cX, \tilde{B}^cZ) {}^c\hat{g}(\tilde{B}^cY, \bar{v}\hat{P}) \\
 &\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B}^vX, \tilde{B}^cZ) {}^c\hat{g}(\tilde{B}^cY, \bar{c}\hat{P})
 \end{aligned}$$

$$\begin{aligned}
&= {}^C\hat{g}\left({}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ\right) + {}^C\hat{g}\left(\tilde{B}^cY, {}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ\right) \\
&\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BX)) \bar{v}(\hat{g}(BY, BZ)) - \frac{1}{2} \bar{v}(\hat{\omega}(BX)) \bar{c}(\hat{g}(BY, BZ)) \\
&\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BY)) \bar{v}(\hat{g}(BX, BZ)) - \frac{1}{2} \bar{v}(\hat{\omega}(BY)) \bar{c}(\hat{g}(BX, BZ)) \\
&\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BX)) \bar{v}(\hat{g}(BY, BZ)) - \frac{1}{2} \bar{v}(\hat{\omega}(BX)) \bar{c}(\hat{g}(BY, BZ)) \\
&\quad - \frac{1}{2} \bar{c}(\hat{\omega}(BZ)) \bar{v}(\hat{g}(BY, BX)) - \frac{1}{2} \bar{v}(\hat{\omega}(BZ)) \bar{c}(\hat{g}(BY, BX)) \\
&\quad + \frac{1}{2} \bar{c}(\hat{g}(BX, BY)) \bar{v}(\hat{\omega}(BZ)) + \frac{1}{2} \bar{v}(\hat{g}(BX, BY)) \bar{c}(\hat{\omega}(BZ)) \\
&\quad + \frac{1}{2} \bar{c}(\hat{g}(BX, BZ)) \bar{v}(\hat{\omega}(BY)) + \frac{1}{2} \bar{v}(\hat{g}(BX, BZ)) \bar{c}(\hat{\omega}(BY)) \\
&= {}^C\hat{g}\left({}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ\right) + {}^C\hat{g}\left(\tilde{B}^cY, {}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ\right) \\
&\quad - \bar{c}(\hat{\omega}(BX)) \bar{v}(\hat{g}(BY, BZ)) - \bar{v}(\hat{\omega}(BX)) \bar{c}(\hat{g}(BY, BZ)) \\
&= {}^C\hat{g}\left({}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ\right) + {}^C\hat{g}\left(\tilde{B}^cY, {}^C\hat{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ\right) \\
&\quad - \bar{c}(\hat{\omega}(BX)) \hat{g}(BY, BZ) \\
&= (\tilde{B}^cX) {}^C\hat{g}(\tilde{B}^cY, \tilde{B}^cZ) - \bar{c}(\hat{\omega}(BX)) \hat{g}(BY, BZ)
\end{aligned}$$

And from following equation

$$\begin{aligned}
(\tilde{B}^cX) {}^C\hat{g}(\tilde{B}^cY, \tilde{B}^cZ) &= ({}^C\bar{\nabla}_{\tilde{B}^cX} {}^C\hat{g})(\tilde{B}^cY, \tilde{B}^cZ) \\
&\quad + {}^C\hat{g}\left({}^C\bar{\nabla}_{\tilde{B}^cX} \tilde{B}^cY, \tilde{B}^cZ\right) \\
&\quad + {}^C\hat{g}\left(\tilde{B}^cY, {}^C\bar{\nabla}_{\tilde{B}^cX} \tilde{B}^cZ\right)
\end{aligned}$$

we get

$$({}^C\bar{\nabla}_{\tilde{B}^cX} {}^C\hat{g})(\tilde{B}^cY, \tilde{B}^cZ) = \bar{c}(\hat{\omega}(BX)) \hat{g}(BY, BZ).$$

Theorem 3.4. Let $\overset{\circ}{\nabla}$ be a Weyl connection with respect to ∇ Riemannian connection in (S, g) . Then ${}^C\overset{\circ}{\nabla}$ is also Weyl connection with respect to ${}^C\nabla$ Riemannian connection in (TS, \tilde{g}) .

Proof. Taking the complete lift on both the sides of equation (3.8) and using equations (2.4), we get

$$\begin{aligned}
\bar{c}(\bar{\nabla}_{BX} BY) &= \bar{c}(\hat{\nabla}_{BX} BY) - \frac{1}{2} \bar{c}(\hat{\omega}(BX) BY) - \frac{1}{2} \bar{c}(\hat{\omega}(BY) BX) \\
&\quad + \frac{1}{2} \bar{c}(\hat{g}(BX, BY) \hat{P})
\end{aligned}$$

$$\begin{aligned}
 \bar{c}(\bar{\nabla}_{BX} BY) &= \bar{c}\left(\widehat{\nabla}_{BX} BY\right) - \frac{1}{2} \bar{c}(\widehat{\omega}(BX)) \bar{v}(BY) \\
 &\quad - \frac{1}{2} \bar{v}(\widehat{\omega}(BX)) \bar{c}(BY) - \frac{1}{2} \bar{c}(\widehat{\omega}(BY)) \bar{v}(BX) \\
 &\quad - \frac{1}{2} \bar{v}(\widehat{\omega}(BY)) \bar{c}(BX) + \frac{1}{2} \bar{c}(\widehat{g}(BX, BY)) \bar{v}\widehat{P} \\
 &\quad + \frac{1}{2} \bar{v}(\widehat{g}(BX, BY)) \bar{c}\widehat{P}
 \end{aligned}$$

$$\begin{aligned}
 \bar{c}\bar{\nabla}_{\tilde{B}^c X} \tilde{B}^c Y &= {}^c\widehat{\nabla}_{\tilde{B}^c X} \tilde{B}^c Y - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c X) (\tilde{B}^c Y) \\
 &\quad - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c X) (\tilde{B}^c Y) - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c Y) (\tilde{B}^c X) \\
 &\quad - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c Y) (\tilde{B}^c X) + \frac{1}{2} \bar{c}\widehat{g}(\tilde{B}^c X, \tilde{B}^c Y) \bar{v}\widehat{P} \\
 &\quad + \frac{1}{2} \bar{c}\widehat{g}(\tilde{B}^c X, \tilde{B}^c Y) \bar{c}\widehat{P}
 \end{aligned}$$

for arbitrary $X, Y \in S$. Hence, from equations (2.5) and (3.6) we obtain

$$\begin{aligned}
 \bar{c}\left(B\left(\overset{\circ}{\nabla}_X Y\right) + m(X, Y)N\right) &= \bar{c}(B(\nabla_X Y) + h(X, Y)N) \\
 &\quad - \frac{1}{2} \bar{c}(\widehat{\omega}(BX)BY) - \frac{1}{2} \bar{c}(\widehat{\omega}(BY)BX) \\
 &\quad + \frac{1}{2} \bar{c}(\widehat{g}(BX, BY)(BP + \eta N)) \\
 &= \bar{c}(B(\nabla_X Y) + h(X, Y)N) - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c X) \tilde{B}^c Y \\
 &\quad - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c X) \tilde{B}^c Y - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c Y) \tilde{B}^c X \\
 &\quad - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c Y) \tilde{B}^c X \\
 &\quad + \frac{1}{2} {}^c\widehat{g}(\tilde{B}^c X, \tilde{B}^c Y) (\tilde{B}^c P + {}^v\eta \bar{v}N) \\
 &\quad + \frac{1}{2} {}^c\widehat{g}(\tilde{B}^c X, \tilde{B}^c Y) (\tilde{B}^c P + {}^c\eta \bar{v}N + {}^v\eta \bar{c}N) \\
 &= \tilde{B}^c\left(\overset{\circ}{\nabla}_X Y\right) + {}^v m({}^c X, {}^c Y) \bar{c}N + {}^c m({}^c X, {}^c Y) \bar{v}N \\
 &= \tilde{B}^c(\nabla_X Y) + {}^v h({}^c X, {}^c Y) \bar{c}N + {}^c h({}^c X, {}^c Y) \bar{v}N \\
 &\quad - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c X) \tilde{B}^c Y - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c X) \tilde{B}^c Y \\
 &\quad - \frac{1}{2} {}^c\widehat{\omega}(\tilde{B}^c Y) \tilde{B}^c X - \frac{1}{2} {}^v\widehat{\omega}(\tilde{B}^c Y) (\tilde{B}^c X)
 \end{aligned}$$

$$\begin{aligned}
& +\frac{1}{2} {}^c\hat{g}(\tilde{B} {}^cX, \tilde{B} {}^cY) \tilde{B} {}^vP + \frac{1}{2} {}^v\eta {}^c\hat{g}(\tilde{B} {}^cX, \tilde{B} {}^cY) \bar{v}N \\
& +\frac{1}{2} {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \tilde{B} {}^cP + \frac{1}{2} {}^c\eta {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \bar{v}N \\
& +\frac{1}{2} {}^v\eta {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \bar{c}N
\end{aligned}$$

Moreover we get

$$\begin{aligned}
\tilde{B} {}^c \left(\overset{\circ}{\nabla}_X Y \right) &= \tilde{B} {}^c (\nabla_X Y) - \frac{1}{2} {}^c\hat{\omega}(\tilde{B} {}^cX) \tilde{B} {}^vY - \frac{1}{2} {}^v\hat{\omega}(\tilde{B} {}^cX) \tilde{B} {}^cY \\
&\quad - \frac{1}{2} {}^c\hat{\omega}(\tilde{B} {}^cY) \tilde{B} {}^vX - \frac{1}{2} {}^v\hat{\omega}(\tilde{B} {}^cY) \tilde{B} {}^cX \\
&\quad + \frac{1}{2} {}^c\hat{g}(\tilde{B} {}^cX, \tilde{B} {}^cY) \tilde{B} {}^vP + \frac{1}{2} {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \tilde{B} {}^cP
\end{aligned}$$

and

$$\begin{aligned}
& {}^v m({}^cX, {}^cY) \bar{c}N + {}^c m({}^cX, {}^cY) \bar{v}N \\
&= \left({}^v h({}^cX, {}^cY) + \frac{1}{2} {}^v\eta {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \right) \bar{c}N \\
&\quad + \left({}^c h({}^cX, {}^cY) + \frac{1}{2} {}^v\eta {}^c\hat{g}(\tilde{B} {}^cX, \tilde{B} {}^cY) + \frac{1}{2} {}^c\eta {}^c\hat{g}(\tilde{B} {}^vX, \tilde{B} {}^cY) \right) \bar{v}N.
\end{aligned}$$

From the equations (2.4), it follows that

$$\begin{aligned}
{}^c \left(\overset{\circ}{\nabla}_X Y \right) &= {}^c (\nabla_X Y) - \frac{1}{2} {}^c\omega({}^cX) {}^vY - \frac{1}{2} {}^v\omega({}^cX) {}^cY - \frac{1}{2} {}^c\omega({}^cY) {}^vX \\
&\quad - \frac{1}{2} {}^v\omega({}^cY) {}^cX + \frac{1}{2} \tilde{g}({}^cX, {}^cY) {}^vP + \frac{1}{2} \tilde{g}({}^vX, {}^cY) {}^cP
\end{aligned}$$

and finally, we obtain

$$\begin{aligned}
{}^c \overset{\circ}{\nabla}_{{}^cX} {}^cY &= {}^c \nabla_{{}^cX} {}^cY - \frac{1}{2} {}^c\omega({}^cX) {}^vY - \frac{1}{2} {}^v\omega({}^cX) {}^cY \\
&\quad - \frac{1}{2} {}^c\omega({}^cY) {}^vX - \frac{1}{2} {}^v\omega({}^cY) {}^cX \\
&\quad + \frac{1}{2} \tilde{g}({}^cX, {}^cY) {}^vP + \frac{1}{2} \tilde{g}({}^vX, {}^cY) {}^cP, \\
{}^c \overset{\circ}{\nabla}_{{}^cY} {}^cX &= {}^c \nabla_{{}^cY} {}^cX - \frac{1}{2} {}^c\omega({}^cY) {}^vX - \frac{1}{2} {}^v\omega({}^cY) {}^cX \\
&\quad - \frac{1}{2} {}^c\omega({}^cX) {}^vY - \frac{1}{2} {}^v\omega({}^cX) {}^cY \\
&\quad + \frac{1}{2} \tilde{g}({}^cY, {}^cX) {}^vP + \frac{1}{2} \tilde{g}({}^vY, {}^cX) {}^cP.
\end{aligned}$$

Thus, we have

$$\begin{aligned}
{}^c \overset{\circ}{T}({}^cX, {}^cY) &= {}^c \overset{\circ}{\nabla}_{{}^cX} {}^cY - {}^c \overset{\circ}{\nabla}_{{}^cY} {}^cX - [{}^cX, {}^cY] \\
&= 0.
\end{aligned}$$

Similarly

$$\begin{aligned}
 & \tilde{g}\left({}^C \overset{\circ}{\nabla}_{c_X} c_Y, c_Z\right) + \tilde{g}\left(c_Y, {}^C \overset{\circ}{\nabla}_{c_X} c_Z\right) \\
 = & \tilde{g}\left({}^C \nabla_{c_X} c_Y - \frac{1}{2} c_\omega({}^C X) v_Y - \frac{1}{2} v_\omega({}^C X) c_Y\right. \\
 & \left. - \frac{1}{2} c_\omega({}^C Y) v_X - \frac{1}{2} v_\omega({}^C Y) c_X\right. \\
 & \left. + \frac{1}{2} \tilde{g}({}^C X, c_Y) v_P + \frac{1}{2} \tilde{g}(v_X, c_Y) c_P, c_Z\right) \\
 & + \tilde{g}\left(c_Y, {}^C \nabla_{c_X} c_Z - \frac{1}{2} c_\omega({}^C X) v_Z - \frac{1}{2} v_\omega({}^C X) c_Z\right. \\
 & \left. - \frac{1}{2} c_\omega({}^C Z) v_X - \frac{1}{2} v_\omega({}^C Z) c_X\right. \\
 & \left. + \frac{1}{2} \tilde{g}({}^C X, c_Z) v_P + \frac{1}{2} \tilde{g}(v_X, c_Z) c_P\right) \\
 = & \tilde{g}({}^C \nabla_{c_X} c_Y, c_Z) + \tilde{g}(c_Y, {}^C \nabla_{c_X} c_Z) \\
 & - \frac{1}{2} c(\omega(X)) \tilde{g}(v_Y, c_Z) - \frac{1}{2} v(\omega(X)) \tilde{g}(c_Y, c_Z) \\
 & - \frac{1}{2} c(\omega(Y)) \tilde{g}(v_X, c_Z) - \frac{1}{2} v(\omega(Y)) \tilde{g}(c_X, c_Z) \\
 & - \frac{1}{2} c(\omega(X)) \tilde{g}(c_Y, v_Z) - \frac{1}{2} v(\omega(X)) \tilde{g}(c_Y, c_Z) \\
 & - \frac{1}{2} c(\omega(Z)) \tilde{g}(c_Y, v_X) - \frac{1}{2} v(\omega(Z)) \tilde{g}(c_Y, c_X) \\
 & + \frac{1}{2} \tilde{g}({}^C X, c_Y) \tilde{g}(v_P, c_Z) + \frac{1}{2} \tilde{g}(v_X, c_Y) \tilde{g}(c_P, c_Z) \\
 & + \frac{1}{2} \tilde{g}({}^C X, c_Z) \tilde{g}(c_Y, v_P) + \frac{1}{2} \tilde{g}(v_X, c_Z) \tilde{g}(c_Y, c_P) \\
 = & \tilde{g}({}^C \nabla_{c_X} c_Y, c_Z) + \tilde{g}(c_Y, {}^C \nabla_{c_X} c_Z) \\
 & - c(\omega(X))^V(g(Y, Z)) - v(\omega(X)) c(g(Y, Z)) \\
 = & \tilde{g}({}^C \nabla_{c_X} c_Y, c_Z) + \tilde{g}(c_Y, {}^C \nabla_{c_X} c_Z) - c(\omega(X) g(Y, Z)) \\
 = & c_X \tilde{g}(c_Y, c_Z) - c(\omega(X) g(Y, Z)).
 \end{aligned}$$

And from following equation

$$\begin{aligned}
 c_X \tilde{g}(c_Y, c_Z) &= \left({}^C \overset{\circ}{\nabla}_{c_X} \tilde{g}\right)(c_Y, c_Z) + \tilde{g}\left({}^C \overset{\circ}{\nabla}_{c_X} c_Y, c_Z\right) \\
 &+ \tilde{g}\left(c_Y, {}^C \overset{\circ}{\nabla}_{c_X} c_Z\right)
 \end{aligned}$$

we get

$$\left({}^C \overset{\circ}{\nabla}_{c_X} \tilde{g}\right)(c_Y, c_Z) = c(\omega(X) g(Y, Z)).$$

The Weyl connection ${}^C\overset{\circ}{\nabla}$ on (TS, \tilde{g}) can be given by

$$\begin{aligned} {}^C\overset{\circ}{\nabla}_{{}^C X} {}^C Y &= {}^C\nabla_{{}^C X} {}^C Y - \frac{1}{2} {}^C\omega({}^C X) {}^V Y - \frac{1}{2} {}^V\omega({}^C X) {}^C Y - \frac{1}{2} {}^C\omega({}^C Y) {}^V X \\ &\quad - \frac{1}{2} {}^V\omega({}^C Y) {}^C X + \frac{1}{2} \tilde{g}({}^C X, {}^C Y) {}^V P + \frac{1}{2} \tilde{g}({}^V X, {}^C Y) {}^C P \end{aligned}$$

and taking the complete lift of both sides of the equations (3.6) we obtain

$${}^C\bar{\nabla}_{\tilde{B} {}^C X} \tilde{B} {}^C Y = \tilde{B} \left({}^C\overset{\circ}{\nabla}_{{}^C X} {}^C Y \right) + {}^V m({}^C X, {}^C Y) \bar{C} N + {}^C m({}^C X, {}^C Y) \bar{V} N$$

From the equation (2.4), it follows that

$$\begin{aligned} {}^V m({}^C X, {}^C Y) &= {}^V h({}^C X, {}^C Y) + \frac{1}{2} {}^V \eta {}^C \hat{g}(\tilde{B} {}^V X, \tilde{B} {}^C Y) \\ {}^C m({}^C X, {}^C Y) &= {}^C h({}^C X, {}^C Y) + \frac{1}{2} {}^V \eta {}^C \hat{g}(\tilde{B} {}^C X, \tilde{B} {}^C Y) \\ &\quad + \frac{1}{2} {}^C \eta {}^C \hat{g}(\tilde{B} {}^V X, \tilde{B} {}^C Y). \end{aligned}$$

According to [11], TS is totally umbilical if and only if there exist differentiable functions λ and μ , such that

$$\begin{aligned} {}^V m(\tilde{X}, \tilde{Y}) &= \lambda \tilde{g}(\tilde{X}, \tilde{Y}) \\ {}^C m(\tilde{X}, \tilde{Y}) &= \mu \tilde{g}(\tilde{X}, \tilde{Y}) \end{aligned}$$

for arbitrary vector fields $\tilde{X}, \tilde{Y} \in \mathfrak{S}_0^1(TS)$. If both λ and μ vanish, then TS is totally geodesic. It is trivial to prove the following theorems by using the equations (2.4).

Theorem 3.5. *TS is totally umbilical with respect to the Weyl connection ${}^C\overset{\circ}{\nabla}$ if and only if it is totally umbilical or totally geodesic with respect to the Riemannian connection ${}^C\nabla$.*

Theorem 3.6. *TS is totally umbilical with respect to the Weyl connection ${}^C\overset{\circ}{\nabla}$ if and only if S is totally umbilical with respect to the Weyl connection $\overset{\circ}{\nabla}$.*

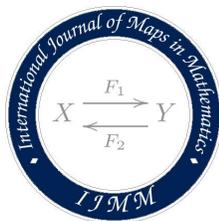
Theorem 3.7. *TS is totally geodesic with respect to the Weyl connection ${}^C\overset{\circ}{\nabla}$ if and only if it is totally geodesic with respect to the Riemannian connection ${}^C\nabla$ and the vector field \hat{P} is tangent to S .*

Theorem 3.8. *TS is totally geodesic with respect to the Weyl connection ${}^C\overset{\circ}{\nabla}$ if and only if S is totally geodesic with respect to the Weyl connection $\overset{\circ}{\nabla}$.*

REFERENCES

- [1] Chen, B. Y. (2019). *Geometry of Submanifolds*, New York: Marcel Dekker Inc.
- [2] Crasmareanu, M. (2012). Recurrent metrics in the geometry of second order differential equations. *B Iran Math Soc*, 38(2), 391-401.
- [3] Çayır H. (2018). Covariant Derivatives of Structures with Respect to Lifts on Tangent Bundle. *Karaelmas Science and Engineering Journal*, 8(1), 273-278.
- [4] Çiçek Gözütok, A., & Esin, E. (2012). Tangent bundle of hypersurface with semi symmetric metric connection. *Int J Contemp Math Sci*, 7(6), 279-289.
- [5] Folland, G. B. (1970). Weyl manifolds. *J Differ Geom*, 4(2), 145-153.
- [6] Hall, G. S. (1992). Weyl manifolds and connections. *J Math Phys*, 33(7), 2633-2638.
- [7] Khan, M. N. I. (2014). Lifts of hypersurfaces with Quarter-symmetric semi-metric connection to tangent bundles. *Afr Mat*, 25(2), 475-482.
- [8] Khan, M. N. I., Ansari, G. A., & Khizer, S. (2017). A study of semi-symmetric semi-metric connection using lifting theory. *Far East J Math Sci*, 102(11), 2727–2739.
- [9] Musso, E., & Tricerri, F. (1988). Riemannian metrics on tangent bundles. *Ann Mat Pura Appl*, 150(1), 1–19.
- [10] Smaranda, D., & Andonie, O. C. (1976). On semi-symmetric connections. *Ann. Fac. Sci. Univ. Nat. Zaire (Kinshasa), Sec. Math.-Phys*, 2, 265-270.
- [11] Tani, M. (1969). Prolongations of hypersurfaces to tangent bundles. *Kodai Math Semp Rep*, 21(1), 85-96.
- [12] Tarafdar, M., & Kundu, S. (2012). Almost Hermitian manifolds admitting Einstein-Weyl connection. *Lobachevskii Journal of Mathematics*, 33(1), 5-9.
- [13] Tarakci, O., Gezer, A., & Salimov, A. A. (2009). On solutions of IHPT equations on tangent bundles with the metric II+ III. *Math Comp Model*, 50(7-8), 953-958.
- [14] Mani Tripathi, M. (2008). A new connection in a Riemannian manifold. *Int Electron J Geom*, 1(1), 15-24.
- [15] Wong, Y. C. (1961). Recurrent tensors on a linearly connected differentiable manifold. *Trans Am Math Soc*, 99(2), 325-341.
- [16] Yano, K., & Ledger, A. J. (1964). Linear connections on tangent bundles. *J London Math Soc*, 39, 495-500.
- [17] Yano, K., & Ishihara, S. (1973). *Tangent and Cotangent Bundle*, New York Marcel Dekker Inc.

KAFKAS UNIVERSITY, FACULTY OF ARTS AND SCIENCES, DEPARTMENT OF MATHEMATICS, 36000, KARS, TURKEY



TRANSLATION-FACTORABLE SURFACES WITH VANISHING CURVATURES IN GALILEAN 3-SPACE

ALEV KELLECI* 

ABSTRACT. In this paper, we define two types of Translation-Factorable (TF-) surfaces in the Galilean 3-space. Then, we obtain the complete classification of these surfaces with vanishing Gaussian curvature and mean curvature and also, we give some explicit graphics of these surfaces.

Keywords: Flat surfaces, minimal surfaces, translation surface, factorable surfaces, Galilean space.

2010 Mathematics Subject Classification: 53A35, 53A40.

1. INTRODUCTION

The history of the view of what constitutes geometry has been changed radically on a number of occasions. For centuries, it was thought that the single aim of geometry is the through investigation of the properties of ordinary 3-dimensional Euclidean space. That view was broadened by Gauss in 1816, by Bolyai 1824 and by Lobachevski in 1826, independently. Furthermore, the explorations and views of Riemann [15] and Klein [11] being a synthesis of the geometric views of Cayley showed that there exist other (non-Euclidean) geometric systems. Until this time, many technical and popular resources have been written about the geometry of non-Euclidean space. Among these space, there are Minkowski space [13], Galilean and pseudo-Galilean space [1, 10, 14, 16] and so on.

Received: 2020.04.10
Accepted: 2020.08.18

Revised: 2020.06.20

Ac-

* Corresponding author

Alev Kelleci; alevkelleci@hotmail.com; <https://orcid.org/0000-0003-2528-2131>

It should be noted that one of the pioneer books of the Galilean geometry is the Yaglom's book [19]. In that book was discussed on the physical basis of this geometry closely related with Galilean's principle of relativity, i.e., Newtonian mechanics. In the last decade, the Galilean and pseudo-Galilean space were used by several researchers as an ambient space for the well-known Euclidean concepts (see in [3, 4, 5, 6, 7, 9, 12, 17, 18]).

In this paper, we first introduce the notations that we are going to use and give a brief summary of basic definitions in theory of surfaces in Galilean 3-space. Then, we define two types of Translation-Factorable (TF-) surfaces in Galilean 3-space, by considering the definition of these surfaces given in [8] in Euclidean and Lorentzian 3-space. Also, we give the complete classification of such surfaces with vanishing Gaussian curvature and mean curvature and also some explicit graphics of them.

2. PRELIMINARIES

First, we would like to give a brief summary of basic definitions, facts and equations in the theory of surfaces of Galilean 3-space (see for detail, [14, 16, 19]).

The Galilean 3-space \mathbb{G}^3 arises in a Cayley-Klein way by pointing out an absolute figure $\{\omega, f, J\}$ in the 3-dimensional real projective space $\mathbb{P}_3(\mathbb{R})$ where ω is the ideal (absolute) plane, f is the absolute line and J is the fixed elliptic involution of points of f . Then the homogeneous coordinates $(x_0 : x_1 : x_2 : x_3)$ are introduced such that ω is given by $x_0 = 0$, f is given by $x_0 = x_1 = 0$ and J , by $(0 : 0 : x_2 : x_3) \mapsto (0 : 0 : -x_3 : x_2)$.

In affine coordinates defined by $(x_0 : x_1 : x_2 : x_3) = (1 : x_1 : x_2 : x_3)$, the distance between two points $P_i = (x_i, y_i, z_i)$ with $i \in \{1, 2\}$ is defined by the formula

$$d_{P_1 P_2} = \begin{cases} |x_2 - x_1| & \text{if } x_1 \neq x_2, \\ \sqrt{(y_2 - y_1)^2 + (z_2 - z_1)^2} & \text{if } x_1 = x_2 \end{cases}$$

The group of motions of \mathbb{G}^3 is a six-parameter group. Regarding this group of motions, except the absolute plane, there exist two classes of planes in \mathbb{G}^3 : Euclidean planes that contain f where the induced metric is Euclidean and isotropic planes that do not contain f whose induced metric is isotropic. Also, there are four types of lines in \mathbb{G}^3 : isotropic lines that intersect f , non-isotropic lines that do not intersect f , non-isotropic lines in ω and the absolute line f , [6].

Let $\vec{X} = (x_1, x_2, x_3)$ be a vector in \mathbb{G}^3 . If $x_1 = 0$, then \vec{X} is called as isotropic; otherwise, it is said to be non-isotropic. Note that, the x_1 -axis is non-isotropic while the x_2 -axis and the x_3 -axis are isotropic, for standart coordinates (x_1, x_2, x_3) . Moreover, a plane of the form

$x_1 = \text{const.}$ is called an Euclidean plane, otherwise isotropic. For two vectors $\vec{X} = (x_1, x_2, x_3)$ and $\vec{Y} = (y_1, y_2, y_3)$, the Galilean scalar product is given by

$$\langle X, Y \rangle = \begin{cases} x_1 y_1 & \text{if } x_1 \neq 0 \text{ or } y_1 \neq 0, \\ x_2 y_2 + x_3 y_3 & \text{if } x_1 = y_1 = 0. \end{cases}$$

The norm of vector \vec{X} in \mathbb{G}^3 is defined by $\|\vec{X}\| := \sqrt{\langle \vec{X}, \vec{X} \rangle}$. If $\|\vec{X}\| = 1$, then \vec{X} is called as unit vector. Also, the Galilean cross product of the vectors \vec{X} and \vec{Y} of which at least one is non-isotropic is defined by

$$\vec{X} \times \vec{Y} = \left(0, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1 \right). \quad (2.1)$$

Assume that U is an open set of \mathbb{R}^2 and S is a C^r -surface such that $r \geq 2$, immersed in \mathbb{G}^3 parametrized by

$$\varphi : U \rightarrow \mathbb{R}^2, \quad \varphi(u_1, u_2) = (\varphi_1(u_1, u_2), \varphi_2(u_1, u_2), \varphi_3(u_1, u_2)). \quad (2.2)$$

Let us denote $\frac{\partial \varphi}{\partial u_i} = \varphi_{,i}$, $\frac{\partial \varphi_k}{\partial u_i} = (\varphi_k)_{,i}$ and $\frac{\partial^2 \varphi_k}{\partial u_i \partial u_j} = (\varphi_k)_{,ij}$ where $1 \leq k \leq 3$ and $1 \leq i, j \leq 2$. Then a surface is admissible (i.e., without Euclidean tangent planes) if and only if $(\varphi_1)_{,i} \neq 0$ for some $i = 1, 2$. Let $S \subset \mathbb{G}^3$ be a regular admissible surface. We define the side tangential vector field by

$$\sigma = \frac{(\varphi_1)_{,1} \varphi_{,2} - (\varphi_1)_{,2} \varphi_{,1}}{W} \quad (2.3)$$

and a unit normal vector N as

$$N = \frac{\varphi_{,1} \times \varphi_{,2}}{W} \quad (2.4)$$

where the function $W = \|\varphi_{,1} \times \varphi_{,2}\|$, [17].

Now, we introduce the coefficients of the second fundamental form

$$L_{ij} = \left\langle \frac{\varphi_{,ij}(\varphi_1)_{,1} - (\varphi_1)_{,ij} \varphi_{,1}}{(\varphi_1)_{,1}}, N \right\rangle = \left\langle \frac{\varphi_{,ij}(\varphi_1)_{,2} - (\varphi_1)_{,ij} \varphi_{,2}}{(\varphi_1)_{,2}}, N \right\rangle. \quad (2.5)$$

Consequently, the Gaussian curvature K and the mean curvature H of M are defined by

$$K = \frac{L_{11} L_{22} - L_{12}^2}{W^2}, \quad (2.6)$$

$$H = \frac{1}{2} \sum_{i,j=1}^2 g^{ij} L_{ij}, \quad (2.7)$$

where

$$g^1 = \frac{(\varphi_1)_{,2}}{W}, \quad g^2 = \frac{(\varphi_1)_{,1}}{W} \quad \text{and} \quad g^{ij} = g^i g^j \quad \text{for } i, j = 1, 2. \quad (2.8)$$

Note that, if M has zero curvatures, i.e., $K = 0$ or $H = 0$, then it is called as flat or minimal, respectively.

2.1. Translation-Factorable Surfaces in Galilean 3-space. In this section, we first would like to state the following definitions given in [3, 4, 17] :

Definition 2.1. *Let M^2 be an admissible surface in Galilean space. Then M is called a factorable surface if it can be locally written as one of the following:*

$$x(s, t) = (s, t, f(s)g(t)), \quad (2.9)$$

or

$$x(s, t) = (f(s)g(t), s, t), \quad (2.10)$$

which are called as first and second kind, respectively. Here f, g are smooth functions of one variable.

Definition 2.2. *Let M^2 be an admissible surface in Galilean space. Then M is called a translation surface if it can be locally written as one of the following:*

$$x(s, t) = (s, t, f(s) + g(t)), \quad (2.11)$$

or

$$x(s, t) = (f(s) + g(t), s, t), \quad (2.12)$$

which are called as first and second kind, respectively. Here f, g are smooth functions of one variable.

Note that as can be seen from the definitions of translation surfaces or factorable surfaces given above, there exist some distinction into two types of them coming from the fact that the x-direction and another direction in the yz-plane play distinct roles due to the degeneracy of the metric. Now by considering these definitions, we would like to give the definition of translation-factorable (TF-) surface in Galilean 3-space, firstly defined in [8] in Euclidean and Lorentzian 3-space, as follows:

Definition 2.3. *Let M^2 be an admissible surface in Galilean 3-space. Then M is called a translation-factorable (TF-) surface if it can be locally written as one of the following:*

$$\varphi(s, t) = (s, t, Bf(s)g(t) + A(f(s) + g(t))), \quad (2.13)$$

or

$$\varphi(s, t) = (Bf(s)g(t) + A(f(s) + g(t)), s, t), \quad (2.14)$$

which are called as first and second type, respectively. Here f and g are real functions and A, B are non-zero constants.

Remark 2.1. From Definition 2.3, one can observe that the surface M given by (2.13) and (2.14) becomes a factorable surface when $A = 0, B \neq 0$. Similarly, if one takes $B = 0$ and $A \neq 0$, then surface is a translation surface.

Hence, we are going to consider the case $AB \neq 0$.

3. CLASSIFICATION OF TRANSLATION-FACTORABLE SURFACES WITH VANISHING CURVATURE IN \mathbb{G}^3

In this section, we obtain the Gaussian and the mean curvature of TF-surfaces in \mathbb{G}^3 . Then, we obtain the complete classification of flat and minimal TF-surfaces.

3.1. Type I TF-surfaces with zero curvature. Let M^2 be a type I TF-surface in \mathbb{G}^3 given by (2.13). Then, we have

$$\varphi_s = (1, 0, (Bg(t) + A)f'(s)), \quad (3.15)$$

$$\varphi_t = (0, 1, g'(t)(Bf(s) + A)). \quad (3.16)$$

In addition by using (2.4), we obtain

$$N = \frac{1}{\sqrt{1 + g'(t)^2(Bf(s) + A)^2}}(0, -g'(t)(Bf(s) + A), 1). \quad (3.17)$$

Here by \prime , we have denoted derivatives with respect to corresponding parameters. For readability, here and in the rest of the paper, we will drop the explicit dependence of the functions on the variables and simply write $f = f(s)$ and $g = g(t)$. Now, by combining (3.15)-(3.17) with (2.5) and (2.8), respectively, we get

$$L_{11} = \frac{f''(Bg + A)}{W}, \quad L_{12} = \frac{Bf'g'}{W}, \quad L_{22} = \frac{g''(Bf + A)}{W}, \quad (3.18)$$

and

$$g^{11} = 0, \quad g^{12} = 0, \quad g^{22} = \frac{1}{W^2}, \quad (3.19)$$

where $W^2 = 1 + g'(t)^2(Bf(s) + A)^2$. Consequently, (2.6) and (2.7) give

$$K = \frac{f''g''(Bf + A)(Bg + A) - B^2(f')^2(g')^2}{(1 + g'^2(Bf + A)^2)}, \quad (3.20)$$

$$H = \frac{g''(Bf + A)}{2(1 + g'^2(Bf + A)^2)^{3/2}}, \quad (3.21)$$

respectively.

Now, we would like to investigate the vanishing curvature problem for TF-surfaces. First, we examine a type I TF-surface in Galilean 3-space, whose Gaussian curvature is identically zero.

Theorem 3.1. *Let M^2 be a type I TF-surface defined by (2.13) in the Galilean 3-space. Then, M^2 is a flat surface if and only if it belongs to one of the following families:*

- (1) M^2 is a part of an isotropic plane,
- (2) M^2 is an admissible cylindrical surface in \mathbb{G}^3 parametrized by

$$\varphi(s, t) = (s, t, C_1g(t) + C_2), \quad (3.22)$$

where C_1, C_2 are non-zero constant and g is arbitrary function or

$$\varphi(s, t) = (s, t, C_1f(s) + C_2) \quad (3.23)$$

where C_1, C_2 are non-zero constant and f is arbitrary function.

- (3) f and g are given by

$$f(s) = -\frac{1}{B}e^{B(c_1s+c_2)} + \frac{A}{B}, \quad g(t) = -\frac{1}{B}e^{B(c_1t+c_2)} + \frac{A}{B}. \quad (3.24)$$

- (4) f and g are given by

$$f(s) = -\frac{A}{B} + B^{\frac{C}{C-1}} \left((1-C)(c_1s + c_2) \right)^{\frac{1}{1-C}}, \quad g(t) = -\frac{A}{B} + B^{\frac{1}{C-1}} \left((1-\frac{1}{C})(c_1t + c_2) \right)^{\frac{C}{C-1}}, \quad (3.25)$$

where $C \neq 1$ is non-zero constant.

Proof. Let M^2 be a type I TF-flat surface. Thus, from (3.20), we have

$$f''g''(Bf + A)(Bg + A) - B^2(f')^2(g')^2 = 0. \quad (3.26)$$

Let us consider on the following possibilities:

Case (1): $f' = 0$ and $g' = 0$. Then, the equation (3.26) is trivially satisfied. By considering these assumptions in (2.13), respectively, we obtain M^2 is an open part of plane. Thus, we have Case (1) of Theorem 3.1.

Case (2): Either $f' = 0$ or $g' = 0$. First, assume that $f' = 0$, i.e., f be constant. In case, the equation (3.26) is trivially satisfied. But, in case g is a arbitrary smooth function. Thus, we get (3.22). Similarly, by considering the assumption of g as $g' = 0$, we can get (3.23) in Theorem 3.1.

Case (3): Let $f'' = 0$ or $g'' = 0$, but not both. First, assume that $f'' = 0$, i.e., f be a linear function. In this case, one get $g' = 0$ to provide the equation (3.26). Second, let $g'' = 0$. Then by the similar way, $f' = 0$ must be. Note that one can easily see that these cases are covered by Case (2).

Case (4): Let f' , g' , f'' and g'' be non-zero. Then, the equation (3.26) can be rewritten as

$$\frac{f''(A + Bf)}{B(f')^2} = \frac{B(g')^2}{g''(A + Bg)} = C, \quad (3.27)$$

for non-zero constant C . We are going to consider the following cases separately:

Case (4a): $C = 1$. In this case (3.27) implies that

$$f''(A + Bf) = B(f')^2 \quad \text{and} \quad B(g')^2 = g''(A + Bg), \quad (3.28)$$

from which, we get (3.24) in Case (3) in Theorem 3.1.

Case (4b): $C \neq 1$. In this case we solve (3.27) to obtain (3.25).

Conversely, a direct computation yields that the Gaussian curvature of each of surfaces given in Theorem 3.1 vanishes identically.

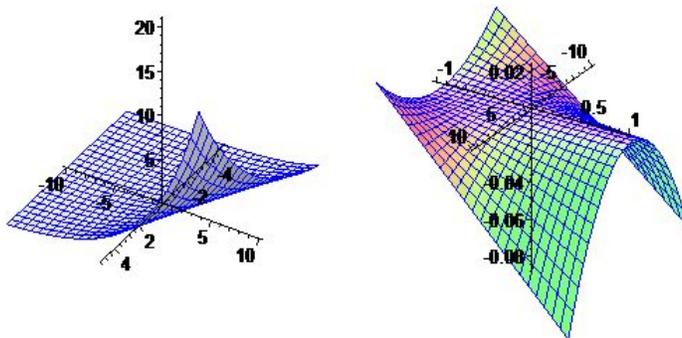


FIGURE 1. A type I TF-flat surfaces parametrized by (3.24) and (3.25), respectively.

Now, we examine a type I TF-surface in Galilean 3-space, whose mean curvature is identically zero.

Theorem 3.2. *Let M^2 be a type I TF-surface defined by (2.13) in the Galilean 3-space. Then, M^2 is a minimal surface if and only if it is either*

- (1) an open part of the plane $z = -\frac{A^2}{B}$ or
- (2) a ruled surface of type C in \mathbb{G}^3 parametrized by

$$\varphi(s, t) = (s, 0, H(s)) + t(0, 1, F(s)) \tag{3.29}$$

where $F(s) = a(Bf + A)$ and $H(s) = Af + b(A + B)$.

Proof. Let M^2 be a type I TF-minimal surface. Thus, from (3.21), it is clear that is sufficient that

$$g''(Bf + A) = 0. \tag{3.30}$$

Let us consider on the following possibilities:

Case (1): $f = -\frac{A}{B}$. Then the surface given in (2.13) can be reparametrized as $\varphi(s, t) = (s, t, -\frac{A^2}{B})$ which is an open part of the plane $z = -\frac{A^2}{B}$. Thus, we have Case (1) of Theorem 3.2.

Case (2): $g'' = 0$. Then, the function $g(t)$ is a linear function, i.e., $g(t) = at + b, a, b \in \mathbb{R}$. Then the surface given in (2.13) can be parametrized as in (3.29).

The converse follows from a direct computation.

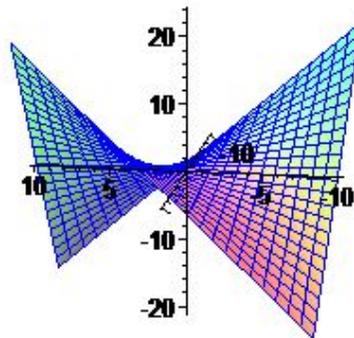


FIGURE 2. A type I TF-minimal surfaces parametrized by (3.29).

Now, we would like to do the calculations for the second type TF-surfaces.

3.2. Type II TF-surfaces with zero curvature. Let M^2 be an admissible type II TF-surface in \mathbb{G}^3 given by (2.14). Then, we have

$$\varphi_s = ((Bg + A)f', 1, 0), \quad (3.31)$$

$$\varphi_t = (g'(Bf + A), 0, 1). \quad (3.32)$$

Moreover, by substituting these into (2.4) we obtain

$$N = \frac{1}{\sqrt{f'^2(Bg + A)^2 + g'^2(Bf + A)^2}}(0, -f'(Bg + A), -g'(Bf + A)). \quad (3.33)$$

Here by ι , we have denoted derivatives with respect to corresponding parameters. Now, by combining the above with (2.5) and (2.8), respectively, we get

$$L_{11} = \frac{f''(Bg + A)}{W}, \quad L_{12} = \frac{Bf'g'}{W}, \quad L_{22} = \frac{g''(Bf + A)}{W}, \quad (3.34)$$

and

$$g^{11} = \frac{(g')^2(Bf + A)^2}{W^2}, \quad g^{12} = \frac{f'g'(Bf + A)(Bg + A)}{W^2}, \quad g^{22} = \frac{(f')^2(Bg + A)^2}{W^2}, \quad (3.35)$$

where $W = \sqrt{f'^2(Bg + A)^2 + g'^2(Bf + A)^2}$. Consequently, (2.6) and (2.7) give

$$K = \frac{f''g''(Bf + A)(Bg + A) - B^2(f')^2(g')^2}{(f'^2(Bg + A)^2 + g'^2(Bf + A)^2)} \quad (3.36)$$

and

$$H = \frac{f''g'^2(Bf + A)^2(Bg + A) + g''f'^2(Bg + A)^2(Bf + A) - 2Bf'^2g'^2(Bf + A)(Bg + A)}{2(f'^2(Bg + A)^2 + g'^2(Bf + A)^2)^{3/2}}, \quad (3.37)$$

respectively.

Remark 3.1. *By comparing Eq. (3.20) and Eq. (3.36) implies that the Gaussian curvatures of type I and type II of TF-surfaces in Galilean 3-space seem to be really very similar. Thus the following classification of type II TF- flat surfaces can be proved as in Theorem 3.1.*

Theorem 3.3. *Let M^2 be a type II TF-surface defined by (2.14) in the Galilean 3-space. Then, M^2 is a flat surface if and only if it belongs to one of the following families:*

- (1) M^2 is a part of an isotropic plane,
- (2) M^2 is an admissible surface in \mathbb{G}^3 parametrized by

$$\varphi(s, t) = (C_1g(t) + C_2, s, t), \quad (3.38)$$

where C_1, C_2 are non-zero constant or

$$\varphi(s, t) = (C_1f(s) + C_2, s, t) \quad (3.39)$$

where C_1, C_2 are non-zero constant.

(3) f and g are given by

$$f(s) = -\frac{1}{B}e^{B(c_1s+c_2)} + \frac{A}{B}, \quad g(t) = -\frac{1}{B}e^{B(c_1t+c_2)} + \frac{A}{B}. \quad (3.40)$$

(4) f and g are given by

$$f(s) = -\frac{A}{B} + B^{\frac{C}{C-1}} \left((1-C)(c_1s+c_2) \right)^{\frac{1}{1-C}}, \quad g(t) = -\frac{A}{B} + B^{\frac{1}{C-1}} \left((1-\frac{1}{C})(c_1t+c_2) \right)^{\frac{C}{C-1}}, \quad (3.41)$$

where $C \neq 1$ and c_1, c_2 are non-zero constant.

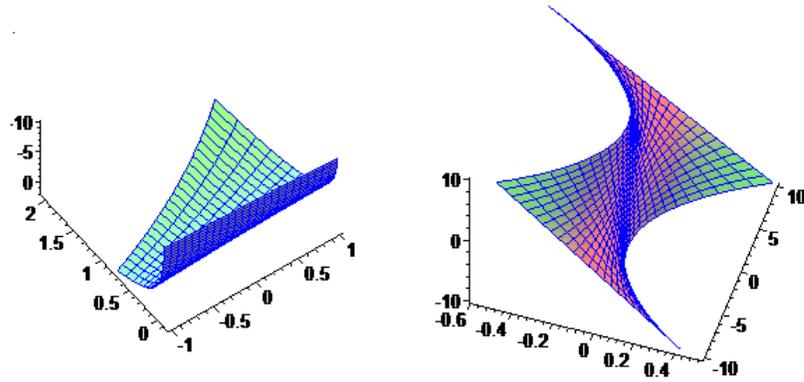


FIGURE 3. A type II TF-flat surfaces parametrized by (3.40) and (3.41), respectively.

Finally, we would like to give the following classification theorem for a type II TF- minimal surface:

Theorem 3.4. *Let M^2 be a type II TF-surface defined by (2.14) in the Galilean 3-space. Then, M^2 is a minimal surface if and only if it belongs to one of the following families:*

- (1) M^2 is an open part of plane,
- (2) M^2 is an admissible surface in \mathbb{G}^3 parametrized by

$$\varphi(s, t) = (s, t, C_1g(t) + C_2), \quad (3.42)$$

where C_1, C_2 are non-zero constant and g is arbitrary function or

$$\varphi(s, t) = (s, t, C_1f(s) + C_2) \quad (3.43)$$

where C_1, C_2 are non-zero constant and f is arbitrary function.

(3) f and g are given by

$$f(s) = -\frac{1}{B}e^{B(c_1s+c_2)} + \frac{A}{B}, \quad g(t) = -\frac{1}{B}e^{B(c_1t+c_2)} + \frac{A}{B}, \quad (3.44)$$

(4) f and g are given by either

(a)

$$f(s) = -\frac{A}{B} + B^{\frac{1-C}{1-C}} \left((1-C)(c_1s + c_2) \right)^{\frac{1}{1-C}}, \quad g(t) = -\frac{A}{B} + B^{\frac{2-C}{1-C}} \left((C-1)(c_1t + c_2) \right)^{\frac{1}{1-C}}, \quad (3.45)$$

or

(b)

$$f(s) = -\frac{A}{B} + B^{\frac{2-C}{1-C}} \left((C-1)(c_1s + c_2) \right)^{\frac{1}{1-C}}, \quad g(t) = -\frac{A}{B} + B^{\frac{1-C}{1-C}} \left((1-C)(c_1t + c_2) \right)^{\frac{1}{1-C}}, \quad (3.46)$$

where c_1, c_2 are non-zero constant and $C \neq 1$.

Proof. Let M^2 be a type II TF-minimal surface. Thus, from (3.37), we have

$$f''g'^2(Bf+A)^2(Bg+A) + g''f'^2(Bg+A)^2(Bf+A) - 2Bf'^2g'^2(Bf+A)(Bg+A) = 0. \quad (3.47)$$

Let us consider on the following possibilities:

Case (1): $f' = 0$ and $g' = 0$. Then, the equation (3.26) is trivially satisfied. By considering these assumptions in (2.14), respectively, we obtain M^2 is an open part of plane. Thus, we have Case (1) of Theorem 3.4.

Case (2): Either $f' = 0$ or $g' = 0$. First, assume that $f' = 0$, i.e., f be constant. In case, the equation (3.30) is trivially satisfied. But, in case g is a arbitrary smooth function. Thus, we have (3.42) in Case (2) of Theorem 3.4. Similarly, by considering the assumption of g as $g' = 0$, we can get (3.43) in Case (2) of Theorem 3.4.

Case (3): Let $f'' = 0$ or $g'' = 0$, but not both. First, assume that $f'' = 0$ and $g'' \neq 0$. Hence, by considering this assumption in (3.47) yields

$$g''(Bg+A)^2 - 2Bg'^2(Bg+A) = 0, \quad (3.48)$$

from which we have two possibilities; $g = -\frac{A}{B}$ or

$$g''(Bg+A) - 2Bg'^2 = 0$$

is valid. But the first statement contradicts with the hypothesis. Hence, we will only deal with the second statement, whose solution is $g(t) = -\frac{1}{B^2(c_1t + c_2)} - \frac{A}{B}$ where $c_1 \neq 0$. Thus, the surface is covered by in Case (4a) in Theorem 3.4 taking $C = 0$.

Second, let $g'' = 0$. Thus, the surface is covered in exactly the same way as in the previous case, as in Case (4b) in Theorem 3.4.

Case (3): f', g' and both f'' and g'' be non-zero. Then, the equation (3.47) can be rewritten as

$$\frac{f''(A + Bf)}{B(f')^2} + \frac{g''(A + Bg)}{B(g')^2} = 2. \tag{3.49}$$

Now, we are going to consider the following cases separately:

Case (3a): $\frac{f''(A + Bf)}{B(f')^2} = 1$ and $\frac{g''(A + Bg)}{B(g')^2} = 1$. From there, we solve these equations to find (3.44) in Case (3) Theorem 3.4.

Case (3b): Let $\frac{f''(A + Bf)}{B(f')^2} = C \neq 1$. From (3.49), one gets $\frac{g''(A + Bg)}{B(g')^2} = 2 - C$. By solving these ODEs, we obtain the functions f, g given in (3.45).

Case (3c): Let $\frac{g''(A + Bg)}{B(g')^2} = C \neq 1$. Similarly, one gets $\frac{f''(A + Bf)}{B(f')^2} = 2 - C$. Thus, we obtain the functions f, g given in (3.46).

Conversely, a direct computation yields that the Gaussian curvature of each of surfaces given in Theorem 3.4 vanishes identically.

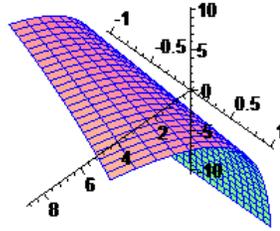


FIGURE 4. A type II TF-minimal surfaces parametrized by (3.44).

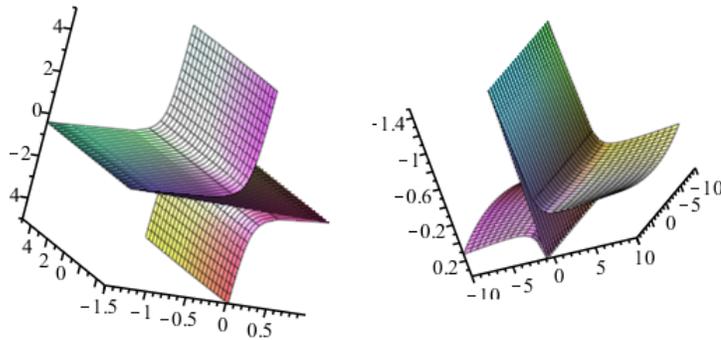


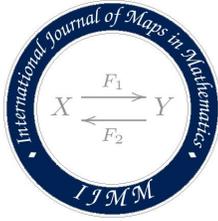
FIGURE 5. A type II TF-minimal surfaces parametrized by (3.45) and (3.46).

ACKNOWLEDGEMENTS

The author would like to thank the referees for their valuable and useful comments that further improve the article.

REFERENCES

- [1] Artykbaev, A., and Sokolov, D. D. (1991). Geometry in the large in a flat space-time. Fan, Tashkent.
- [2] Aydın, M. E., Kūlahcı, M., and Öğrenmiş, A. O. (2018). Non-zero constant curvature factorable surfaces in pseudo-Galilean space, *Comm. Korean Math. Soc*, 33(1), 247-259.
- [3] Aydın, M. E., Kūlahcı, M. A., and Ogrenmis, A. O. (2019). Constant Curvature Translation Surfaces in Galilean 3-Space. *International Electronic Journal of Geometry*, 12(1), 9-19.
- [4] Aydın, M. E., Öğrenmiş, A. O., and Ergüt, M. (2015). Classification of factorable surfaces in the pseudo-Galilean space. *Glasnik matematički*, 50(2), 441-451.
- [5] Dede, M. (2013). Tubular surfaces in Galilean space. *Mathematical Communications*, 18(1), 209-217.
- [6] Dede, M., Ekici, C., and Goemans, W. (2018). Surfaces of Revolution with Vanishing Curvature in Galilean 3-Space. *Journal of Mathematical Physics, Analysis, Geometry*, 14(2), 141-152.
- [7] Dede, M., Ekici, C., Goemans, W., and Unluturk, Y. (2018). Twisted surfaces with vanishing curvature in Galilean 3-space. *International Journal of Geometric Methods in Modern Physics*, 15(01), 1850001.
- [8] Difi SA., Ali H., Zoubir H. (2018). Translation-factorable surfaces in the 3-dimensional Euclidean and Lorentzian spaces satisfying $\Delta r_i = \lambda_i, r_i$, *Electronic Journal of Mathematical Analysis and Applications*, 6(2), 227-236.
- [9] Divjak, B., and Milin Sipus, Z. (2008). Some special surfaces in the pseudo-Galilean space. *Acta Mathematica Hungarica*, 118(3), 209-226.
- [10] Giering, O. (1982). *Vorlesungen über höhere Geometrie*. Friedr. Vieweg and Sohn.
- [11] Klein, F., Fricke, R., and Ostrowski, A. (1921). Ueber die sogenannte nicht-euklidische Geometrie. In *Gesammelte mathematische Abhandlungen* (pp. 254-305). Springer Berlin Heidelberg.
- [12] Karacan, M. K., and Tuncer, Y. (2013). Tubular surfaces of Weingarten types in Galilean and pseudo-Galilean. *Bull. Math. Anal. Appl*, 5(2), 87-100.
- [13] O'neill, B. (1983). *Semi-Riemannian geometry with applications to relativity*. Academic press.
- [14] Palman, D. (1991). Drehyzykliden des Galileischen Raumes G_3 , *Math. Pannon*. 2(1), 98-104.
- [15] Riemann, B. (1923). *Über die Hypothesen welche der Geometrie zugrunde liegen 1867*.
- [16] Roschel O. (1984). *Die Geometrie des Galileischen Raumes*, Bericht der Mathematisch-Statistischen Sektion in der Forschungsgesellschaft Joanneum, Bericht Nr. 256, Habilitationsschrift, Leoben.
- [17] Milin Sipus, Z., and Divjak, B. (2011). Translation surfaces in the Galilean space. *Glasnik matematički*, 46(2), 455-469..
- [18] Milin Sipus, Z., and Divjak, B. (2012). Surfaces of constant curvature in the pseudo-Galilean space. *International Journal of Mathematics and Mathematical Sciences*, 2012.
- [19] Yaglom, I. M. (1979). *A simple non-Euclidean geometry and its physical basis*. Heidelberg Science Library.



SHEFFER STROKE BG-ALGEBRAS

TAHSIN ONER , TUGCE KALKAN , AND NECLA KIRCALI GURSOY *

ABSTRACT. In this paper, Sheffer stroke BG-algebra is defined and its features are investigated. It is indicated that the axioms of a Sheffer stroke BG-algebra are independent. It is stated the connection between a Sheffer stroke BG-algebra and a BG-algebra by defining a unary operation on a Sheffer stroke BG-algebra. After describing a subalgebra and a normal subset of a Sheffer stroke BG-algebra, the relationship of these structures is shown.

Keywords: BG-algebras, Sheffer stroke, Sheffer stroke BG-algebras

2010 Mathematics Subject Classification: 06F05, 03G25.

1. INTRODUCTION

Y. Imai and K. Iséki presented a novel algebraic structure named BCK algebra in 1966. Today, many authors study BCK algebras and this algebra is applied to many branches of mathematics, such as group theory, functional analysis, probability theory, topology, fuzzy set theory, ect. K. Iséki introduced the new idea which is called BCI algebra in 1980 [4]. BCK/BCI algebra is a significant class of logical algebras and is researched by many researchers. Moreover, the class of BCK-algebras is a proper subclass of the class of BCI-algebras.

Neggers and Kim developed a new notion called a B-algebras [8]. B-algebras is connected several classes of algebras of interest such as BCK/BCI-algebras. In addition, BG-algebras which is a generalization of B-algebras was presented by C. B. Kim and H. S. Kim [5].

*Received:*2020.06.29

*Revised:*2020.08.16

*Accepted:*2020.08.18

* Corresponding author

Tahsin Oner; tahsin.oner@ege.edu.tr; <https://orcid.org/0000-0002-6514-4027>

Tugce Kalkan; tugcekalkan92@gmail.com; <https://orcid.org/0000-0002-9721-5424>

Necla Kircali Gursoy; necla.kircali.gursoy@ege.edu.tr; <https://orcid.org/0000-0002-1732-9676>

An algebraic structure BG-algebra was constructed on a non-empty set X with a binary operation $*$ and a constant 0 satisfying some axioms. In 2004, S. S. Ahn and H. D. Lee discussed BG-algebra and some of its properties such as fuzzy subalgebras of BG-algebras [1]. R. Muthuraj et al worked on anti Q-fuzzy BG-ideals in BG-algebra in 2010 [7] and D. K. Basnet investigated on fuzzy ideals of BG-algebras in 2011 [2].

The Sheffer stroke operation, which was first introduced by H. M. Sheffer [13], engages many scientists' attention, because any Boolean function or axiom can be expressed by means of this operation [6]. It reduces axiom systems of many algebraic structures. So, many researchers want to use this operation on their studies. For example, interval Sheffer stroke basic algebras [9], relation between Sheffer stroke operation and Hilbert algebras [10], filters of strong Sheffer stroke non-associative MV-algebras [11], (Fuzzy) filters of Sheffer stroke BL-algebras [12] and Sheffer operation in ortholattices [3] are given as some research on Sheffer stroke operation in recent years.

After giving basic definitions and notions about a Sheffer stroke and a BG-algebra, it is defined a Sheffer stroke BG-algebra. By presenting fundamental notions about this algebraic structure, it is proved that the axiom system of a Sheffer stroke BG-algebra is independent. Sheffer stroke B-algebra is defined and it is indicated that the axioms of a Sheffer stroke B-algebra are independent. The relationship between a Sheffer stroke BG-algebra and a Sheffer stroke B-algebra is indicated. It is shown that the connection between a Sheffer stroke BG-algebra and a BG-algebra and Cartesian product of two Sheffer stroke BG-algebras is a Sheffer stroke BG-algebra. A subalgebra and a normal subset of a Sheffer stroke BG-algebra is defined and the relationship between this structures is demonstrated. Finally, it is shown that the Sheffer stroke BG-algebra is a group-derived under one condition.

2. PRELIMINARIES

In this part, we give the basic definitions and notions about a Sheffer stroke and a BG-algebra.

Definition 2.1. [3] *Let $\mathcal{A} = \langle A, | \rangle$ be a groupoid. The operation $|$ is said to be Sheffer stroke if it satisfies the following conditions:*

$$(S1) \ a_1|a_2 = a_2|a_1,$$

$$(S2) \ (a_1|a_1)|(a_1|a_2) = a_1,$$

$$(S3) \ a_1|((a_2|a_3)|(a_2|a_3)) = ((a_1|a_2)|(a_1|a_2))|a_3,$$

$$(S4) \ (a_1|((a_1|a_1)|(a_2|a_2))|(a_1|((a_1|a_1)|(a_2|a_2)))) = a_1.$$

Definition 2.2. [5] *A BG-algebra is a non-empty set A with a constant 0 and a binary operation $*$ satisfying the following axioms:*

$$(BG.1) \quad a_1 * a_1 = 0,$$

$$(BG.2) \quad a_1 * 0 = a_1,$$

$$(BG.3) \quad (a_1 * a_2) * (0 * a_2) = a_1,$$

for all $a_1, a_2 \in A$.

A BG-algebra is called bounded if it has the greatest element.

Lemma 2.1. [5] *In a BG-algebra A , the following properties hold for all $a_1, a_2, a_3 \in A$:*

$$(i) \quad a_1 * a_2 = a_3 * a_2 \text{ implies } a_1 = a_3,$$

$$(ii) \quad 0 * (0 * a_1) = a_1,$$

$$(iii) \quad \text{If } a_1 * a_2 = 0, \text{ then } a_1 = a_2,$$

$$(iv) \quad \text{If } 0 * a_1 = 0 * a_2, \text{ then } a_1 = a_2,$$

$$(v) \quad (a_1 * (0 * a_1)) * a_1 = a_1.$$

Definition 2.3. [5] *A nonempty subset S of a BG-algebra A is called a BG-subalgebra if $a_1 * a_2 \in S$, for all $a_1, a_2 \in S$.*

Definition 2.4. [8] *Let A be a BG-algebra. A nonempty subset N of A is said to be normal if $(a_1 * x) * (a_2 * y) \in N$ for any $a_1 * a_2, x * y \in N$.*

Definition 2.5. [8] *A B-algebra is a non-empty set A with a constant 0 and a binary operation $*$ satisfying the following axioms:*

$$(i) \quad a_1 * a_1 = 0,$$

$$(ii) \quad a_1 * 0 = a_1,$$

$$(iii) \quad (a_1 * a_2) * a_3 = a_1 * (a_3 * (0 * a_2)),$$

for all $a_1, a_2, a_3 \in A$.

3. SHEFFER STROKE BG-ALGEBRAS

In this part, we define a Sheffer Stroke BG-algebra and give some properties.

Definition 3.1. *A Sheffer stroke BG-algebra is an algebra $(A, |, 0)$ of type $(2, 0)$ such that 0 is the constant in A and the following axioms are satisfied:*

$$(sBG.1) \quad (a_1 | (a_1 | a_1)) | (a_1 | (a_1 | a_1)) = 0,$$

$$(sBG.2) \quad (0 | (a_2 | a_2)) | (a_1 | (a_2 | a_2)) | (a_1 | (a_2 | a_2)) = a_1 | a_1,$$

for all $a_1, a_2 \in A$.

Let A be a Sheffer stroke BG-algebra, unless otherwise is indicated.

Lemma 3.1. *The axioms (sBG.1) and (sBG.2) are independent.*

Proof.

(1) Independence of (sBG.1):

We construct an example for this axiom which is false while (sBG.2) is true. Let $(\{0, 1\}, |_1)$ be the groupoid defined as follows:

$$\begin{array}{c|cc} |_1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 0 \end{array}$$

Then $|_1$ satisfies (sBG.2) but not (sBG.1) when $a_1 = 1$.

(2) Independence of (sBG.2):

Let $(\{0, 1\}, |_2)$ be the groupoid defined as follows:

$$\begin{array}{c|cc} |_2 & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & 0 \end{array}$$

Then $|_2$ satisfies (sBG.1) but not (sBG.2) when $a_1 = 1$ and $a_2 = 1$.

Lemma 3.2. *Let A be a Sheffer stroke BG-algebra. Then the following features hold for all $a_1, a_2, a_3 \in A$:*

- (1) $(0|0)|(a_1|a_1) = a_1$,
- (2) $(a_1|(0|0)|(a_1|(0|0)) = a_1$,
- (3) $(a_1|(a_2|a_2)|(a_1|(a_2|a_2)) = (a_3|(a_2|a_2)|(a_3|(a_2|a_2))$ implies $a_1 = a_3$,
- (4) $(0|(0|(a_1|a_1))) = a_1|a_1$,
- (5) *If $(a_1|(a_2|a_2)|(a_1|(a_2|a_2)) = 0$ then $a_1 = a_2$,*
- (6) *If $(0|(a_1|a_1)) = (0|(a_2|a_2))$ then $a_1 = a_2$,*
- (7) $((a_1|(0|(a_1|a_1))|(a_1|(0|(a_1|a_1))))|(a_1|a_1)) = a_1|a_1$,
- (8) $(a_1|(a_1|a_1)|(a_1|a_1)) = a_1$.

Proof.

(1) By using (sBG.1), (S1) and (S2), we obtain

$$\begin{aligned}
(0|0)|(a_1|a_1) &= (((a_1|(a_1|a_1))|(a_1|(a_1|a_1))))|((a_1|(a_1|a_1))|(a_1|(a_1|a_1))))|(a_1|a_1) \\
&= (a_1|(a_1|a_1))|(a_1|a_1) \\
&= (a_1|a_1)|(a_1|(a_1|a_1)) \\
&= a_1.
\end{aligned}$$

(2) By using (S1), (S2) and (1), we have

$$\begin{aligned}
(a_1|(0|0))|(a_1|(0|0)) &= (((a_1|(a_1)|(a_1|a_1))|(0|0))|((a_1|(a_1)|(a_1|a_1))|(0|0))) \\
&= ((0|0)|((a_1|a_1)|(a_1|a_1)))|((0|0)|((a_1|a_1)|(a_1|a_1))) \\
&= (a_1|a_1)|(a_1|a_1) \\
&= a_1.
\end{aligned}$$

(3) Let $(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) = (a_3|(a_2|a_2))|(a_3|(a_2|a_2))$. By using (sBG.1), we get

$$\begin{aligned}
a_1|a_1 &= (0|(a_2|a_2))|((a_1|(a_2|a_2))|(a_1|a_2|a_2)) \\
&= (0|(a_2|a_2))|((a_3|(a_2|a_2))|(a_3|a_2|a_2)) \\
&= a_3|a_3.
\end{aligned}$$

By using (S2), we have $a_1 = (a_1|a_1)|(a_1|a_1) = (a_3|a_3)|(a_3|a_3) = a_3$.

(4) In (sBG.2), we substitute $[a_2 := a_1]$ and by using (sBG.1) and (S1), we obtain

$$\begin{aligned}
a_1|a_1 &= (0|(a_1|a_1))|((a_1|(a_1|a_1))|(a_1|(a_1|a_1))) \\
&= (0|(a_1|a_1))|0 \\
&= 0|(0|(a_1|a_1)).
\end{aligned}$$

(5) By using (sBG.1) and (3), we get $(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) = 0 = (a_2|(a_2|a_2))|(a_2|(a_2|a_2))$. Then $a_1 = a_2$.

(6) In (sBG.2) we substitute $[a_2 := a_1]$ and by using (sBG.1), we obtain

$$\begin{aligned}
a_1|a_1 &= (0|(a_1|a_1))|(a_1|(a_1|a_1))|(a_1|(a_1|a_1)) \\
&= (0|(a_1|a_1))|0 \\
&= (0|(a_2|a_2))|0 \\
&= (0|(a_2|a_2))|(a_2|(a_2|a_2))|(a_2|(a_2|a_2)) \\
&= a_2|a_2.
\end{aligned}$$

Thus, $a_1 = (a_1|a_1)|(a_1|a_1) = (a_2|a_2)|(a_2|a_2) = a_2$ from (S2).

(7) In (sBG.2) we substitute $[a_2 := (0|(a_1|a_1))|(0|(a_1|a_1))]$ and by using (S1), (S2) and (4), we get

$$\begin{aligned}
a_1|a_1 &= (((a_1|(0|(a_1|a_1))))|(a_1|(0|(a_1|a_1))))|(0|(0|(a_1|a_1))) \\
&= (((a_1|(0|(a_1|a_1))))|(a_1|(0|(a_1|a_1))))|(a_1|a_1).
\end{aligned}$$

(8) Substituting $[a_2 := (a_1|a_1)]$ in (S2), we obtain

$$(a_1|a_1)|(a_1|(a_1|a_1)) = a_1.$$

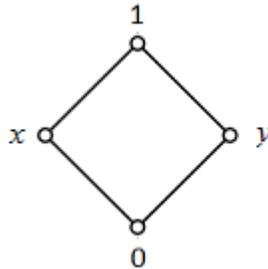
By using (S1), we get $(a_1|(a_1|a_1))|(a_1|a_1) = a_1$.

Definition 3.2. A Sheffer stroke B -algebra is an algebra $(A, |, 0)$ of type $(2, 0)$, where A is a non-empty set, 0 is the constant in A and $|$ is Sheffer stroke on A , such that the following identities are satisfied for all $a_1, a_2, a_3 \in A$:

$$(sB.1) (a_1|(a_1|a_1))|(a_1|(a_1|a_1)) = 0,$$

$$(sB.2) ((a_1|(a_2|a_2))|(a_1|(a_2|a_2))|(a_3|a_3) = (a_1|(a_3|(0|(a_2|a_2)))).$$

Example 3.1. Consider $(A, |, 0)$ with the following Hasse diagram, where $A = \{0, x, y, 1\}$:



The binary operation $|$ on A has Cayley table as follow:

	0	x	y	1
0	1	1	1	1
x	1	y	1	y
y	1	1	x	x
1	1	y	x	0

Then this structure is a Sheffer stroke B -algebra.

Lemma 3.3. *The axioms (sB.1) and (sB.2) are independent.*

Proof.

(1) Independence of (sB.1):

We construct an example for this axiom which is false while (sB.2) is true. Let $(\{0, 1\}, |_3)$ be the groupoid defined as follows:

$ _3$	0	1
0	1	1
1	0	0

Then $|_3$ satisfies (sB.2) but not (sB.1) when $a_1 = 1$.

(2) Independence of (sB.2):

Let $(\{0, 1\}, |_4)$ be the groupoid defined as follows:

$ _4$	0	1
0	1	1
1	1	0

Then $|_4$ satisfies (sB.1) but not (sB.2) when $a_1 = 1$, $a_2 = 1$ and $a_3 = 0$.

Theorem 3.1. *Every Sheffer stroke B -algebra is a Sheffer stroke BG -algebra.*

Proof. Since the axioms (sB.1) and (sBG.1) are the same, we show only (sBG.2).

By using (S1), (S2), (sB.2) and Lemma 3.2 (2), we have

$$\begin{aligned}
(0|(a_2|a_2))|(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) &= ((a_1|(a_2|a_2))|(a_1|(a_2|a_2))|((0|(a_2|a_2))|(0|(a_2|a_2))| \\
&\quad (0|(a_2|a_2))|(0|(a_2|a_2))) \\
&= (a_1|(((0|(a_2|a_2))|(0|(a_2|a_2))))|(0|(a_2|a_2))) \\
&= (a_1|((0|(a_2|a_2))|((0|(a_2|a_2))|(0|(a_2|a_2)))) \\
&= (a_1|(0|0)) \\
&= a_1|a_1.
\end{aligned}$$

Theorem 3.2. *Let $(A, |, 0)$ be a Sheffer stroke BG-algebra. If we define*

$$a_1 * a_2 := (a_1|(a_2|a_2))|(a_1|a_2|a_2),$$

*then $(A, *, 0)$ is a BG-algebra.*

Proof. By using (S1), (S2), (sBG.1), (sBG.2), Lemma 3.2 (2), we have:

$$(BG.1) : a_1 * a_1 = (a_1|(a_1|a_1))|(a_1|(a_1|a_1)) = 0.$$

$$(BG.2): a_1 * 0 = (a_1|(0|0))|(a_1|(0|0)) = a_1.$$

(BG.3):

$$\begin{aligned} (a_1 * a_2) * (0 * a_2) &= ((a_1|(a_2|a_2))|(a_1|(a_2|a_2)))|((0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))| \\ &\quad (0|(a_2|a_2)))|((a_1|(a_2|a_2))|(a_1|(a_2|a_2)))|((0|(a_2|a_2))|(0|(a_2|a_2))| \\ &\quad (0|(a_2|a_2))|(0|(a_2|a_2))) \\ &= (((a_1|(a_2|a_2))|(a_1|(a_2|a_2)))|(0|(a_2|a_2)))|(((a_1|(a_2|a_2))|(a_1|(a_2|a_2))) \\ &\quad |(0|(a_2|a_2))) \\ &= (0|(a_2|a_2))|(a_1|(a_2|a_2))|(a_1|(a_2|a_2))|(0|(a_2|a_2))|(a_1|(a_2|a_2))|(a_1 \\ &\quad |(a_2|a_2)) \\ &= (a_1|a_1)|(a_1|a_1) \\ &= a_1. \end{aligned}$$

Theorem 3.3. *Let $(A, *, 0, 1)$ be a bounded BG-algebra. If we define*

$$a_1|a_2 := (a_1 * a_2^0)^0,$$

where $a_1^0 = a_1|a_1$, then $(A, |, 0)$ is a Sheffer stroke BG-algebra.

Proof. (i) By using (BG.1), we have

$$\begin{aligned} (a_1|(a_1|a_1))|(a_1|(a_1|a_1)) &= (a_1|a_1^0)|(a_1|a_1^0) \\ &= (a_1 * a_1)^0|(a_1 * a_1)^0 \\ &= ((a_1 * a_1)^0)^0 \\ &= a_1 * a_1 \\ &= 0. \end{aligned}$$

(ii) By using (BG.2), we obtain

$$\begin{aligned}
((a_1|(a_2|a_2))|(a_1|(a_2|a_2))|(0|(a_2|a_2))) &= ((a_1 * a_2)^0|(a_1 * a_2)^0)|(0 * a_2)^0 \\
&= ((a_1 * a_2)^0)^0|(0 * a_2)^0 \\
&= (a_1 * a_2)|(0 * a_2)^0 \\
&= ((a_1 * a_2) * (0 * a_2))^0 \\
&= (a_1)^0 \\
&= a_1|a_1.
\end{aligned}$$

Theorem 3.4. *Let $(A, |_A, 0_A)$ and $(B, |_B, 0_B)$ be Sheffer stroke BG-algebras. Then, $(A \times B, |_{A \times B}, 0_{A \times B})$ is a Sheffer stroke BG-algebra, where the operation $|_{A \times B}$ is defined by*

$$(a_1, b_1)|_{A \times B}(a_2, b_2) = (a_1|_A a_2, b_1|_B b_2)$$

and $0_{A \times B} = (0_A, 0_B)$.

Definition 3.3. *A non-empty subset S of a Sheffer stroke BG-algebra A is called a Sheffer stroke BG-subalgebra of A if $(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) \in S$ for all $a_1, a_2 \in S$.*

Theorem 3.5. *Let $(A, |, 0)$ be a Sheffer stroke BG-algebra and $\emptyset \neq S \subseteq A$. Then the following are equivalent:*

- (a) S is a subalgebra of A ,
- (b) $(a_1|(0|(a_2|a_2))|(a_1|(0|(a_2|a_2)))) \in S$, $(0|(a_2|a_2))|(0|(a_2|a_2)) \in S$ for any $a_1, a_2 \in S$.

Proof. (a) \Rightarrow (b): Since $S \neq \emptyset$, there exists an element $a_1 \in S$ and $0 = (a_1|(a_1|a_1))|(a_1|(a_1|a_1)) \in S$. Since S is closed under $|$, $(0|(a_2|a_2))|(0|(a_2|a_2)) \in S$ and thus $(a_1|((0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))))|(a_1|((0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2)))) \in S$. From (S2), we get $(a_1|(0|(a_2|a_2))|(a_1|(0|(a_2|a_2)))) \in S$.

(b) \Rightarrow (a): By using Lemma 3.2 (4), $(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) = (a_1|((0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2)))))|(a_1|((0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2)))))|(a_1|(a_2|a_2))|(a_1|(a_2|a_2)) \in S$ for any $a_1, a_2 \in S$.

Definition 3.4. *Let A be a Sheffer stroke BG-algebra. A non-empty subset N of A is said to be normal subset of A if*

$$(((a_1|(x|x))|(a_1|(x|x))|(a_2|(y|y))))|(((a_1|(x|x))|(a_1|(x|x))|(a_2|(y|y)))) \in N,$$

for any $(a_1|(a_2|a_2))|(a_1|(a_2|a_2)), (x|(y|y))|(x|(y|y)) \in N$.

Then 0 acts like an identity element on A . Since

$$\begin{aligned}
a_1 \circ (0|(a_1|a_1))|(0|(a_1|a_1)) &= (a_1|(0|((0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1)))) \\
&\quad |(a_1|(0|((0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1)))) \\
&= (a_1|(0|(0|a_1|a_1))|(a_1|(0|(0|a_1|a_1))) \\
&= (a_1|((0|(0|a_1|a_1))|(0|(0|a_1|a_1))|(0|(0|a_1|a_1))|(0|(0|a_1|a_1)))) \\
&\quad |(a_1|((0|(0|a_1|a_1))|(0|(0|a_1|a_1))|(0|(0|a_1|a_1))|(0|(0|a_1|a_1)))) \\
&= (a_1|(a_1|a_1))|(a_1|(a_1|a_1)) \\
&= 0
\end{aligned}$$

and

$$\begin{aligned}
((0|(a_1|a_1))|(0|(a_1|a_1))) \circ a_1 &= ((0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1))|(0|(a_1|a_1))| \\
&\quad (0|(a_1|a_1))|(0|(a_1|a_1))) \\
&= 0,
\end{aligned}$$

we obtain that $(0|(a_1|a_1))|(0|(a_1|a_1))$ behaves like a multiplicative inverse for a_1 with respect to the operation "o". We claim that $(A; \circ)$ is a semi-group. Indeed,

$$\begin{aligned}
a_1 \circ (a_2 \circ a_3) &= (a_1|(0|(a_2|(0|(a_3|a_3))))|(a_1|(0|(a_2|(0|(a_3|a_3)))) \\
&= (a_1|(0|((0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))))|(0|(a_3|a_3))))|(a_1|(0|((0|(0|(a_2|a_2)) \\
&\quad |(0|(0|(a_2|a_2))))|(0|(a_3|a_3)))) \\
&= (a_1|(0|((0|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(0|(a_2|a_2))| \\
&\quad (0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))))|(0|(a_3|a_3))))|(a_1|(0|((0|(0|(a_2|a_2)) \\
&\quad |(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2)) \\
&\quad |(0|(a_2|a_2))))|(0|(a_3|a_3)))) \\
&= ((a_1|(0|(a_2|a_2))|(a_1|(0|(a_2|a_2))))|(0|(a_3|a_3))|(a_1|(0|(a_2|a_2)))) \\
&\quad |(a_1|(0|(a_2|a_2))|(0|(a_3|a_3))) \\
&= (a_1 \circ a_2) \circ a_3.
\end{aligned}$$

Note that

$$\begin{aligned}
a_1 \circ (a_2)^{-1} &= (a_1|(0|((0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2))))|(a_1|(0|((0|(a_2|a_2)) \\
&\quad |(0|(a_2|a_2))|(0|(a_2|a_2))|(0|(a_2|a_2)))) \\
&= (a_1|(0|(0|(a_2|a_2))))|(a_1|(0|(0|(a_2|a_2)))) \\
&= (a_1|(((0|(0|(a_2|a_2))))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))))| \\
&\quad (a_1|(((0|(0|(a_2|a_2))))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2))|(0|(0|(a_2|a_2)))))) \\
&= (a_1|(a_2|a_2))|(a_1|(a_2|a_2)).
\end{aligned}$$

Hence $(A; |, 0)$ is also a group-derived Sheffer stroke BG-algebra. This completes the proof.

4. CONCLUSION

In this study, we introduce a Sheffer stroke BG-algebra, Cartesian product, a subalgebra, a normal subset and their some properties. After giving basic definitions and notions about Sheffer stroke and a BG-algebra, we describe a Sheffer stroke BG-algebra and a Sheffer stroke B-algebra and present basic notions about this algebraic structures. We indicate that the axiom systems of a Sheffer stroke BG-algebra and a Sheffer stroke B-algebra are independent. We show that a Sheffer stroke BG-algebra is a BG-algebra and that Cartesian product of two Sheffer stroke BG-algebras is a Sheffer stroke BG-algebra. After defining a subalgebra and a normal subset, we present the relationship between a subalgebra and a normal subset on Sheffer stroke BG-algebra. Finally, we show that the Sheffer stroke BG-algebra is a group-derived under one condition.

Acknowledgments. The authors would like to thank the referee for some useful comments and their helpful suggestions that have improved the quality of this paper.

REFERENCES

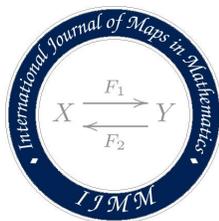
- [1] Ahn, S. S., Lee, H. D. (2004). Fuzzy subalgebras of BG-algebras. *Communications of the Korean Mathematical Society*, 19(2), 243-251.
- [2] Basnet, D. K., Singh, L. B. (2011). fuzzy ideal of BG-algebra. *International Journal of Algebra*, 5(15), 703-708.
- [3] Chajda, I. (2005). Sheffer operation in ortholattices. *Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica*, 44(1), 19-23.
- [4] Iséki K.(1980). On BCI-algebras, *Mathematics Seminar Notes* 8(1): 125–130.
- [5] Kim, C. B., Kim, H. S. (2008). On BG-algebras. *Demonstratio Mathematica*, 41(3), 497-506.

- [6] McCune, W., Veroff, R., Fitelson, B., Harris, K., Feist, A., Wos, L. (2002). Short single axioms for Boolean algebra. *Journal of Automated Reasoning*, 29(1), 1-16.
- [7] Muthuraj, R., Sridharan, M., Muthuraman, M. S., Sitharselvam, P. M. (2010). Anti Q-Fuzzy BG-Ideals in BG-Algebra. *International Journal of Computer Applications*, 975, 8887.
- [8] Neggers, J., Sik, K. (2002). On B-algebras. *Matematički vesnik*, 54(1-2), 21-29.
- [9] Oner, T., Katican, T., Ülker, A. (2019). Interval sheffer stroke basic algebras. *TWMS Journal of Applied and Engineering Mathematics*, 9(1), 134-141.
- [10] Oner, T., Katican, T., Borumand Saeid, A. (2020). Relation between Sheffer Stroke and Hilbert algebras. *Categories and General Algebraic Structures with Applications*.
- [11] Oner, T, Katican T, Borumand Saeid A, Terziler M. (2020). Filters of strong Sheffer stroke non-associative MV-algebras, *Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica*.
- [12] Oner T, Katican T, Borumand Saeid A. (2023). (Fuzzy) Filters of Sheffer Stroke BL Algebras, *Kragujevac Journal of Mathematics*, 47(1), 39–55.
- [13] Sheffer, H. M. (1913). A set of five independent postulates for Boolean algebras, with application to logical constants. *Transactions of the American mathematical society*, 14(4), 481-488.

DEPARTMENT OF MATHEMATICS, EGE UNIVERSITY

DEPARTMENT OF MATHEMATICS, EGE UNIVERSITY

TIRE VOCATIONAL SCHOOL, EGE UNIVERSITY



PLANE CURVES WITH SAME EQUI-AFFINE AND EUCLIDEAN INVARIANTS

MUHITTIN EVREN AYDIN , ESRA ERDEM , AND MUNEVVER YILDIRIM YILMAZ *

ABSTRACT. In the present paper, we consider and solve the problem of finding parametric plane curves with the same equi-affine and Frenet curvatures. We then classify the parametric plane curves with prescribed equi-affine curvature by solving certain ordinary differential equations. Our classification generalizes the plane curves with constant equi-affine curvature. Several examples are also given by figures.

Keywords: Plane curve, Equiaffine transformation, Equiaffine curvature, Euclidean curvature

2010 Mathematics Subject Classification: Primary 53A10; Secondary 53C42, 53C44, 34A05.

1. INTRODUCTION

Affine Differential Geometry, since nineteenth century, has been investigated and developed by a larger group of geometers led by Pick, Tzitzeica, Berwald, Blaschke among others. See [13] for this process in detail. This branch of Geometry is based on the study of the invariant properties of affine n -space \mathbb{R}^n under the (equi-)affine transformations.

The theory of curves in \mathbb{R}^n has had a great interest from past to present [1, 2, 4, 5, 10, 11, 16, 18, 20, 21, 23, 24]. In this paper, we mainly consider the problem of finding parametric plane curves with the same equi-affine and Frenet curvatures. For example, a unit circle in

Received:2020.06.23

Revised:2020.07.27

Accepted:2020.09.02

* Corresponding author

Muhittin Evren Aydın; meaydin@firat.edu.tr; <https://orcid.org/0000-0001-9337-8165>

Esra Erdem; esra.6666.23@gmail.com; <https://orcid.org/0000-0001-8656-0196>

Munevver Yıldırım Yılmaz; myildirim@firat.edu.tr; <https://orcid.org/0000-0003-1278-3981>

the Euclidean setting has the same constant equi-affine and Frenet curvatures, i.e. 1. We find the motivation for this study from [3, equation 28], [17, Theorem 4, Theorem 5], [22, Remark 6]. Although, in these cited papers, all authors constructed certain relations between the equi-affine and Frenet curvatures for a 2d curve, as far as we know, to solve our main problem has been overlooked till now.

In the context of affine curves, another interest has been to find the parametric equations of the curves with prescribed affine curvatures, see [9, 8, 14, 25]. As a secondary purpose of this paper, we follow this mainstream and classify parametric plane curves with prescribed equi-affine curvatures by solving certain vector ordinary differential equations (ODEs).

The framework of this paper can be explained as follows in detail.

Let \mathbb{R}^2 be the affine plane equipped with a fixed area form $|\cdot \cdot|$ such that $|\mathbf{u} \mathbf{v}| = u_1v_2 - u_2v_1$, for some vectors $\mathbf{u} = (u_1, u_2)$ and $\mathbf{v} = (v_1, v_2)$. The *equi-affine group* of \mathbb{R}^2 is generated by the action of the special linear group $SL(2, \mathbb{R})$ and the group of translations of \mathbb{R}^2 . An *equi-affine transformation* of \mathbb{R}^2 is given in matrix form

$$\bar{\mathbf{x}} = A\mathbf{x} + \mathbf{b}, \quad (1.1)$$

where $\bar{\mathbf{x}}, \mathbf{x}, \mathbf{b} \in \mathbb{R}^{2 \times 1}$ and $A \in SL(2, \mathbb{R})$. Point out that the area of a parallelogram is preserved by (1.1) and hence it is so-called *area-preserving affine transformation* [15].

(1.1) turns to a *Euclidean transformation* of \mathbb{R}^2 if $A \in SO(2)$ [6]. By an *equi-affine* (resp. a *Euclidean*) *invariant* we mean a property of \mathbb{R}^2 that remains unchanged under the equi-affine (resp. Euclidean) group.

Let $\mathbf{x} = \mathbf{x}(\sigma) = (x(\sigma), y(\sigma))$, $\sigma \in I \subset \mathbb{R}$, be a smooth parametric curve in \mathbb{R}^2 . The equi-affine arc-length parameter σ and curvature κ_a of \mathbf{x} are equi-affine invariants of \mathbb{R}^2 while the Euclidean arc-length parameter s and Frenet curvature κ_f of \mathbf{x} are Euclidean invariants. The Fundamental Theorem of equi-affine (Euclidean) plane curves implies that a plane curve with constant equi-affine (Frenet) curvature is a quadratic curve (a straight line or a circle) [15, 19]. An equi-affine plane curve with constant equi-affine curvature is homogeneous, i.e. the orbit of a point under a 1-parameter group of the transformations given by (1.1). The converse is true as well [7].

We point out that a unit circle in the Euclidean setting has the same constant equi-affine and Frenet curvatures (i.e. $\kappa_a = \kappa_f = 1$) as well as the same arc-length parameters. Naturally the following question occurs: *is there any plane curve \mathbf{x} with $\kappa_a = \kappa_f$ besides the unit circle in the Euclidean setting?* In the mean while, we state that the plane curve \mathbf{x} is

a unit circle in the Euclidean setting if and only if its equi-affine and Euclidean arc-length parameters are same (see Lemma 3.1.) We answer to this question (see Theorem 3.2) by assuming that \mathbf{x} has different equi-affine and Euclidean arc-length parameters, because it turns to a unit circle in the Euclidean setting otherwise.

It is worth to specify that, in centro-affine context, Liu [14, Proposition 4.1] obtained a characterization for a plane curve in terms of its Frenet curvature that the centro-affine and Euclidean arc-length parameters are same.

Furthermore, by solving a vector ODE of Euler-Cauchy type [12, p. 69] we obtain the parametric plane curves with $\kappa_a(\sigma) = a(b\sigma + c)^{-2}$, for some constants a, b, c with $b^2 + c^2 \neq 0$. When a or b is equal to zero, these reduce to the plane curves with constant equi-affine curvature and thus our case is more general.

2. PRELIMINARIES

Theorem 2.1. *We provide basic differential geometric objects of plane curves from [6, 7, 15, 19].*

2.1. Equi-affine plane curves. Let $\mathbf{x} = \mathbf{x}(t) = (x(t), y(t))$, $t \in I \subset \mathbb{R}$, be a *non-degenerate* smooth parametric curve in \mathbb{R}^2 , namely $|\dot{\mathbf{x}} \ddot{\mathbf{x}}| \neq 0$ for any t , where $\dot{\mathbf{x}} = \frac{d\mathbf{x}}{dt}$ and $\ddot{\mathbf{x}} = \frac{d^2\mathbf{x}}{dt^2}$. This yields that nowhere \mathbf{x} has inflection points. *Equi-affine arc-length function* σ is defined by

$$\sigma(t) = \int_{t_0}^t \sqrt[3]{|\dot{\mathbf{x}} \ddot{\mathbf{x}}|} dt. \quad (2.1)$$

Denote $\mathbf{x}' = \frac{d\mathbf{x}}{d\sigma}$ and $\mathbf{x}'' = \frac{d^2\mathbf{x}}{d\sigma^2}$. It follows

$$|\mathbf{x}' \mathbf{x}''| = 1 \text{ for all } \sigma, \quad (2.2)$$

in which the parameter σ is said to be *equi-affine arc-length*. Taking derivative of (2.2) with respect to σ yields $|\mathbf{x}' \mathbf{x}'''| = 0$, which means that \mathbf{x}' and \mathbf{x}''' are linearly dependent. Then there exist a function κ_a of σ such that $\mathbf{x}''' = -\kappa_a \mathbf{x}'$. Therefore the following occurs

$$\kappa_a(\sigma) = |\mathbf{x}'' \mathbf{x}'''|, \quad (2.3)$$

called *equi-affine curvature* of \mathbf{x} . Because κ_a is given by determinant, it is invariant of equi-affine transformations of \mathbb{R}^2 . It is also clear that the following vector ODE holds

$$\mathbf{x}''' + \kappa_a \mathbf{x}' = 0. \quad (2.4)$$

The Fundamental Theorem of equi-affine plane curves states that for a given smooth function $\kappa_a(\sigma)$, $\sigma \in I$, there exist a unique equi-affine plane curve \mathbf{x} admitting σ as equi-affine arc-length and κ_a as equi-affine curvature up to an equi-affine transformation of \mathbb{R}^2 . In this regard, if $\kappa_a(\sigma)$ is a constant function then the solutions of (2.4) yield that, up to suitable equi-affine transformations, \mathbf{x} is either a parabola ($\kappa_a = 0$) or an ellipse ($\kappa_a > 0$) or a hyperbola ($\kappa_a < 0$) given in explicit forms $y = \frac{1}{2}x^2$ and $\kappa_a x^2 + \kappa_a^2 y^2 = 1$. Point out that \mathbf{x} turns to a unit circle in the Euclidean setting when $\kappa_a = 1$ identically.

2.2. Euclidean plane curves. Let $\mathbf{x} = \mathbf{x}(t) = (x(t), y(t))$, $t \in I \subset \mathbb{R}$, be a *regular* smooth parametric curve in the Euclidean plane \mathbb{E}^2 , namely $\|\dot{\mathbf{x}}\| \neq 0$ for any t , where $\|\cdot\|$ stands for the Euclidean norm. *Euclidean arc-length function* s of \mathbf{x} is given by

$$s(t) = \int_{t_0}^t \|\dot{\mathbf{x}}\| dt,$$

in which $\frac{ds}{dt}$ is strictly positive and the inverse of s exists. Therefore $\mathbf{x}(s^{-1}(t))$ is so-called *unit-speed* curve, i.e. $\left\| \frac{d\mathbf{x}(s^{-1}(t))}{dt} \right\| = 1$, and the parameter s is said to be *Euclidean arc-length*. If $\mathbf{x} = \mathbf{x}(s)$ is a unit-speed curve then its *Frenet curvature* is given by $\kappa_f(s) = \left\| \frac{d^2\mathbf{x}}{ds^2} \right\|$. In this sense, there is a smooth function θ of s , called *turning angle* of \mathbf{x} , such that

$$\frac{d\mathbf{x}}{ds} = (\cos \theta(s), \sin \theta(s)). \tag{2.5}$$

Here we easily get $\kappa_f(s) = \left| \frac{d\theta}{ds} \right|$. Note that $\frac{d\theta}{ds}$ is also called the *signed Frenet curvature* of \mathbf{x} .

The Fundamental Theorem of Euclidean plane curves states that for given smooth function $\kappa_f(s)$, $s \in I$, there exist a unique Euclidean plane curve \mathbf{x} admitting s as Euclidean arc-length and κ_f as signed Frenet curvature up to a Euclidean transformation of \mathbb{E}^2 . In this regard, if $\kappa_f(s)$ is a constant function then the solutions of (2.5) yield that, up to suitable Euclidean transformations, \mathbf{x} is either a straight line ($\kappa_f = 0$) or a circle ($\kappa_f \neq 0$) with radius $\frac{1}{\kappa_f}$.

3. PLANE CURVES WITH $\kappa_a = \kappa_f$

Throughout the section, for a plane curve, the equi-affine arc-length parameter is denoted by σ , the Euclidean arc-length parameter by s , the equi-affine curvature by κ_a and the Frenet curvature by κ_f .

Lemma 3.1. *Let \mathbf{x} be a non-degenerate smooth parameterized curve in \mathbb{R}^2 by the same equi-affine and Euclidean arc-length parameters. Then, up to a Euclidean transformation, it is the quadratic curve with $\kappa_a = 1$ parameterized by $\mathbf{x}(\sigma) = (\cos \sigma, \sin \sigma)$.*

Remark 3.1. *In Euclidean setting it is the unit circle and its Frenet curve is also $\kappa_f = 1$.*

Proof. Let σ denote both the equi-affine and Euclidean arc-length parameters of \mathbf{x} . It then follows

$$\|\mathbf{x}'\| = |\mathbf{x}' \mathbf{x}''| = 1, \quad (3.1)$$

where $\mathbf{x}' = \frac{d\mathbf{x}}{d\sigma}$ and $\mathbf{x}'' = \frac{d^2\mathbf{x}}{d\sigma^2}$. Denoting the curve \mathbf{x} as $\mathbf{x}(\sigma) = (x(\sigma), y(\sigma))$ and using (3.1) we get

$$(x')^2 + (y')^2 = 1 \quad (3.2)$$

and

$$x'y'' - x''y' = 1. \quad (3.3)$$

Differentiating (3.2) with respect to σ we have

$$x'x'' + y'y'' = 0 \text{ or } x'' = \frac{-y'y''}{x'}, \quad (3.4)$$

where $x' \neq 0$ due to (3.3). Substituting (3.4) into (3.3) gives

$$y'' = x'. \quad (3.5)$$

By differentiating (3.5) with respect to σ we find

$$y' = x + c, \quad (3.6)$$

for a constant of integration c . Using (3.5) and (3.6) into (3.4) implies that

$$x'' + x = -c. \quad (3.7)$$

By solving (3.7), we derive

$$x(\sigma) = \lambda_1 \cos \sigma + \lambda_2 \sin \sigma - c. \quad (3.8)$$

It follows from (3.6) and (3.8) that

$$y(\sigma) = \lambda_1 \sin \sigma - \lambda_2 \cos \sigma + d,$$

for a constant of integration d . (3.2) immediately implies

$$\lambda_1^2 + \lambda_2^2 = 1$$

and therefore the curve \mathbf{x} can be parametrically written as

$$\mathbf{x}(\sigma) = (\lambda_1 \cos \sigma + \lambda_2 \sin \sigma - c, \lambda_1 \sin \sigma - \lambda_2 \cos \sigma + d).$$

Up to a Euclidean transformation we complete the proof.

Next we observe the non-degenerate plane curves whose the equi-affine and Frenet curvatures are same. Obviously, this curvature cannot be zero in our case. Remark also that the equi-affine arc-length of such a curve is related by its Frenet curvature as follows

$$\sigma(s) = \int_{s_0}^s \sqrt[3]{\kappa_f(t)} dt.$$

Therefore we have the following result.

Theorem 3.1. *Let \mathbf{x} be a non-degenerate smooth parametric curve in \mathbb{R}^2 with the same equi-affine and signed Frenet curvatures $\kappa = \kappa(\sigma)$. Then, up to suitable equi-affine transformations, it is either a quadratic curve with $\kappa = 1$ (namely a unit circle in Euclidean setting) or parameterized by*

$$\mathbf{x}(\sigma) = \left(\int \cos \left(\int \kappa^{\frac{2}{3}} d\sigma \right) \kappa^{-\frac{1}{3}} d\sigma, \int \sin \left(\int \kappa^{\frac{2}{3}} d\sigma \right) \kappa^{-\frac{1}{3}} d\sigma \right), \quad (3.9)$$

where σ is the equi-affine arc-length parameter of \mathbf{x} given by one of the following

$$\sigma = \frac{1}{3} \left(1 + \kappa^{-\frac{1}{3}} \right) \sqrt{-1 + 2\kappa^{-\frac{1}{3}}}, \quad (3.10)$$

and

$$\sigma = c^{-1} \sqrt{-1 + 2\kappa^{-\frac{1}{3}} + c\kappa^{-\frac{2}{3}}} - c^{\frac{-3}{2}} \ln \left| 1 + c\kappa^{-\frac{1}{3}} + \sqrt{c} \sqrt{-1 + 2\kappa^{-\frac{1}{3}} + c\kappa^{-\frac{2}{3}}} \right|, \quad (3.11)$$

for some constant $c \neq 0$.

Remark 3.2. *In (3.11) it is not easy to express the curvature function κ in terms of σ , however (3.10) can be simplified as follows: put $y = 1 + \kappa^{-\frac{1}{3}}$ and then (3.10) turns to the following algebraic equation of degree 3*

$$2y^3 - 3y^2 - 9\sigma^2 = 0,$$

in which the real root is

$$y = \frac{1}{2} \left[-1 + \left(-1 + 18\sigma^2 + 6\sqrt{-\sigma^2 + 9\sigma^4} \right)^{\frac{-1}{3}} + \left(-1 + 18\sigma^2 + 6\sqrt{-\sigma^2 + 9\sigma^4} \right)^{\frac{1}{3}} \right].$$

Therefore we deduce

$$\kappa(\sigma) = \left[\frac{-3}{2} + \frac{1}{2} \left(-1 + 18\sigma^2 + 6\sqrt{-\sigma^2 + 9\sigma^4} \right)^{\frac{-1}{3}} + \frac{1}{2} \left(-1 + 18\sigma^2 + 6\sqrt{-\sigma^2 + 9\sigma^4} \right)^{\frac{1}{3}} \right]^{-3}.$$

Proof. A plane curve is completely determined by its signed Frenet curvature $\kappa = \kappa(s)$, namely

$$\mathbf{x}(s) = \left(\int \cos \left(\int \kappa ds \right) ds, \int \sin \left(\int \kappa ds \right) ds \right). \quad (3.12)$$

Let a derivative with respect to σ be denoted by a dash '. Differentiating (3.12) three times with respect to σ gives the following equations

$$\mathbf{x}' = \left(\cos \left(\int \kappa ds \right), \sin \left(\int \kappa ds \right) \right) s' \quad (3.13)$$

$$\begin{aligned} \mathbf{x}'' = & \left(-\kappa (s')^2 \sin \left(\int \kappa ds \right) + s'' \cos \left(\int \kappa ds \right), \right. \\ & \left. \kappa (s')^2 \cos \left(\int \kappa ds \right) + s'' \sin \left(\int \kappa ds \right) \right) \end{aligned} \quad (3.14)$$

and

$$\begin{aligned} \mathbf{x}''' = & \left(- \left[\kappa' (s')^2 + 3\kappa s' s'' \right] \sin \left(\int \kappa ds \right) + \left[-\kappa^2 (s')^3 + s''' \right] \cos \left(\int \kappa ds \right), \right. \\ & \left. \left[-\kappa^2 (s')^3 + s''' \right] \sin \left(\int \kappa ds \right) + \left[\kappa' (s')^2 + 3\kappa s' s'' \right] \cos \left(\int \kappa ds \right) \right). \end{aligned} \quad (3.15)$$

Substituting (3.13) and (3.15) into (2.4) gives

$$\begin{aligned} & \mathbf{x}''' + \kappa \mathbf{x}' = \\ & = \left(- \left[\kappa' (s')^2 + 3\kappa s' s'' \right] \sin \left(\int \kappa (s) ds \right) + \left[-\kappa^2 (s')^3 + s''' + \kappa s' \right] \cos \left(\int \kappa (s) ds \right), \right. \\ & \left. \left[-\kappa^2 (s')^3 + s''' + \kappa s' \right] \sin \left(\int \kappa (s) ds \right) - \left[\kappa' (s')^2 + 3\kappa s' s'' \right] \cos \left(\int \kappa (s) ds \right) \right) = 0. \end{aligned} \quad (3.16)$$

By using the linearly independence of Sine and Cosine in (3.16) we find

$$\kappa' (s')^2 + 3\kappa s' s'' = 0$$

and

$$-\kappa^2 (s')^3 + \kappa s' + s''' = 0. \quad (3.17)$$

On the other hand from (2.3), (3.12) and (3.13) we conclude

$$\kappa (s')^3 = 1, \quad (3.18)$$

which leads to

$$ds = \kappa^{-\frac{1}{3}} d\sigma. \quad (3.19)$$

By (3.12) and (3.19) we have (3.9). Assume now in (3.18) that both κ and s' are constants. Put $\kappa = \kappa_0$. It follows from (2.5) that \mathbf{x} turns to a circle in the Euclidean setting with radius $\frac{1}{|\kappa_0|}$. In order for such a curve to have constant equi-affine curvature, \mathbf{x} must be a quadratic curve with $\kappa_a = 1$. Otherwise, namely neither κ nor s' is constant, it then follows from (3.17) and (3.18) that

$$\kappa \left[\kappa^{-\frac{1}{3}} - 1 \right] + \left(\kappa^{-\frac{1}{3}} \right)'' = 0. \quad (3.20)$$

Letting $\kappa = (y+1)^{-3}$ into (3.20) yields

$$y'' + \frac{y}{(y+1)^3} = 0. \quad (3.21)$$

After putting $p = y'$ and $\frac{dp}{dy} = \frac{y''}{y'}$ into (3.21) we deduce

$$p \frac{dp}{dy} + \frac{y}{(y+1)^3} = 0. \quad (3.22)$$

Solving (3.22) gives

$$p(y) = \sqrt{c + \frac{1+2y}{(1+y)^2}}. \quad (3.23)$$

Because $y = \kappa^{\frac{-1}{3}} - 1$, (3.23) follows

$$d\sigma = \frac{d\left(\kappa^{\frac{-1}{3}}\right)}{\sqrt{c + 2\kappa^{\frac{1}{3}} - \kappa^{\frac{2}{3}}}}. \quad (3.24)$$

By solving (3.24) we obtain (3.10) and (3.11) according to $c = 0$ or $c \neq 0$.

4. PLANE CURVES WITH PRESCRIBED EQUI-AFFINE CURVATURE

As we can see from (2.4), classifying parametric plane curves with prescribed equi-affine curvature directly reduces to solve vector ODE with variable coefficient. In general, solving such equations is not easy and one of the well-known ODEs with variable coefficient is of Euler-Cauchy type. If we put the equi-affine curvature as

$$\kappa_a(\sigma) = a(b\sigma + c)^{-2}, \quad b^2 + c^2 \neq 0, \quad (4.1)$$

for some constants a, b, c , then (2.4) leads to a vector ODE of Euler-Cauchy type. Moreover, our choice (4.1) generalizes plane curves with constant equi-affine curvature as a secondary purpose of this paper because \mathbf{x} turns to a parabola if $a = 0$, an ellipse $b = 0$ and $ac^{-2} > 0$, and a hyperbola $b = 0$ and $ac^{-2} < 0$.

In this section, we try to classify parametric plane curves whose the equi-affine curvature is given by (2.4). Since we want to generalize plane curves with constant equi-affine curvature we may assume that $ab \neq 0$. Putting $p = ab^{-2}$, (4.1) turns to $\kappa_a(\sigma) = p\sigma^{-2}$ up to a suitable translation of σ . Therefore we have the following result

Theorem 4.1. *Let the interval I do not contain zero and a plane curve $\mathbf{x} : I \rightarrow \mathbb{R}^2$ have the equi-affine curvature $\kappa_a(\sigma) = p\sigma^{-2}$, $p \neq 0$. Then, up to suitable equi-affine transformations, it has one of the following parametric expressions*

(1) if $p = -2$,

$$\mathbf{x}(\sigma) = \frac{1}{3}(\sigma^3, -\ln \sigma);$$

(2) if $p < \frac{1}{4}$ and $p \neq -2$, $p \neq 0$,

$$\mathbf{x}(\sigma) = \left(\frac{2}{3 + \sqrt{1-4p}} \sigma^{\frac{3+\sqrt{1-4p}}{2}}, \frac{2}{1-4p-3\sqrt{1-4p}} \sigma^{\frac{3-\sqrt{1-4p}}{2}} \right);$$

(3) if $p = \frac{1}{4}$,

$$\mathbf{x}(\sigma) = \left(\frac{2}{3} \sigma^{\frac{3}{2}}, \frac{2}{9} \sigma^{\frac{3}{2}} (-2 + 3 \ln \sigma) \right);$$

(4) if $p > \frac{1}{4}$,

$$\begin{aligned} \mathbf{x}(\sigma) = & \frac{2\sigma^{\frac{3}{2}}}{5+16p} \left(3 \cos(\sqrt{4p-1} \ln \sigma) + 2\sqrt{4p-1} \sin(\sqrt{4p-1} \ln \sigma) \right) \\ & - 2 \cos(\sqrt{4p-1} \ln \sigma) + \frac{3}{\sqrt{4p-1}} \sin(\sqrt{4p-1} \ln \sigma). \end{aligned}$$

Proof. By (2.4) we write the following vector ODE

$$\mathbf{x}''' + \frac{p}{\sigma^2} \mathbf{x}' = 0, \quad p \neq 0, \quad (4.2)$$

where $\mathbf{x}' = \frac{d\mathbf{x}}{d\sigma}$, etc. Let $\mathbf{x}' = \mathbf{y}$ and $\mathbf{x}''' = \mathbf{y}''$, then (4.2) implies to the ODE of Euler-Cauchy type

$$\sigma^2 \mathbf{y}'' + p\mathbf{y} = 0, \quad (4.3)$$

which can be reduced to the vector linear ODE with constant coefficient

$$\ddot{\mathbf{y}} - \dot{\mathbf{y}} + p\mathbf{y} = 0, \quad (4.4)$$

where $\dot{\mathbf{y}} = \frac{d\mathbf{y}}{du}$, $\ddot{\mathbf{y}} = \frac{d^2\mathbf{y}}{du^2}$ and $\sigma = e^u$. The characteristic equation of (4.4) follows

$$\lambda^2 - \lambda + p = 0,$$

in which the roots are $\lambda_{1,2} = \frac{1 \pm \sqrt{1-4p}}{2}$. According to the sign of the discriminant $1-4p$, we have to distinguish three cases:

(1) $p < \frac{1}{4}$. We write the solution of (4.4) as

$$\mathbf{y}(\sigma) = c_1 \sigma^{\frac{1+\sqrt{1-4p}}{2}} + c_2 \sigma^{\frac{1-\sqrt{1-4p}}{2}} \quad (4.5)$$

for some constant vectors $c_1, c_2 \in \mathbb{R}^2$. We have two cases:

(a) $p = -2$. Integrating (4.5) gives

$$\mathbf{x}(\sigma) = \frac{1}{3} c_1 \sigma^3 + c_2 \ln \sigma + c_0,$$

for a constant vector $c_0 \in \mathbb{R}^2$. The fact that $|\mathbf{x}' \mathbf{x}''| = 1$ for each $\sigma \in I$ implies $|c_1 \ c_2| = \frac{-1}{3}$ and hence we may set $c_0 = (0, 0)$, $c_1 = (1, 0)$ and $c_2 = (0, \frac{-1}{3})$.

This proves the first statement of the theorem.

(b) $p \neq -2$. Then integrating (4.5) leads to

$$\mathbf{x}(\sigma) = \frac{2}{3 + \sqrt{1-4p}} c_1 \sigma^{\frac{3+\sqrt{1-4p}}{2}} + \frac{2}{3 - \sqrt{1-4p}} c_2 \sigma^{\frac{3-\sqrt{1-4p}}{2}} + c_0,$$

for a constant vector $c_0 \in \mathbb{R}^2$. The condition that $|\mathbf{x}' \mathbf{x}''| = 1$ for each $\sigma \in I$ gives $|c_1 c_2| = \frac{-1}{\sqrt{1-4p}}$ and hence we may set $c_0 = (0, 0)$, $c_1 = (1, 0)$ and $c_2 = \left(0, \frac{-1}{\sqrt{1-4p}}\right)$, which gives the proof of the second statement of the theorem.

(2) $p = \frac{1}{4}$. Then the solution of (4.4) follows

$$\mathbf{y}(\sigma) = \sigma^{\frac{1}{2}} [c_1 + c_2 \ln \sigma], \quad (4.6)$$

for some constant vectors $c_1, c_2 \in \mathbb{R}^2$. Integrating (4.6) yields

$$\mathbf{x}(\sigma) = \frac{2}{3} \sigma^{\frac{3}{2}} c_1 + \frac{2}{9} \sigma^{\frac{3}{2}} (-2 + 3 \ln \sigma) c_2 + c_0,$$

for a constant vector $c_0 \in \mathbb{R}^2$. Because $|\mathbf{x}' \mathbf{x}''| = 1$ for each $\sigma \in I$ we get $|c_1 c_2| = 1$ and may set $c_0 = (0, 0)$, $c_1 = (1, 0)$ and $c_2 = (0, 1)$. Therefore we derive the proof of the third statement of the theorem.

(3) $p > \frac{1}{4}$. (4.4) leads to

$$\mathbf{y}(\sigma) = \sigma^{\frac{1}{2}} \left[\cos(\sqrt{4p-1} \ln \sigma) c_1 + \sin(\sqrt{4p-1} \ln \sigma) c_2 \right], \quad (4.7)$$

for some constant vectors $c_1, c_2 \in \mathbb{R}^2$. By integrating (4.7) we conclude

$$\begin{aligned} \mathbf{x}(\sigma) = & \frac{2\sigma^{\frac{3}{2}}}{5+16p} \left\{ [3 \cos(\sqrt{4p-1} \ln \sigma) + 2\sqrt{4p-1} \sin(\sqrt{4p-1} \ln \sigma)] c_1 - \right. \\ & \left. [-2\sqrt{4p-1} \cos(\sqrt{4p-1} \ln \sigma) + 3 \sin(\sqrt{4p-1} \ln \sigma)] c_2 \right\} + c_0, \end{aligned}$$

for a constant vector $c_0 \in \mathbb{R}^2$. Because $|\mathbf{x}' \mathbf{x}''| = 1$ for each $\sigma \in I$ we have $|c_1 c_2| = \frac{1}{\sqrt{4p-1}}$ and may set $c_0 = (0, 0)$, $c_1 = (1, 0)$ and $c_2 = \left(0, \frac{1}{\sqrt{4p-1}}\right)$. This completes the proof.

Example 4.1. *Let the following plane curves with prescribed equi-affine curvature be parameterized by*

- (1) $\mathbf{x}(\sigma) = \frac{1}{3} (\sigma^3, -\ln \sigma)$, $\kappa_a(\sigma) = -2\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$,
- (2) $\mathbf{x}(\sigma) = \left(\frac{2}{7}\sigma^{\frac{7}{2}}, \frac{1}{2}\sigma^{-\frac{1}{2}}\right)$, $\kappa_a(\sigma) = \frac{-15}{4}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, 1]$,
- (3) $\mathbf{x}(\sigma) = \left(\frac{2}{3}\sigma^{\frac{3}{2}}, \frac{2}{9}\sigma^{\frac{3}{2}}(-2 + 3 \ln \sigma)\right)$, $\kappa_a(\sigma) = \frac{1}{4}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$,
- (4) $\mathbf{x}(\sigma) = \frac{2\sigma^{\frac{3}{2}}}{13} (3 \cos(\ln \sigma) + 2 \sin(\ln \sigma), -2 \cos(\ln \sigma) + 3 \sin(\ln \sigma))$, $\kappa_a(\sigma) = \frac{1}{2}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$.

These curves can be plotted as below:

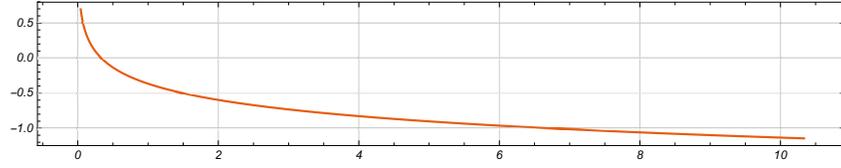


FIGURE 1. Plane curve with $\kappa_a(\sigma) = -2\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$.

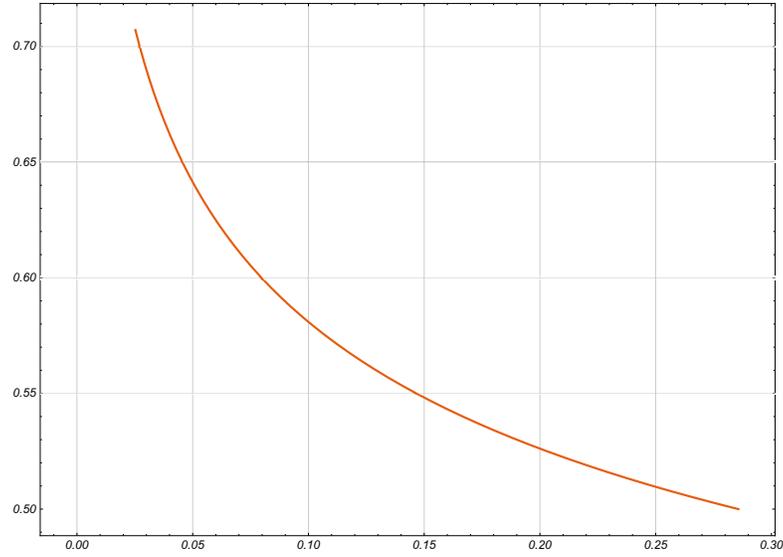


FIGURE 2. Plane curve with $\kappa_a(\sigma) = \frac{-15}{4}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, 1]$.

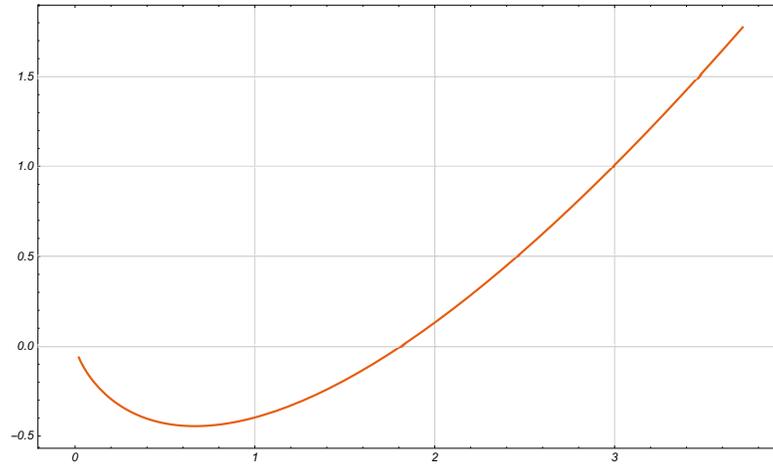


FIGURE 3. Plane curve with $\kappa_a(\sigma) = \frac{1}{4}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$.

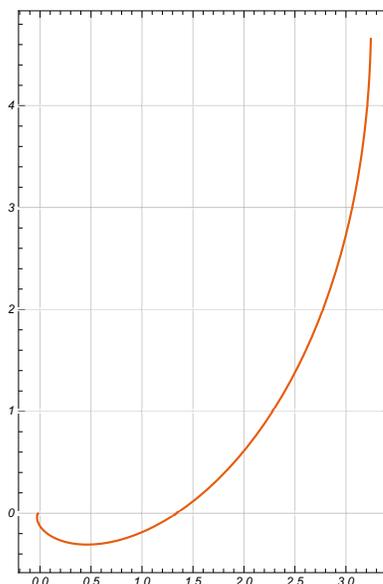


FIGURE 4. Plane curve with $\kappa_a(\sigma) = \frac{1}{2}\sigma^{-2}$ for $\sigma \in [\frac{1}{2}, \pi]$.

REFERENCES

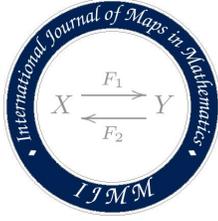
- [1] Calabi, E., Olver, P.J. and Tannenbau.(1996). A.Affine geometry, curve flows, and invariant numerical approximations, *Adv. Math.*124,154–196.
- [2] Davis, D.(2006).Generic affine differential geometry of curves in R^n , *Proc. Royal Soc. Edinburgh A* 136, 1195–1205.
- [3] Flash, T. and Handzel, A.(2007). Affine differential geometry analysis of human arm movements, *Biol. Cybern.* 96, 577-601.
- [4] Gardner, R.B. and Wilkens, G.R.(1997). The fundamental theorems of curves and hypersurfaces in centroaffine geometry, *Bull. Belg. Math. Soc. Simon Stevin* 4, 379–401.
- [5] Giblin, P.J. and Sano,T.(2012). Generic equi-centro-affine differential geometry of plane curves, *Top. Appl.*, 159 , 476–483.
- [6] Gray, A.(1998). *Modern Differential Geometry of Curves and Surfaces with Mathematica*, Second Ed. CRC Press.
- [7] Guggenheimer, H.W.(1963). *Differential Geometry*, McGraw-Hill, New York.
- [8] Hu, N.(2011). Centroaffine space curves with constant curvatures and homogeneous surfaces, *J. Geom.* 102 , 103–114.
- [9] Hu, N.(2012). *Affine Geometry of Space Curves and Homogeneous Surfaces*, PH.D. thesis, Dept. Math., G.S. Sci., Hokkaido University, Japan.
- [10] Izumiya, S. and Sano, T.(1998). Generic affine differential geometry of plane curves, *Proc. Royal Soc. Edinburgh A* 41 , 315–324.
- [11] Kreyszig, E. and Pendl, A.(1975). Spherical curves and their analogues in affine differential geometry, *Proc. Am. Math. Soc.* 48 1975, 423–428.

- [12] Kreyszig, E.(2006). *Advanced Engineering Mathematics*, John Wiley and Sons, Inc, Daners.
- [13] Li, A.-M., Simon, U., Zhao, G. and Hu,Z.(2015). *Global Affine Differential Geometry of Hypersurfaces*, 2nd edn. W. de Gruyter, Berlin .
- [14] Liu, H.(2014). Curves in affine and semi-Euclidean spaces, *Results. Math.* 65 , 235–249.
- [15] Nomizu, K. and Sasaki, T.(1994). *Affine Differential Geometry. Geometry of Affine Immersions*. Cambridge Tracts in Mathematics, vol. 111. Cambridge University Press, Cambridge.
- [16] Olver, P.J.(2010). Moving frames and differential invariants in centro-affine geometry, *Lobachevskii J. Math.* 31 , 77-89.
- [17] Olszak, K. and Olszak, Z.(2017). The equi-affine and Frenet curvatures of curves in pseudo-Riemannian 2-manifolds, *Colloq. Math.* 150 , 103-112.
- [18] Peksen, O. and Khadjev, D.(2004). On invariants of curves in centro-affine geometry, *J. Math. Kyoto Univ.* 44, 603–613.
- [19] Pressley, A.(2010). *Elementary Differential Geometry*, Berlin, Germany: Springer Verlag.
- [20] Sagiroglu, Y. and Peksen, O.(2010). The equivalence of centro-equiaffine curves, *Turk. J. Math.* 34(1) , 95–104
- [21] Sagiroglu, Y. and Peksen, O.(2010). The equivalence of equi-affine curves, *Turk. J. Math.* 34 , 95–104.
- [22] Sapiro, G. and Tannenbaum, A.(1994). On affine plane curve evolution, *J. Funct. Anal.* 119 , 79-120.
- [23] Tuncer, Y., Kocayigit, H. and Karacan, M.K.(2019). Naturel mates of equiaffine space curves in affine 3-space, *Thermal Science* . <https://doi.org/10.2298/TSCI190901404T>.
- [24] Verpoort, S.(2011). Curvature functionals for curves in the equi-affine plane, *Czechoslovak Math. J.* 61(2) , 419–435.
- [25] Yang, Y. and Yu, Y.(2020). Moving frames and differential invariants on fully affine planar curves, *Bull. Malays. Math. Sci. Soc.* 43 , 3229-3258.

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, FIRAT UNIVERSITY, ELAZIG, 23200, TURKEY

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, FIRAT UNIVERSITY, ELAZIG, 23200, TURKEY

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, FIRAT UNIVERSITY, ELAZIG, 23200, TURKEY



A GENERALIZATION OF NTRU CRYPTOSYSTEM AND A NEW DIGITAL SIGNATURE VERSION

MEHMET SEVER  AND AHMET ŞÜKRÜ ÖZDEMİR  *

ABSTRACT. In this study, it is made new generalizations by adding a security parameter “ n ” to NTRU cryptosystem. These generalizations are analyzed in three categories. The first category clarifies summative generalization, the second category explains a multiplicative generalization and the latest category expresses a dimension generalization, and the system is researched with greater sets and many choosings of parameters. As a result of all these evidences, it is stated that these generalization outputs creates a new NTRUSIGN.

Keywords: NTRU, NTRU cryptosystem, NTRUSIGN, cryptology, (digital) signature

2010 Mathematics Subject Classification: 11T71, 14G50, 94A60, 94A62.

1. INTRODUCTION

In 1996, NTRU was first introduced by J. Hoffstein, J. Pipher ve J. Silverman in Crypto’ 96 [5]. Then NTRU’s developers contributed to NTRU which is denoted as a ring-based and a public key encryption method by making parameter optimization [4]. In 2003, they introduced $NTRU_{SIGN}$ [9], i. e., a digital signature version of NTRU. In the same year, they with another team made a presentation which analyzed description errors of NTRU [21]. J. H. Silverman published a technical report about invertible polynomials in a ring in 2003 [13]. In 2005, J. H. Silverman and W. Whyte published a technical report which analyzed error probabilities in NTRU decryption [22]. Also, the founding team which published an article

Received:2020.05.22

Revised:2020.09.24

Accepted:2020.10.07

* Corresponding author

Mehmet Sever; msever@agri.edu.tr; <https://orcid.org/0000-0003-2967-1943>

Ahmet Şükrü Özdemir; ahmet.ozdemir@marmara.edu.tr; <https://orcid.org/0000-0002-0597-3093>

on effects increasing security level of parameter choosing [11] has published related reports in the website www.ntru.com.

NTRU is quite resistant to quantum computers based attacks as well as its speed. The basic reason of protecting this resistant bases on finding a lattice vector with the least length and powerfulness of problems of finding a lattice point closest to private key into a high dimensional lattice [20]. Unlike the other public key cryptosystems, the sheltering structure of the NTRU cryptosystems against these quantum based attacks moves it more interesting and developing position day by day.

Some examples of quitely full-scale non-destructive attacks to the NTRU cryptosystem were originally made by Coppersmith et al. in 1997 [1]. Then new parameters which does away with effects of this attack were presented by Hoffstein et al. in 2003 [8].

As an another example of attack [14], it has increased importance up till today by presenting to more powerful, current and new parameters and solutions to the NTRU cryptosystem organized an attack of splitting the difference [15].

On behalf of detailed readings, it can be seen to [16, 17, 24] for different types of attacks types, and on the contrary, it can be seen to [12, 19, 3] for proposed new parameters and new system.

2. MOTIVATION AND METHOD

Hoffstein et al. introduced the first NTRU based digital signature in 2001 [18]. Then they gave a verification method for the NTRU cryptosystem in the same year [6]. The basic aim of these studies which present a digital signature and a verification method is to guarantee which there is no leakage into the system.

Even decoding a cryptological message falls short to state that you are an approved user of the system. Hence, solving a verification code or a reposted different text in the same way can co-opt you. It is clear in this age which the development of mobile payment methods and all business and government works are solved on the network that the discipline of digital signature is open for improvement. In this sense, the basic motivation of this study studies proposed in [7] and [23], and also the articles in [2, 25, 10] can be helpful on behalf of extra readings.

3. AIM AND SCOPE

This study aims primarily to generalize the NTRU cryptosystem. This study which can be summarized as sending the sum, product or enhancing dimension of composed encoded texts by hiding a message with multi public keys and error polynomials purposes specially to avoid an attack on the plain text. It is obtained that the message is divided into parts with this method and also can be sent partially by showing that several two message can be sent in the generalization of enhancing dimension simultaneously.

Besides, this article explains the conditions that all these generalization offers can be used as a digital signature. If a new encoded text composed in the form of generalizations is sent just after previously partial encoded texts, the recipient is interpreted as a correct system user since s/he reads and obtains the message, and it can transform to a digital signature.

The most important output of this study is to enlarge still the NTRU cryptosystem against the developing quantum computers attacks and render to sheltering case.

4. NTRU PARAMETERS

These are parameters using in the encryption and decryption operations of NTRU and in the key generation processes:

- N : it determines a maximum degree of polynomials being used. N is chosen as a prime so that the process is preserved against attacks, and it is chosen big enough so that the process is preserved from lattice attacks.
- q : it is a large module and it is chosen as a positive integer. Its values differ relatedly what we aim in the process.
- p : it is a small module and generally a positive integer. It is rarely chosen as a polynomial with small coefficients.

The parameters N , q and p can be differently chosen according to the preferred security level. The case $(p, q) = 1$ is always preserved so that the ideal (p, q) is equal to the whole ring.

- L_f, L_g : sets of private key, sets in which it is chosen polynomials to be kept confidential chosen for encryption.
- L_m : it is a plain text set. it is stated a set of unencrypted and codable polynomials.
- L_r : it is a set of error polynomials. It is stated a set of arbitrarily chosen error polynomials with small coefficients in the phase of encryption.

- *center* : it is a centralization method. An algorithm guaranteeing which *mod q* reductions works in perfect truth in the phase of decryption.

It can be seen [5] for a perscrutation of the NTRU parameter which is introduced above in general for now and can be given its values in the next section.

5. ALGEBRAIC BACKGROUND OF NTRU

5.1. Definitions and notation. The encryption operations of NTRU is performed in a quotient ring $R = Z[x]/(x^N - 1)$. N is a positive integer and it is generally chosen as a prime. If $f(x)$ is a polynomial in R , then f_k denotes a coefficient of x_k for every $k \in [0, N - 1]$ and $f(x)$ denotes a value of f in x for $x \in \mathbb{C}$. A convolution product $h = f \star g$ is given by $h_k = \sum_{i+j \equiv k \pmod N} f_i \cdot g_j$ where f and g are two polynomials in R . When NTRU was first introduced, it was chosen p and q as a power of 3 and 2, respectively. The subset L_m : consisted of polynomials with the coefficients $\{-1, 0, 1\}$ called ternary polynomials. The private keys $f \in L_f$ was usually chosen in the form $1 + p \cdot F$. The studies shows that it can be chosen p as a polynomial and parameters can be varied.

5.2. Key generation.

1. $f \in L_f$ and $g \in L_g$ is arbitrarily chosen such that f is invertible in *mod p* and *mod q*.
2. $F_q = f^{-1} \pmod q$ and $F_p = f^{-1} \pmod p$.
3. A private key is (p, F_p) .
4. A public key is $H = p \cdot g \star F_q \pmod q$.

It is noted that g cannot be used in the phase of decryption. Thus, it cannot be given as a private key. Since $H \star f = p \cdot g \pmod q$, $H \star f = 0 \pmod p$ which cannot be used when *mod p* is substituted.

5.3. Encryption.

If the encryption is represented in an algorithmic language;

Input: a message $m \in L_m$ and a public key H .

Output: a cipher message $e \in \mathcal{Y}(m)$

1. Chose $r \in L_r$ arbitrarily.
2. Return $e = r \star H + m \pmod q$.

The set $\mathcal{Y}(m)$ denotes plain texts m which can be encrypted.

5.4. Decryption. If a phase of decryption is represented as algorithmic, an algorithm D acts e as below:

Input: a cipher message $e \in \mathcal{Y}(m)$ and a private key (p, F_p) .

Output: a plain text $D(e) = m \in L_m$.

1. Calculate $a \bmod q = e \star f \bmod q$.
2. Have a polynomial $a \bmod q$ with integer coefficients from $a = p \cdot r \star g + f \star m \in R$ by performing centralization operation.
3. $m \bmod p = a \star F_p \bmod p$.
4. a plain text $m = \Psi \bmod p$.

It is noted that Ψ is the mapping $\Psi : m \mapsto m \bmod p$. That is, it performs $\Psi : L_m \rightarrow L_m \bmod p$. It is important choosing of a convenient parameter in order to work decryption operation impeccably, i.e., $D(e) = m$.

6. CHOOSING PARAMETERS OF THE NEW SYSTEM

The proposed generalized system has used some parameters literally. That is, the choosings of the prime number p and q , the number N , the polynomials f , g , r etc. is the same as in the classical NTRU system. The only difference is that different polynomials f , g and r can be chosen for different public keys generation.

7. USING NOTATIONS IN THE NEW SYSTEM

The same representations can be used under the same conditions and the same choosings by holding to all classical NTRU notations. It is only useful to introduce three notations $f_{(n)}^*$, $f_{(n,j)}^*$ and $f_{(n)}^{-1}$. $f_{(n)}^*$ consists of a convolution product of n chosen all secret keys where $f_{(n)}^* = f_1 \star f_2 \star \dots \star f_n$. $f_{(n,j)}^* = f_1 \star f_2 \star \dots \star f_{j-1} \star f_{j+1} \star \dots \star f_n$ consists of a convolution product of all except the j . secret key. Let $f_{(n)}^{-1}$ denote an inverse of product of n unitary secret keys f on $\bmod p$.

8. HOW DOES THE SUMMATIVE GENERALIZATION SYSTEM WORK?

This generalized system pre-encrypts differently a message by choosing n different public keys and n different error polynomials. The sum of these composed pre-encrypted texts is sent as a recent encrypted message. The number n is relatively prime p and q , respectively. However, there exist two different cases where the number n is greater and less than the

numbers p and q being modules. Thus, it leads to add a new parameter in the old classical system NTRU since it works as a security parameter of this system. Now, we show how the system works in the case $n < p$, $n < q$ and $(n, p) = 1$, $(n, q) = 1$. We consider initially this system in the classical NTRU rings as $Z_p[x]/(x^N - 1)$ and $Z_q[x]/(x^N - 1)$. Then it is reconsidered by taking a field instead of a ring.

Lemma 8.1. *A message polynomial m is encrypted n times by choosings of a public key $h_i = f_{iq}^{-1} \star g_i$ and an error polynomial r_i , $1 \leq i \leq n$ according to the classical method of the NTRU cryptosystem and then the plain text m can be achieved in the case which the sum of composed encrypted texts e_i $1 \leq i \leq n$ is sent.*

Proof. Let the encrypted forms of messages m be written and summed obviously and one under the other. We have

$$\begin{array}{rcl}
 e_1 & = & ph_1 \star r_1 + m \pmod{q} \\
 e_2 & = & ph_2 \star r_2 + m \pmod{q} \\
 : & & : \\
 + e_n & = & ph_n \star r_n + m \pmod{q} \\
 \hline
 e_1 + e_2 + \dots + e_n & = & p[(h_1 \star r_1) + (h_2 \star r_2) + \dots + (h_n \star r_n)] + nm \pmod{q}.
 \end{array} \tag{8.1}$$

Now, we obtain

$$\begin{aligned}
 f_{(n)}^*(e_1 + e_2 + \dots + e_n) &= p[(f_{(n,1)}^* \star g_1 \star r_1) + (f_{(n,2)}^* \star g_2 \star r_2) + \dots \\
 &\quad + (f_{(n,n)}^* \star g_n \star r_n)] + f_{(n)}^* \star nm \pmod{q}
 \end{aligned} \tag{8.2}$$

by applying the product of each unitary polynomial f_i , $1 \leq i \leq n$ to Equation (8.1). Since $f_{(n)}^*$ consists of the product of the invertible secret keys f and this product is invertible in the statement (8.2), both sides of the equation is multiplied by $f_{(n)}^{-1}$ and then the message nm should not impressed by these values if we consider the equation in \pmod{p} instead of \pmod{q} . So,

$$e_1 + e_2 + \dots + e_n = nm \pmod{p}.$$

Since an user knows the security parameter n into the system, he knows that taken message is m or the message nm being its n -fold by the notion in the form

$$e_1 + e_2 + \dots + e_n = \underbrace{m + m + \dots + m}_n \pmod{p}.$$

This case goes into the probabilistic cryptology. That is, it is based on the assumption that an user of the system can exit the intricate situation. Now, let us give a certain decryption method by means of fields.

Lemma 8.2. *Let p and q be prime numbers, and let M and S be two N -order irreducible polynomials in $F_p[x]$ and $F_q[x]$. Then the system proposal given in Lemma 8.1 works in the fields $F_p[x]/(M)$ and $F_q[x]/(S)$ non-probabilistically.*

Proof. Let us remind that the polynomials f , g , r and m can be only chosen in $F_p[x]/(M)$ or $F_q[x]/(S)$ such that all conditions in Lemma 8.1 remain the same. Similarly, let the polynomial m be encrypted by n different public keys h and n different error polynomials r , and whole encrypted text be divided by n and be sent. Let the statement (8.1) in Lemma 8.1 be divided by n , and let

$$\begin{aligned} a &= \frac{e_1 + e_2 + \dots + e_n}{n} \\ &= p \cdot \frac{1}{n} [(h_1 \star r_1) + (h_2 \star r_2) + \dots + (h_n \star r_n)] + m \pmod{q} \end{aligned}$$

be sent as a encrypted text. If the polynomial a is first multiplied by $f_{(n)}^*$ and then $f_{(n)}^{-1}$, and the current statement calculate in $\text{mod } p$, the system works non-probabilistically as

$$\frac{e_1 + e_2 + \dots + e_n}{n} = m \pmod{p}.$$

Now, we state how the system works in the case $q > n > p$ and $(p, n) = 1$.

Lemma 8.3. *All conditions in Lemma 8.1 remain the same, and the system works with small probability part in the case $q > n > p$ and $(p, n) = 1$.*

Proof. To avoid writing repetition, we skip the steps of decryption in Lemma 8.1 and consider the last step as follows:

$$e_1 + e_2 + \dots + e_n = nm \pmod{p}. \tag{8.3}$$

When $n < q$, we reach to $\text{mod } p$ without changing. But, there exist $k, l \in Z$ such that $n = kp + l$ when $n > p$. Then Equation (8.3) becomes

$$e_1 + e_2 + \dots + e_n = lm \pmod{p}.$$

When $l < n$ in the last situation, a probabilistic decryption should be done. That is, taken message can be only m , lm or nm . Since the user of the system knows parameters n , p , q , he chooses an appropriate text from the set $\{m, lm, nm\}$.

Proposition 8.1. *The system works with the probability 4 since there is a possibility of multiplying by a as a result of $b \pmod p$ from $n = aq + b$ in addition to the operations in Lemma 8.3 in the case $n > q > p$.*

9. MULTIPLICATIVE GENERALIZATION

We clarify a method that a message encrypts n times and then the product of recent composed encrypted polynomials is sent as an encrypted text. The choosings and operations of summative generalization told in the first chapter remain the same, and let's encrypt a message m in n different forms. Let all pre-encrypted texts m be written and multiplied one under the other. We specify that it is helpful choosing the prime p large enough so that the residue classes does not constitute a complex situation.

9.1. How does the system work?

$$\begin{aligned}
 e_1 &= ph_1 \star r_1 + m \pmod q \\
 e_2 &= ph_2 \star r_2 + m \pmod q \\
 &\vdots \\
 \star e_n &= ph_n \star r_n + m \pmod q
 \end{aligned} \tag{9.4}$$

$$\begin{aligned}
 e_1 \star e_2 \star \dots \star e_n &= p^n (h_1 \star h_2 \star \dots \star h_n) \star (r_1 \star r_2 \star \dots \star r_n) \star p[H \star R] \star m \\
 &\quad + m^n \pmod q
 \end{aligned}$$

where $H \star R$ is a short result of the convolution product of h_i and r_i . In the decryption phase, a symbolic result is only written since its inverse need not to be calculated and is zeroized in mod p . If Equation (9.4) is multiplied by $f_{(n)}^*$ and $f_{(n)}^{-1}$ as in Lemma 8.1, respectively, and the result is calculated in $\pmod p$, then we have an equation

$$e_1 \star e_2 \star \dots \star e_n = m^n \pmod p.$$

If $m^n \pmod p$ is chosen in the form that need not to be the reduction, then

$$e_1 \star e_2 \star \dots \star e_n = m^n \tag{9.5}$$

is possible. Equation (9.5) reached in the latest phase proposes us a two probability decryption:

- (1) The message is only m . That is, m becomes known by means of the security parameter n in a polynomial m^n .
- (2) Or the message is already m^n .

Now, we give the nonprobability working situation of the system.

Lemma 9.1. *If all conditions and choosings are done as in the previous chapter, we consider Equation (9.4). The system works non probabilistically in the case that $[e_1 \star e_2 \star \dots \star e_n]^n$ is sent as a encrypted text by exponentiating n -th power of the polynomial $e_1 \star e_2 \star \dots \star e_n$ instead of $e_1 \star e_2 \star \dots \star e_n$.*

Proof. When the n -th power of the encrypted text is exponentiated in the statement (9.4) and is sent in the form

$$[e_1 \star e_2 \star \dots \star e_n]^n,$$

if all decryption steps are done appropriately then an equation

$$(e_1 \star e_2 \star \dots \star e_n)^n = m^n \text{ mod } p$$

consists of instead of the statement (9.5) so that the message becomes directly known in the form

$$e_1 \star e_2 \star \dots \star e_n = m$$

when p is chosen as a sufficiently large parameter.

10. COORDINATE GENERALIZATION AND ENHANCING DIMENSION

When a NTRU cryptographic operation is made in a ring $R = Z[x]/(x^N - 1)$, a different public key h_2 can be generated by choosing an error polynomial $r_2 \in R$ from a generated public key h_1 . The first cryptographic operation is made in the form which $e_1 = h_1 \star r_1 + m \text{ (mod } q)$ if $h_1 = pf_q^{-1} \star g$ for $f, g \in R$. The same message (it can be different) can be hidden in the form $e_2 = h_2 \star r_2 + m$ by means of an another public key produced by $h_2 = h_1 \star r_1 + r_2$ for an arbitrarily chosen $r_2 \in R$. In the latest case, (h_1, h_2) is a public key, (e_1, e_2) is a encrypted text and (f, g) is a secret key where the choosings of f and g is as in the classical NTRU operations. The message that wishes sent can be (m, m) or (m_1, m_2) . It is worth noting that all polynomials are the same degree. If they are not, an appropriate monomial with 0 coefficient must be added. To explain the algebraic structure on which this new proposed system is constructed, it is clear that a mapping

$$\theta : R = Z[x]/(x^N - 1) \longrightarrow Z^N$$

defined by

$$\theta(a) = (a_0, a_1, \dots, a_{N-1})$$

is a homeomorphism for $a(x) = a_0 + a_1x + \dots + a_{N-1}x^{N-1} \in R$. We define a mapping μ by means of the mapping θ .

$$\mu : R \times R \longrightarrow Z^N \times Z^N, \quad \mu((a, b)) = (\theta(a), \theta(b))$$

under the operations $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) \odot (c, d) = (a \star c, b \star d)$ for a, b, c and $d \in R$, i.e., we define by

$$\mu((a, b)) = ((a_0, a_1, \dots, a_{N-1}), (b_0, b_1, \dots, b_{N-1})).$$

It can be seen easily that the operations \oplus and \odot are well-defined. μ is a homeomorphism since

$$\begin{aligned} \mu((a, b) \oplus (c, d)) &= \mu((a + c, b + d)) \\ &= (\theta(a + c), \theta(b + d)) \\ &= (\theta(a) + \theta(c), \theta(b) + \theta(d)) \\ &= (\theta(a), \theta(b)) + (\theta(c), \theta(d)) \\ &= \mu((a, b)) + \mu((c, d)) \end{aligned}$$

and

$$\begin{aligned} \mu((a, b) \odot (c, d)) &= \mu((a \star c, b \star d)) \\ &= (\theta(a \star c), \theta(b \star d)) \\ &= (\theta(a) \star \theta(c), \theta(b) \star \theta(d)) \\ &= (\theta(a), \theta(b)) \star (\theta(c), \theta(d)) \\ &= \mu((a, b)) \star \mu((c, d)) \end{aligned}$$

so that it is shown that μ is a homeomorphism. More clearly, it is written by the laws

$$\begin{aligned} (f, g) \oplus (f', g') &= (f + f', g + g') \\ (f, g) \odot (f', g') &= (f \star f', g \star g') \end{aligned}$$

in $R \times R$ for the operations $f, f', g, g' \in R$. Since the ring R can be embedding into $R \times R$ by $f \mapsto (1, f)$, $(1, f) \in R \times R$ is used for all $f \in R$. Then it is possible that the element $(1, f)$ is invertible since $f \in R$ is invertible. That is, if $f \star f' \equiv 1 \pmod{p}$ for $f \in R$ then $(1, f) \odot (1, f') = (1, 1)$ so that $(1, 1)$ is a unit element of $R \times R$.

After all these details and explanations, we present a NTRU on this structure. Let $f, g, r_i \in R$ be determined according to the classical NTRU methodology. Let a message (m_1, m_2) be sent for the message polynomials $m_1, m_2 \in R$. A vector $(e_1, e_2) \in R \times R \cong Z^{2N}$ constituted by the polynomials e_1 and e_2 which are determined by the pre-encryptions

$$e_1 = pf_q^{-1} \star g \star r_1 + m_1 \pmod{q}$$

$$e_2 = ph_2 + m_2 \pmod{q}$$

is sent where $h_1 = pf_q^{-1} \star g$ and $h_2 = ph_1 \star r_1 + r_2 \pmod{q}$ are two public keys. (f, f) and (f_p, f_p) represent secret keys and (r_1, r_2) represents error vectors of the new proposed system where (h_1, h_2) is a public key and f_p is an inverse of f in \pmod{p} . Since the arbitrarily choosings of g generate many secret keys, it is stated that the keys (f, f) and (f_p, f_p) is only sufficient for the system.

10.1. How does the system work? The receiver opens the vector (e_1, e_2) by means of secret keys (f, f) and (f_p, f_p) as follow.

$$\begin{aligned} (e_1, e_2) \odot (f, f) &= (e_1 \star f, e_2 \star f) \pmod{q} \\ &= (p \star g \star r_1 + f \star m_1, p^2 \star g \star r_1 + pr_2 \star f + f \star m_2) \pmod{q} \\ &= (f \star m_1, f \star m_2) \pmod{p}. \end{aligned} \quad (10.6)$$

If the statement (10.6) is multiplied by (f_p, f_p) , then $(f_p, f_p) \odot (e_1, e_2) \odot (f, f) = (m_1, m_2) \pmod{p}$ and the decryption result becomes directly known the message.

10.2. Advantages of the system.

- The receiver uses two public keys such as h_1 and h_2 . Hence, even if a key is obtained, the other is not obtained easily.
- A larger message such as (m_1, m_2) is sent in a lump instead of a message m .
- On the constituted system is on $Z^{2N} \cong Z^N \times Z^N$, NTRU is more sheltering according to the ring $Z^N \cong R = Z[x]/(x^N - 1)$.
- If $f \in R$ is a private key, then $(f, f) \in R \times R$ is a private key so that no extra search operation and time are needed.

10.3. Disadvantage of the system. Although involving multiple operations and producing multiple secret keys tighten the security, it leads to a regression in time and effort capacity.

11. NTRU DIGITAL SIGNATURES

It is understood that if the messages $e_i, 1 \leq i \leq n$ are sent to the receiver and are correctly read by the receiver, then there is not infiltration into the system and this receiver is the right person in summative generalization method given in the first chapter as follow:

If you decode the codes e_1, e_2, \dots, e_n , you must also decode the code $e_1 + e_2 + \dots + e_n$, thus you prove that you are a confidential user! If the receiver also decodes this summative code, then he digitally signs. Similarly, the multiplicative generalization method is also used

as a digital signature and finally sending related codes (e_1, e_2) in an upper dimension, i.e., working in $R \times R$ instead of R can be used as a new digital signature method. e_1 and e_2 are sent in this method and it is expected that the receiver decodes finally the text (e_1, e_2) . Its another decipherment acts as a digital signature. Enlarging dimension can remove to the set

$$R^N = \underbrace{R \times R \times \dots \times R}_N$$

easily. Thus, it is understood that the receiver is the right user when the code (e_1, e_2, \dots, e_n) is read.

It is shown that the conducted system generalizations can be worked as a digital signature and a verification method. If a generalization parameter "n" is chosen as $n = p_1q_1$ for a multiplicative generalization, then the top step of the decryption phase of the system is reduced to solve the RSA problem. It is shown how the proposed generalization systems are based on a strong foundation. That is, the reached final phase is

$$e \equiv m^{p_1q_1} \pmod{q}$$

when NTRU decryption steps are applied properly.

A digital signature

$$D_{NTRUSIGN}^n : m \mapsto (m, \sum e_i), \quad 1 \leq i \leq n$$

is defined by means of a mapping

$$D_{NTRUEncrypt}^i : (m, r_i, h_i) \mapsto e_i, \quad 1 \leq i \leq n$$

where all of the parameters are chosen as introduced in the classical NTRU cryptosystem, and a verification of this signature is defined by

$$D_{verification} : \sum e_i \mapsto (m, n, n \pmod{q}), \quad 1 \leq i \leq n$$

and a new NTRU based digital signature is obtained.

12. CONCLUSION AND RECOMMENDATIONS

The basic output of this study is to make a production of NTRU on more comprehensive structure. In this sense, the obtained datas enlarged the system and proposed to constitute the system on large sets for choosings of extra public keys, error polynomials. However, this proposals supporting security, effectiveness and sheltering necessitate the devices which contain a larger processor and more comprehensive memory as a result of many operations

and choosings of key from a larger set. It is obvious that the speed is affected negatively but effectiveness increases by enhancing an usage area and intended use effectiveness increase under existing conditions. These proposals which can be used as a new digital signature method can be affirmed practically. The Cryptoanalysis of a new NTRU generalized system can be done by trying attacks and analyzing new lattice structures corresponding to all these generalizations. Since the main sending message which is constituted in the form of a sum or product of encrypted messages consisting of during the sending of the same message can mean n messages, it can be developed as a probabilistically encryption method. In addition to this, sending different messages in the same time according to this method means sending a huge message in different parts by choosing a larger parameter p so that it is important to preserve the plain text.

REFERENCES

- [1] D. Coppersmith and A. Shamir, Lattice attacks on NTRU, Euro-crypto'97, Lecture Notes in Computer Science, Vol. 1233, Springer, Berlin, (1997).
- [2] Elbasheer, M. O., Mohammed, T. (2015, April). Signing and verifying certificates by NTRU and RSA algorithms. In 2015 International Conference on Cloud Computing (ICCC) (pp. 1-4). IEEE.
- [3] Gentry, C., Szydlo, M. (2002, April). Cryptanalysis of the revised NTRU signature scheme. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 299-320). Springer, Berlin, Heidelberg.
- [4] Hoffstein, J., Silverman, J. (1971). Optimizations for NTRU. Public-Key Cryptography and Computational Number Theory, De Gruyter Proceedings in Mathematics, 77-88.
- [5] Hoffstein, J., Pipher, J., Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.
- [6] Hoffstein, J., Pipher, J., Silverman, J. H. (2001, May). NSS: An NTRU lattice-based signature scheme. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 211-228). Springer, Berlin, Heidelberg.
- [7] Hoffstein, J., Pipher, J., Silverman, J. H. (2001). Enhanced encoding and verification methods for the NTRU signature scheme. Previously posted on <http://www.ntru.com/technology/tech.technical.htm>.
- [8] Hoffstein, J., Silverman, J. H. and Whyte, W. (2003). Estimating breaking times for NTRU lattices, Technical Report 12. Available at <http://www.ntru.com>.
- [9] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., Whyte, W. (2003, April). NTRUSIGN: Digital signatures using the NTRU lattice. In Cryptographers' track at the RSA conference (pp. 122-140). Springer, Berlin, Heidelberg.
- [10] Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W. (2014, October). Transcript secure signatures based on modular lattices. In International Workshop on Post-Quantum Cryptography (pp. 142-159). Springer, Cham.

- [11] Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W., Zhang, Z. (2015). Choosing parameters for NTRU encrypt. NTRU Challenge . Available at <http://www.ntru.com/ntru-challenge>.
- [12] Hong, J., Han, J. W., Kwon, D., Han, D. (2002). Chosen-Ciphertext Attacks on Optimized NTRU. <http://www.ntru.com>.
- [13] Howgrave-Graham, N., Nguyen, P. Q., Pointcheval, D., Proos, J., Silverman, J. H., Singer, A., Whyte, W. (2003, August). The impact of decryption failures on the security of NTRU encryption. In Annual International Cryptology Conference (pp. 226-246). Springer, Berlin, Heidelberg.
- [14] Howgrave-Graham, N., Silverman, J. H., Whyte, W. (2003). A Meet-in-the-Middle Attack on an NTRU Private key (Vol. 4). Technical report, NTRU Cryptosystems, June 2003. Report. Available at <http://www.ntru.com>.
- [15] Howgrave-Graham, N., Silverman, J. H., Singer, A., Whyte, W., Cryptosystems, N. T. R. U. (2003). NAEP: Provable Security in the Presence of Decryption Failures. IACR Cryptol. ePrint Arch., 2003, 172.
- [16] Howgrave-Graham, N., Silverman, J. H., Whyte, W. (2005, February). Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In Cryptographers' Track at the RSA Conference (pp. 118-135). Springer, Berlin, Heidelberg.
- [17] Meskanen, T., Renvall, A. (2003). A Wrap Error Attack against NTRUEncrypt. Turku Centre for Computer Science.
- [18] Näslund, M., Shparlinski, I. E., Whyte, W. (2003, January). On the bit security of NTRUEncrypt. In International Workshop on Public Key Cryptography (pp. 62-70). Springer, Berlin, Heidelberg.
- [19] Nguyen, P. Q., Pointcheval, D. (2002, August). Analysis and improvements of NTRU encryption paddings. In Annual International Cryptology Conference (pp. 210-225). Springer, Berlin, Heidelberg.
- [20] Nitaj, A. (2015). The Mathematics of the NTRU Public Key Cryptosystem. Mathematical Concepts IGI Global.
- [21] Silverman, J. H. (2003). Invisibility truncated polynomial rings. Technical Report . NTRU Cryptosystems, Available at <http://www.ntru.com>.
- [22] Silverman, J. H., Whyte, W. (2005). Estimating decryption failure probabilities for NTRU encrypt, Technical Report 18 . Available at <http://www.ntru.com>.
- [23] Park, S. W., Lee, I. Y. (2013). Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment. Journal of Information Processing Systems, 9(3), 461-476.
- [24] Proos, J. (2003). Imperfect decryption and an attack on the NTRU encryption scheme. Faculty of Mathematics, University of Waterloo.
- [25] Yu-Pu, H. U. (2008). A novel NTRU-class digital signature scheme [J]. Chinese Journal of Computers, 31(9), 1661-1666.

DEPARTMENT OF MATHEMATICS, FACULTY OF ARTS AND SCIENCES, AĞRI İBRAHİM ÇEÇEN UNIVERSITY, AĞRI-TURKEY

DEPARTMENT OF MATHEMATICS AND SCIENCE EDUCATION, ATATURK FACULTY OF EDUCATION, MARMARA UNIVERSITY, ISTANBUL-TURKEY

Contents

1. [Weyl connection on tangent bundle of hypersurface](#)
Rabia Çakan Akpınar 2-13
2. [Translation-factorable surfaces with vanishing curvatures in Galilean 3-spaces](#)
Alev Kelleci 14-26
3. [Sheffer stroke BG-algebras](#)
Tahsin Oner, Tugce Kalkan, Necla Kircali Gursoy 27-39
4. [Plane curves with same equi-affine and Euclidean invariants](#)
Muhittin Evren Aydın, Esra Erdem, Munevver Yıldırım Yılmaz 40-52
5. [A generalization of NTRU cryptosystem and a new digital signature version](#)
Mehmet Sever, Ahmet Sukru Ozdemir 53-66

