axioms

Special Issue Reprint

Computational Algebra, Coding Theory and Cryptography

Theory and Applications, 2nd Edition

Edited by
Hashem Bordbar

mdpi.com/journal/axioms

MDPI

Computational Algebra, Coding Theory and Cryptography: Theory and Applications, 2nd Edition

Computational Algebra, Coding Theory and Cryptography: Theory and Applications, 2nd Edition

Guest Editor

Hashem Bordbar

MDPI

Basel • Beijing • Wuhan • Barcelona • Belgrade • Novi Sad • Cluj • Manchester

Guest Editor
Hashem Bordbar
Center for Information
Technologies and Applied
Mathematics
University of Nova Gorica
Nova Gorica
Slovenia

Editorial Office
MDPI AG
Grosspeteranlage 5
4052 Basel, Switzerland

This is a reprint of the Special Issue, published open access by the journal *Axioms* (ISSN 2075-1680), freely accessible at: https://www.mdpi.com/journal/axioms/special_issues/8I240L33LC.

For citation purposes, cite each article independently as indicated on the article page online and as indicated below:

Lastname, A.A.; Lastname, B.B. Article Title. *Journal Name* **Year**, *Volume Number*, Page Range.

ISBN 978-3-7258-8065-2 (Hbk)
ISBN 978-3-7258-8066-9 (PDF)
https://doi.org/10.3390/books978-3-7258-8066-9

© 2026 by the authors. Articles in this reprint are Open Access and distributed under the Creative Commons Attribution (CC BY) license. The reprint as a whole is distributed by MDPI under the terms and conditions of the Creative Commons Attribution-NonCommercial-NoDerivs (CC BY-NC-ND) license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

Contents

About the Editor . . . . . **vii**

Hashem Bordbar
Computational Algebra, Coding Theory and Cryptography: Theory and Applications, 2nd Edition
Reprinted from: *Axioms* **2026**, *15*, 313, https://doi.org/10.3390/axioms15050313 . . . . . **1**

Dimitrinka Vladeva
Idempotent Triangular Matrices over Additively Idempotent Semirings: Decompositions into Products of Semicentral Idempotents
Reprinted from: *Axioms* **2025**, *14*, 137, https://doi.org/10.3390/axioms14020137 . . . . . **4**

Zhe Yu, Hao Zhan, Yiheng Wang, Zhe Lin and Fei Liang
On the Equational Theory of Lattice-Based Algebras for Layered Graphs
Reprinted from: *Axioms* **2025**, *14*, 257, https://doi.org/10.3390/axioms14040257 . . . . . **32**

Tahsin Oner, Rajesh Neelamegarajan, Ravi Kumar Bandar and Hashem Bordbar
An Investigation into Bipolar Fuzzy Hoop Algebras and Their Applications
Reprinted from: *Axioms* **2025**, *14*, 338, https://doi.org/10.3390/axioms14050338 . . . . . **48**

Artūras Dubickas
Numbers Whose Powers Are Arbitrarily Close to Integers
Reprinted from: *Axioms* **2025**, *14*, 420, https://doi.org/10.3390/axioms14060420 . . . . . **70**

Steven Duplij and Qiang Guo
Polyadic Encryption
Reprinted from: *Axioms* **2025**, *14*, 835, https://doi.org/10.3390/axioms14110835 . . . . . **81**

Hengjia Cao and Chang Tan
An Algorithm for Determining Whether the Quotient Ring Modulo an Ideal Has a Cyclic Basis
Reprinted from: *Axioms* **2025**, *14*, 838, https://doi.org/10.3390/axioms14110838 . . . . . **88**

Tsonka Baicheva and Svetlana Topalova
On the Existence of Optimal (v, 5, 1) and (v, 6, 1) Binary Cyclically Permutable Constant-Weight Codes
Reprinted from: *Axioms* **2026**, *15*, 35, https://doi.org/10.3390/axioms15010035 . . . . . **100**

María Ángeles Moreno-Frías and José C. Rosales
Radical Numerical Semigroups
Reprinted from: *Axioms* **2026**, *15*, 36, https://doi.org/10.3390/axioms15010036 . . . . . **115**

About the Editor

Hashem Bordbar

Hashem Bordbar is an Assistant Professor at the Center for Information Technologies and Applied Mathematics at the University of Nova Gorica. His research interests include commutative and homological algebra, ordered algebra and lattice theory, hypercompositional algebra, algebraic coding theory, cryptography, and fuzzy logic. His recent work focuses on the application of algebraic structures to coding theory, cryptographic systems, and computational mathematics, with particular attention to categorical and combinatorial aspects of hyperstructures and ordered algebras. He has been involved in several international research projects, including projects supported by ARIS and TÜBİTAK, and has collaborated with researchers from different countries. He has published more than 70 papers in WoS and Scopus-indexed journals, authored and edited scientific books and special issues, and serves on the editorial boards of several international journals. His achievements also include research awards, teaching distinctions, invited conference presentations, and the supervision of graduate students.

axioms

MDPI

Editorial

Computational Algebra, Coding Theory and Cryptography: Theory and Applications, 2nd Edition

Hashem Bordbar

Centre for Information Technologies and Applied Mathematics, University of Nova Gorica, 5000 Nova Gorica, Slovenia; hashem.bordbar@ung.si

1. Introduction

Recent developments in algebra, coding theory, and cryptography have shown that algebraic structures play an important role in both theoretical research and practical applications, with modern communication systems, reliable data transmission, and secure information exchange dependent on efficient coding techniques and strong cryptographic protocols. Many of these techniques are closely related to different branches of algebra, including computational algebra; fuzzy algebraic systems; and semigroup, lattice, and semiring theory.

The aim of this Special Issue is to present recent advances that connect algebraic structures with coding theory and cryptography, with a particular focus on new theoretical results; algorithmic developments; and applications related to encoding and decoding procedures, algebraic methods in coding theory, and mathematical tools used in secure communication systems.

This Special Issue contains eight research papers that present different perspectives on the interactions between algebra and applications in coding theory, cryptography, and computational mathematics.

2. Overview of the Published Papers

Contribution 1 studies radical numerical semigroups. For an integer $n \geq 2$, the radical $r(n)$ is defined as the product of all positive prime divisors of n. A numerical semigroup S is called a radical if $s + r(s) \in S$ for every $s \in S \setminus \{0\}$. The authors present three algorithms that help to analyze the structure of radical semigroups, which make it possible to compute all radical numerical semigroups with a fixed genus, Frobenius number, or multiplicity. Furthermore, the authors prove that for every set X of positive integers with $\gcd(X) = 1$, there exists the smallest radical semigroup containing X, and they provide an algorithm to construct it.

Contribution 2 investigates binary cyclically permutable constant-weight codes. The existence problem for optimal $(v, k, 1)$ CPCW codes is completely solved for codeword weights $k < 5$. The authors consider the smallest open cases, namely $k = 5$ and $k = 6$, and construct such codes for small values of the code length v and derive necessary conditions for the existence of optimal $(k(k-1)t + 2, k, 1)$ CPCW codes. These conditions can be used both to construct new codes and to show that optimal codes with certain parameters do not exist. In particular, they prove that an optimal $(92, 6, 1)$ CPCW code does not exist.

Contribution 3 focuses on cyclic bases for quotient rings' modulo zero-dimensional ideals. Based on a necessary and sufficient condition for the existence of cyclic bases, the authors derive an equivalent condition and propose a new algorithm for determining whether a cyclic basis exists, which constructs a matrix and calculates its determinant in

order to verify the condition. Compared with the previous approach, the new algorithm reduces the number of candidate elements that must be considered and therefore improves computational efficiency.

In Contribution 4, a new encryption and decryption procedure based on polyadic algebraic structures and signal processing methods is proposed, which uses signals with integer amplitudes to transmit information. Polyadic techniques are applied to convert the plaintext into sequences of special integers. The receiver restores the plaintext by applying specific rules and solving systems of equations. This work demonstrates how algebraic structures can be used to design alternative cryptographic schemes.

Contribution 5 studies a problem related to fractional parts of sequences of the form $\{\xi_n \alpha^n\}$. The authors prove that for any sequence of positive numbers ξ_n that does not converge to zero faster than an exponential function, and for any sequence of positive numbers δ_n, there exists an uncountable set of positive numbers S such that for each $\alpha > 1$ in S, there are infinitely many integers n for which the inequality $\{\xi_n \alpha^n\} < \delta_n$ holds. The result remains valid regardless of how quickly δ_n approaches zero.

Contribution 6 introduces bipolar fuzzy sub-hoops and bipolar fuzzy filters in hoop algebras, structures which extend classical fuzzy logic by allowing both positive and negative membership degrees. The authors study their main algebraic properties and establish several characterizations of bipolar fuzzy filters using level sets. They also determine the conditions under which these filters become implicative filters. These results contribute to the development of fuzzy algebraic systems and their applications in decision-making, image processing, and reasoning under uncertainty.

Contribution 7 introduces layered algebras and applies them to layered graphs, the latter of which provide a useful abstract model for analyzing complex systems, including applications related to coding in communication systems and access control in security. The authors investigate several classes of lattice-based layered algebras and show that the corresponding varieties have decidable equational theories due to the finite model property.

Contribution 8 studies triangular matrices over additively idempotent semirings. The authors determine explicit forms of idempotent and semicentral idempotent triangular matrices, introducing a diamond composition operation and showing that an idempotent $n \times n$ matrix can be represented as the $(n-1)$th power of a sum of diamond compositions of semicentral idempotents. Using this approach, several types of matrices, including strictly upper triangular, unitriangular, and nil-clean matrices, are decomposed into semicentral idempotents.

The papers collected in this Special Issue demonstrate the strong connection between algebraic structures and modern applications in coding theory, cryptography, and computational mathematics, presenting new theoretical results, algorithms, and mathematical techniques that may stimulate further research in these areas.

As the Guest Editor, I would like to thank all of the authors for their valuable contributions to this Special Issue. I also express my sincere gratitude to the reviewers for their careful evaluation and helpful comments, which greatly improved the quality of the published papers. Finally, I would like to thank the editorial office for their support during the preparation of this Special Issue.

Conflicts of Interest: The author declares no conflicts of interest.

List of Contributions:

1. Moreno-Frías, M.Á.; Rosales, J.C. Radical Numerical Semigroups. *Axioms* **2025**, *15*, 36. https://doi.org/10.3390/axioms15010036.
2. Baicheva, T.; Topalova, S. On the Existence of Optimal (v, 5, 1) and (v, 6, 1) Binary Cyclically Permutable Constant-Weight Codes. *Axioms* **2026**, *15*, 35. https://doi.org/10.3390/axioms15010035.

3. Cao, H.; Tan, C. An Algorithm for Determining Whether the Quotient Ring Modulo an Ideal Has a Cyclic Basis. *Axioms* **2025**, *14*, 838. https://doi.org/10.3390/axioms14110838.
4. Duplij, S.; Guo, Q. Polyadic Encryption. *Axioms* **2025**, *14*, 835. https://doi.org/10.3390/axioms14110835.
5. Dubickas, A. Numbers Whose Powers Are Arbitrarily Close to Integers. *Axioms* **2025**, *14*, 420. https://doi.org/10.3390/axioms14060420.
6. Oner, T.; Neelamegarajan, R.; Bandaru, R.K.; Bordbar, H. An Investigation into Bipolar Fuzzy Hoop Algebras and Their Applications. *Axioms* **2025**, *14*, 338. https://doi.org/10.3390/axioms14050338.
7. Yu, Z.; Zhan, H.; Wang, Y.; Lin, Z.; Liang, F. On the Equational Theory of Lattice-Based Algebras for Layered Graphs. *Axioms* **2025**, *14*, 257. https://doi.org/10.3390/axioms14040257.
8. Vladeva, D. Idempotent Triangular Matrices over Additively Idempotent Semirings: Decompositions into Products of Semicentral Idempotents. *Axioms* **2025**, *14*, 137. https://doi.org/10.3390/axioms14020137.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

Idempotent Triangular Matrices over Additively Idempotent Semirings: Decompositions into Products of Semicentral Idempotents

Dimitrinka Vladeva

Department of Algebra and Logic, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; d_vladeva@abv.bg

Abstract: The explicit forms of idempotent and semicentral idempotent triangular matrices over an additively idempotent semiring are obtained. We define a diamond composition of idempotents and give a representation of an idempotent $n \times n$ matrix as an $(n-1)$ th degree of a sum of diamond compositions of semicentral idempotents. We construct a decomposition of a strictly upper matrix, a unitriangular matrix, and a nil-clean matrix by semicentral idempotents.

Keywords: additively idempotent semirings; matrix semirings; triangular matrices; idempotents; semicentral idempotents

MSC: 15A24; 15A80; 16S50; 16Y60; 17C27

1. Introduction and Preliminaries

In the second half of the past century, a number of mathematicians realized the useful features and the significant applications of a certain type of semiring structure. Semirings are structures that are associative and distributive on both sides but do not, in general, have additive inverses. These semiring structures are additively idempotent, like Boolean and fuzzy algebras.

There are prominent applications for additively idempotent semirings including optimization and control, differential equations, algebraic geometry, dynamic programming, mathematical physics and chemistry, mathematical biology, interval analysis, mathematical economics, game theory, computer technology, Petri nets, and cryptography (see [1–8]).

On the other hand, idempotents play an important role in ring theory and are closely related to matrices since the matrix units are idempotents. There is very extensive research dealing with idempotents. Following V. Drensky (see [9]), idempotents were introduced by Benjamin Peirce [10] in 1870.

In 2021, X. Hou (see [11]) provided a complete characterization of idempotent triangular matrices over a ring in which zero and one were the only idempotent elements.

In 2022, S. Wright (see [12]) characterized the idempotency of upper triangular matrices with entries from an arbitrary ring. Very recently, D. Vladeva (see [13,14]) considered the semicentral idempotents of upper triangular matrix rings.

The study of idempotents of additively idempotent semirings has a short history. In 2013, I. Trendafilov and D. Vladeva (see [15]) proved that in the endomorphism semiring of a finite chain, the set of all idempotents with s fixed points, $k_1, \ldots, k_s$, $1 \leq s \leq n-1$, is a semiring of order $\prod_{m=1}^{s-1}(k_{m+1} - k_m)$. In the main result of the paper the authors prove that

the set of roots of a fixed idempotent of the endomorphism semiring of a finite chain is a semiring of the order $C_{k_{1,1}}\left(\prod_{i=1}^{\ell-1} C_{t_i}C_{s_i}\right)C_{n-1-k_{\ell,m_\ell}}$, where C_p is the p–th Catalan number.

In 2018, I. Chajda and H. Länger (see [16]) investigated a variety of commutative additively and multiplicatively idempotent semirings.

In 2020, D. Vladeva (see [17]) studied a class of the right ideals of a subsemiring of the endomorphism semiring of a finite chain and considered projections on these ideals, which were derivations. For one of these derivations, $d_{\ell,m}$, and for the fixed endomorphism α_0, the set of endomorphisms α such that $d_{\ell,m}(\alpha) = \alpha_0$ is denoted by $\int \alpha_0 d_{\ell,m}$. The last set is a semiring if and only if α_0 is an idempotent. The number of the semirings, $\int \alpha_0 d_{\ell,m}$, where $1 \leq m \leq n-1$, is equal to F_{2m}, which is the $2m$ th Fibonacci number.

In 2023, D. Vladeva (see [18]) suggested the following definitions:

1. Let S and S_0 be additively idempotent semirings, S be a noncommutative semiring and an S_0-semimodule, S_0 be a commutative semiring, and $\alpha s = s\alpha$ for any $\alpha \in S_0$ and $s \in S$. Then, S is called an S_0-semialgebra.
2. Let S be an S_0-semialgebra and $\mathcal{B}(S) = \{e_{ij}\},\ i,j = 1,\ldots,n$, a basis of S (relative to S_0) with the following properties:
   - $e_{ij}e_{kl} = \begin{cases} e_{il}, & \text{if } j \leq k \\ 0, & \text{if } j > k \end{cases}, i,j,k,l = 1,\ldots,n.$
   - $\sum_{i=1}^{n} e_{ii} = 1_S$, where 1_S is the identity of S.
   - $e_{ij} > e_{ik}$ for all $k > j$ and $e_{ij} > e_{hj}, h < i$.

Then, $\mathcal{B}(S)$ is called an e-basis. The basis elements e_{ii} are idempotents, and since $e_{ii}e_{jj} = e_{ij}$ but $e_{jj}e_{ii} = 0$, if $i < j$, they do not commute. In this paper, we prove the following: *Let S be an S_0-semialgebra and $\mathcal{B}(S) = \{e_{ij}\},\ i,j = 1,\ldots,n$ an e-basis of S. Then, S is isomorphic to a matrix subsemiring of $M_n(S_0)$.* From this theorem, it follows that if $\mathcal{B}(S)$ is a triangular e-basis, then S is isomorphic to a subsemiring of the semiring of upper triangular matrices.

Throughout the present paper, all semirings considered shall be assumed to be additively idempotent and possess an identity and a zero. Basic facts about additively idempotent semirings can be found in the seminal book of J. Golan (cf. [19]).

The present paper contains only new results and is arranged as follows. In Section 2, we obtain the explicit form of an arbitrary idempotent triangular matrix over an additively idempotent semiring. The next section deals with the left and right semicentral idempotents of an additively idempotent semiring. A new type of semicentral idempotent, called Jordan, specific for an additively idempotent semiring, is studied. We define a diamond composition, $e_1 \diamond e_2 = e_1 + e_2 + e_1e_2$, where e_1 and e_2 are idempotents and $e_2e_1 = 0$, which plays a crucial role in the decompositions of many triangular matrices. In Section 4, we find the explicit form of an arbitrary left and right semicentral idempotent triangular matrix. In the last four sections, we consider the decompositions of idempotent, strictly upper, unitriangular, and nil-clean triangular matrices by semicentral idempotent matrices.

2. Results on Idempotents of Triangular Matrix Semiring

In the following, S is an additively idempotent semiring and $T_n(S)$ is the semiring of $n \times n$ triangular matrices over S.

Example 1. *It is well known that all the entries on the main diagonal of an idempotent triangular matrix are idempotents. Let* $\begin{pmatrix} e_1 & x_{12} \\ 0 & e_2 \end{pmatrix}^2 = \begin{pmatrix} e_1 & x_{12} \\ 0 & e_2 \end{pmatrix}$, *where* $e_1, e_2, x_{12} \in S$ *and* $e_i^2 = e_i$,

$i = 1, 2$. *Then,* $e_1x_{12} + x_{12}e_2 = x_{12}$, *which implies that* $e_1x_{12} + e_1x_{12}e_2 = e_1x_{12}$ *and* $x_{12} = e_1x_{12} + e_1x_{12}e_2 + x_{12}e_2$. *For an arbitrary* $\alpha_{12} \in S$, *it follows that*

$$E(e_1, e_2) = \begin{pmatrix} e_1 & e_1\alpha_{12} + e_1\alpha_{12}e_2 + \alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix} \tag{1}$$

is an idempotent matrix. Thus, (1) *represents the idempotent matrices of* $T_2(S)$.

Note that when $\alpha_{12} = e_1\beta_{12}e_2$, *we obtain the idempotent matrix* $\begin{pmatrix} e_1 & e_1\beta_{12}e_2 \\ 0 & e_2 \end{pmatrix}$, *and this matrix is a particular case of* (1). *Moreover, we have* $\begin{pmatrix} e_1 & e_1\alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}\begin{pmatrix} e_1 & e_1\beta_{12}e_2 \\ 0 & e_2 \end{pmatrix} = \begin{pmatrix} e_1 & e_1\alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix} + \begin{pmatrix} e_1 & e_1\beta_{12}e_2 \\ 0 & e_2 \end{pmatrix}$; *thus, idempotent matrices of this form commute.*

Example 2. *Let* $X = \begin{pmatrix} e_1 & x_{12} & x_{13} \\ 0 & e_2 & x_{23} \\ 0 & 0 & e_3 \end{pmatrix}$, *where* $e_i, x_{ij} \in S$, $i, j = 1, 2, 3$, $i < j$, *and* $e_i^2 = e_i$, *be an idempotent matrix. As in the previous example, we have* $x_{12} = e_1x_{12} + e_1x_{12}e_2 + x_{12}e_2$, $x_{23} = e_2x_{23} + e_2x_{23}e_3 + x_{23}e_3$, *and* $x_{13} = e_1x_{13} + e_1x_{13}e_3 + x_{13}e_3 + x_{12}x_{23}$.

For arbitrary $\alpha_{12}, \alpha_{13}, \alpha_{23} \in S$, *we denote* $\delta_{ij} = e_i\alpha_{ij} + e_i\alpha_{ij}e_j + \alpha_{ij}e_j$ *(this concept should not be confused with the Kroneker symbol). Thus,* $x_{12} = \delta_{12}$, $x_{23} = \delta_{23}$, *and* $x_{13} = \delta_{13} + \delta_{12}\delta_{23}$. *Conversely, for arbitrary* $\alpha_{12}, \alpha_{13}, \alpha_{23} \in S$, *we consider* $X = \begin{pmatrix} e_1 & \delta_{12} & \delta_{13} + \delta_{12}\delta_{23} \\ 0 & e_2 & \delta_{23} \\ 0 & 0 & e_3 \end{pmatrix}$, *where* $\delta_{ij} = e_i\alpha_{ij} + e_i\alpha_{ij}e_j + \alpha_{ij}e_j$. *We obtain that* $e_1\delta_{12} + \delta_{12}e_2 = \delta_{12}$ *and* $e_2\delta_{23} + \delta_{23}e_3 = \delta_{23}$. *Since* $e_i\delta_{ij} + \delta_{ij} = \delta_{ij}$ *and* $\delta_{ij}e_j + \delta_{ij} = \delta_{ij}$, *it follows that* $e_1\delta_{12}\delta_{23} + \delta_{12}\delta_{23} = \delta_{12}\delta_{23}$ *and* $\delta_{12}\delta_{23}e_3 + \delta_{12}\delta_{23} = \delta_{12}\delta_{23}$. *Then,* $e_1(\delta_{13} + \delta_{12}\delta_{23}) + \delta_{12}\delta_{23} + (\delta_{13} + \delta_{12}\delta_{23})e_3 = \delta_{13} + \delta_{12}\delta_{23}$ *and* X *is an idempotent matrix. Hence,*

$$E(e_1, e_2, e_3) = \begin{pmatrix} e_1 & \delta_{12} & \delta_{13} + \delta_{12}\delta_{23} \\ 0 & e_2 & \delta_{23} \\ 0 & 0 & e_3 \end{pmatrix}$$

is the general form of the idempotent matrix of $T_3(S)$.

The next result is similar to Theorem 3.1 of S. Wright (cf. [12]) but different as we work in an additively idempotent matrix semiring.

Theorem 1. *An* $n \times n$ *upper triangular matrix,* $X = (x_{ij})$, *over the additively idempotent semiring* S *is idempotent if and only if* $x_{ii} = e_i$, *where* $e_i^2 = e_i$ *for* $i = 1, \ldots, n$, *and* $x_{ij} = \delta_{ij} + \sum_{k=i+1}^{j-1} x_{ik}x_{kj}$, *where* $\delta_{ij} = e_i\alpha_{ij} + e_i\alpha_{ij}e_j + \alpha_{ij}e_j$, $\alpha_{ij} \in S$ *for* $i, j = 1, \ldots, n$ *and* $i + 1 < j$. *If* $j = i + 1$, *then* $x_{i\,i+1} = \delta_{i\,i+1}$.

Proof. Let $X = (x_{ij})$ be an idempotent matrix. Then, $x_{ii} = e_i$ are idempotents for $i = 1, \ldots, n$, and for $i + 1 < j$, it follows that $x_{ij} = \sum_{k=i}^{j} x_{ik}x_{kj} = e_ix_{ij} + x_{ij}e_j + \sum_{k=i+1}^{j-1} x_{ik}x_{kj}$. Since $e_ix_{ij} + x_{ij} = x_{ij}$ and $x_{ij}e_j + x_{ij} = x_{ij}$, we have $e_ix_{ij}e_j + x_{ij}e_j = x_{ij}e_j$ and $e_ix_{ij}e_j + e_ix_{ij} = e_ix_{ij}$. Therefore, $e_ix_{ij} + x_{ij}e_j = \delta_{ij}$. If $j = i + 1$, we have $x_{i\,i+1} = e_ix_{i\,i+1} + x_{i\,i+1}e_{i+1} = \delta_{i\,i+1}$.

Conversely, for the matrix $X = (x_{ij})$, we assume that $x_{ii} = e_i$, $i = 1, \ldots, n$ are idempotents, $x_{i\,i+1} = \delta_{i\,i+1}$ and $x_{ij} = \delta_{ij} + \sum_{k=i+1}^{j-1} x_{ik}x_{kj}$, for $i + 1 < j$. Our induction hypothesis is the following.

Suppose that for a fixed $j \leq n$, the matrices with the main diagonal $x_{ii}, \ldots, x_{kk}$, where i is an arbitrary positive integer and $i < k < j$, are idempotent.

Now, X is an idempotent matrix if and only if for the arbitrary element x_{ij}, where $i+1 < j$, we prove that $x_{ij} = e_i x_{ij} + x_{ij} e_j + \sum_{k=i+1}^{j-1} x_{ik} x_{kj}$. From the assumption of x_{ij}, it follows that the right side of the last equality is

$$e_i \left(\delta_{ij} + \sum_{k=i+1}^{j-1} x_{ik} x_{kj} \right) + \sum_{k=i+1}^{j-1} x_{ik} x_{kj} + \left(\delta_{ij} + \sum_{k=i+1}^{j-1} x_{ik} x_{kj} \right) e_j =$$

$$= e_i \delta_{ij} + \delta_{ij} e_j + \sum_{k=i+1}^{j-1} \left(e_i x_{ik} x_{kj} + x_{ik} x_{kj} e_j \right) + \sum_{k=i+1}^{j-1} x_{ik} x_{kj}.$$

From this inductive conjecture, we have $e_i x_{ik} + x_{ik} = x_{ik}$ and $x_{kj} e_j + x_{kj} = x_{kj}$ for $k, i < k < j$. Then, $e_i x_{ik} x_{kj} + x_{ik} x_{kj} = x_{ik} x_{kj}$ and $x_{ik} x_{kj} e_j + x_{ik} x_{kj} = x_{ik} x_{kj}$. Hence,

$$\sum_{k=i+1}^{j-1} \left(e_i x_{ik} x_{kj} + x_{ik} x_{kj} e_j \right) + \sum_{k=i+1}^{j-1} x_{ik} x_{kj} = \sum_{k=i+1}^{j-1} x_{ik} x_{kj}.$$

Since $e_i \delta_{ij} + \delta_{ij} e_j = \delta_{ij} = e_i x_{ij} + x_{ij} e_j$, it follows that X is an idempotent matrix. □

For matrices over a field, the root of the matrix X is the matrix Y, such that $Y^m = X$ for some positive integer, $m > 1$ (see F. R. Gantmacher [20], Ch. 8). In 1979, S. K. Jain et al. (see [21]) studied the nonnegative m th roots of a nonnegative 0-symmetric idempotent matrix. Now, let Y be a matrix over an additively idempotent semiring and $Y = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Since $Y^2 = X = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, it follows that Y is a square root of X. It is easy to check that X is an idempotent matrix. Thus, the following question is reasonable:

Can we find a square root of an arbitrary 3×3 *idempotent triangular matrix?*

In the following, we will answer a more general question in the semiring of upper triangular matrices over an additively idempotent semiring, S.

Let us consider the matrix $\Delta = (\delta_{ij})$, $i, j = 1, \ldots, n$, $i \leq j$, where $\delta_{ii} = e_i$, $e_i^2 = e_i$, $\delta_{ij} = e_i \alpha_{ij} + e_i \alpha_{ij} e_j + \alpha_{ij} e_j$, and α_{ij} are arbitrary elements of S for $i, j = 1, \ldots, n$ and $i < j$. From Theorem 1, it follows that if X is an arbitrary idempotent triangular matrix, then $X + \Delta = X$. This implies that $X + \Delta X = X$ and $X + X\Delta = X$ and then from $(X + \Delta)^2 = X$ we have $X + \Delta^2 = X$. In the same way, it follows that $X + \Delta^m = X$, where m is a positive integer. Now, we will prove that $\Delta^{n-1} = \Delta^n$.

Theorem 2. *Let S be an additively idempotent semiring, $\Delta = (\delta_{ij}) \in T_n(S)$, $i, j = 1, \ldots, n$, $i \leq j$, where $\delta_{ii} = e_i$, $e_i^2 = e_i$ and $\delta_{ij} = e_i \alpha_{ij} + e_i \alpha_{ij} e_j + \alpha_{ij} e_j$, $\alpha_{ij} \in S$ for $i, j = 1, \ldots, n$ and $i < j$. Then, $\Delta^{n-1} = \Delta^n$ and Δ^{n-1} is an idempotent matrix.*

Proof. We obtain that $\Delta^2 = (\delta_{ij}^{(2)})$, where $\delta_{ii}^{(2)} = e_i$, $\delta_{i\,i+1}^{(2)} = \delta_{i\,i+1}$ and for $j \geq i+2$, $\delta_{ij}^{(2)} = \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik} \delta_{kj}$. Note that from the last equality, it follows that on the second super-diagonal all entries are $\delta_{i\,i+2} + \delta_{i\,i+1} \delta_{i+1\,i+2}$ and on the third super-diagonal all entries are $\delta_{i\,i+3} + \delta_{i\,i+1} \delta_{i+1\,i+3} + \delta_{i\,i+2} \delta_{i+2\,i+3}$. The proof is by induction. Let us assume

that for an integer, m, where $m \geq 2$, we have $\Delta^m = (\delta_{ij}^{(m)})$, where $\delta_{ii}^{(m)} = e_i$, $\delta_{ii+1}^{(m)} = \delta_{i\,i+1}$, $\delta_{i\,i+2}^{(m)} = \delta_{i\,i+2} + \delta_{i\,i+1}\delta_{i+1\,i+2}$, and for $j \geq i+m$

$$\delta_{ij}^{(m)} = \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} + \cdots + \sum_{\substack{k_1,\ldots,k_{m-1}=i+1 \\ k_1<\cdots<k_{m-1}}}^{j-1} \delta_{ik_1}\ldots\delta_{k_{m-1}j}.$$

In order to find Δ^{m+1}, we obtain that

$$\begin{aligned}
&\delta_{ii}^{(m+1)} = e_i\delta_{ii}^{(m)} = e_i^2 = e_i,\\
&\delta_{ii+1}^{(m+1)} = e_i\delta_{ii+1}^{(m)} + \delta_{ii+1}e_{i+1} = \delta_{ii+1},\\
&\delta_{i\,i+2}^{(m+1)} = e_i\delta_{i\,i+2}^{(m)} + \delta_{i\,i+1}\delta_{i+1\,i+2}^{(m)} + \delta_{i\,i+2}e_{i+2} =\\
&= e_i\delta_{i\,i+2} + e_i\delta_{i\,i+1}\delta_{i+1\,i+2} + \delta_{i\,i+1}\delta_{i+1\,i+2} + \delta_{i\,i+2}e_{i+2} = \delta_{i\,i+2} + \delta_{i\,i+1}\delta_{i+1\,i+2},
\end{aligned}$$

For $j \geq i+m+1$, it follows that

$$\begin{aligned}
\delta_{ij}^{(m+1)} &= e_i\delta_{ij}^{(m)} + \delta_{i\,i+1}\delta_{i+1\,j}^{(m)} + \delta_{i\,i+2}\delta_{i+2\,j}^{(m)} + \cdots + \delta_{i\,j-2}\delta_{j-2\,j}^{(m)} + \delta_{i\,j-1}\delta_{j-1\,j}^{(m)} + \delta_{ij}e_j =\\
&= e_i\delta_{ij} + e_i\left(\sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} + \cdots + \sum_{\substack{k_1,\ldots,k_{m-1}=i+1 \\ k_1<\cdots<k_{m-1}}}^{j-1} \delta_{ik_1}\ldots\delta_{k_{m-1}j}\right) +\\
&+\delta_{i\,i+1}\left(\delta_{i+1\,j} + \sum_{k=i+2}^{j-1} \delta_{i+1\,k}\delta_{kj} + \cdots + \sum_{\substack{k_1,\ldots,k_{m-1}=i+2 \\ k_1<\cdots<k_{m-1}}}^{j-1} \delta_{i+1\,k_1}\ldots\delta_{k_{m-1}j}\right) +\\
&+\delta_{i\,i+2}\left(\delta_{i+2\,j} + \sum_{k=i+3}^{j-1} \delta_{i+2\,k}\delta_{kj} + \cdots + \sum_{\substack{k_1,\ldots,k_{m-1}=i+3 \\ k_1<\cdots<k_{m-1}}}^{j-1} \delta_{i+2\,k_1}\ldots\delta_{k_{m-1}j}\right) +\\
&+\cdots + \delta_{i\,j-2}\delta_{j-2\,j} + \delta_{i\,j-2}\delta_{j-2\,j-1}\delta_{j-1\,j} + \delta_{i\,j-1}\delta_{j-1\,j} + \delta_{ij}e_j =\\
&= \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} + \cdots + \sum_{\substack{k_1,\ldots,k_m=i+1 \\ k_1<\cdots<k_m}}^{j-1} \delta_{i\,k_1}\ldots\delta_{k_mj}.
\end{aligned}$$

Therefore,

$$\Delta^{n-1} = \begin{pmatrix}
e_1 & \delta_{12} & \delta_{13}+\delta_{12}\delta_{23} & \cdots & \delta_{1n} + \sum_{k=2}^{n-1}\delta_{1k}\delta_{kn} + \cdots + \delta_{12}\delta_{23}\ldots\delta_{n-1\,n}\\
0 & e_2 & \delta_{23} & \cdots & \delta_{2n} + \sum_{k=3}^{n-1}\delta_{2k}\delta_{kn} + \cdots + \delta_{23}\ldots\delta_{n-1\,n}\\
0 & 0 & e_3 & \cdots & \delta_{3n} + \sum_{k=4}^{n-1}\delta_{3k}\delta_{kn} + \cdots + \delta_{34}\ldots\delta_{n-1\,n}\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
0 & 0 & 0 & \cdots & e_n
\end{pmatrix}.$$

Now, it is easy to check that $\Delta^n = \Delta^{n-1}$. As a consequence, it follows that $\Delta^{n-1} = \Delta^{n+1} = \cdots = (\Delta^{n-1})^2$. □

The next result describes all idempotent triangular matrices over an additively idempotent semiring.

Theorem 3. *An $n \times n$ upper triangular matrix, $X = (x_{ij})$, over the additively idempotent semiring S is idempotent if and only if $x_{ii} = e_i$, where $e_i^2 = e_i$ for $i = 1, \dots, n$, $x_{i\,i+1} = \delta_{i\,i+1}$ for $i = 1, \dots, n-1$, and*

$$x_{ij} = \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} + \sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \delta_{ik}\delta_{kk_1}\delta_{k_1j} + \cdots + \delta_{ii+1}\dots\delta_{j-1j},$$

where $\delta_{ij} = e_i\alpha_{ij} + e_i\alpha_{ij}e_j + \alpha_{ij}e_j$, $\alpha_{ij} \in S$ for $i, j = 1, \dots, n$ and $i+1 < j$.

Proof. From Theorem 1, we know that the matrix $X = (x_{ij})$ is idempotent if and only if $x_{ii} = e_i$, where $e_i^2 = e_i$ for $i = 1, \dots, n$, $x_{i\,i+1} = \delta_{i\,i+1}$ and $x_{ij} = \delta_{ij} + \sum_{k=i+1}^{j-1} x_{ik}x_{kj}$ for $i+1 < j$. Successively applying this equality, we obtain $x_{ij} =$

$$\delta_{ij} + \sum_{k=i+1}^{j-1} \left(\delta_{ik} + \sum_{k_2=i+1}^{k-1} x_{ik_2}x_{k_2k}\right)\left(\delta_{kj} + \sum_{k_1=k+1}^{j-1} x_{kk_1}x_{k_1j}\right) = \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} +$$

$$+ \sum_{k=i+1}^{j-1} \delta_{ik}\left(\sum_{k_1=k+1}^{j-1}\left(\delta_{kk_1} + \sum_{k_3=k1+1}^{k_1-1} x_{kk_3}x_{k_3k_1}\right)\left(\delta_{k_1j} + \sum_{k_4=k_1+1}^{j-1} x_{k_1k_4}x_{k_4j}\right)\right) +$$

$$+ \sum_{k=i+1}^{j-1}\left(\sum_{k_2=i+1}^{k-1}\left(\delta_{ik_2} + \sum_{k_5=i+1}^{k_2-1} x_{ik_5}x_{k_5k_2}\right)\left(\delta_{k_2k} + \sum_{k_6=k_2+1}^{k-1} x_{k_2k_6}x_{k_6k}\right)\right)\delta_{kj} =$$

$$= \delta_{ij} + \sum_{k=i+1}^{j-1} \delta_{ik}\delta_{kj} + \sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \delta_{ik}\delta_{kk_1}\delta_{k_1j} + \sigma.$$

Some summands are reproduced; for example, $\sum_{k_2=i+1}^{k-1} \delta_{ik_2}\delta_{k_2k}\delta_{kj}$ is a part of $\sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \delta_{ik}\delta_{kk_1}\delta_{k_1j}$. For the sum

$$\sigma = \sum_{k=i+1}^{j-1} \delta_{ik}\left[\sum_{k_1=k+1}^{j-1}\left(\delta_{kk_1}\sum_{k_4=k_1+1}^{j-1} x_{k_1k_4}x_{k_4j} + \sum_{k_3=k+1}^{k_1-1} x_{kk_3}x_{k_3k_1}\delta_{k_1j}\right) +\right.$$

$$\left. + \sum_{k_2=i+1}^{k-1}\left(\delta_{ik_2}\sum_{k_6=k_2+1}^{k-1} x_{k_2k_6}x_{k_6k} + \sum_{k_5=i+1}^{k_2-1} x_{ik_5}x_{k_5k_2}\delta_{k_2k}\right)\right]\delta_{kj},$$

we have the following:

σ contains $\sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \delta_{ik}\delta_{kk_1}\delta_{k_1j}$ and is part of this sum;

σ contains all products $\delta_{im_1}\dots\delta_{m_sj}$ where $m_1 < \cdots < m_s$ and consequently the product $\delta_{ii+1}\dots\delta_{j-1j}$.

Hence, the result follows. □

Remark 1. *We denote the equality from Theorem 3 briefly by*

$$x_{ij} = \delta_{ij} + \sum_{i}^{j} * \tag{2}$$

and use it in Section 4.

Immediately from Theorems 2 and 3, we have the following.

Corollary 1. *Each $n \times n$ upper triangular idempotent matrix $E(e_1, \ldots, e_n)$ over the additively idempotent semiring S has the form*

$$\begin{pmatrix} e_1 & \delta_{12} & \delta_{13} + \delta_{12}\delta_{23} & \cdots & \delta_{1n} + \sum_{k=2}^{n-1} \delta_{1k}\delta_{kn} + \cdots + \delta_{12}\delta_{23}\ldots\delta_{n-1\,n} \\ 0 & e_2 & \delta_{23} & \cdots & \delta_{2n} + \sum_{k=3}^{n-1} \delta_{2k}\delta_{kn} + \cdots + \delta_{23}\ldots\delta_{n-1\,n} \\ 0 & 0 & e_3 & \cdots & \delta_{3n} + \sum_{k=4}^{n-1} \delta_{3k}\delta_{kn} + \cdots + \delta_{34}\ldots\delta_{n-1\,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & e_n \end{pmatrix}, \tag{3}$$

where $\delta_{ij} = e_i\alpha_{ij} + e_i\alpha_{ij}e_j + \alpha_{ij}e_j$, $\alpha_{ij} \in S$ for $i, j = 1, \ldots, n$ and $i < j$.

Each idempotent matrix, $E(e_1, \ldots, e_n)$, has roots, which are the matrices Δ^m, where $m = 1, \ldots, n-2$.

As a consequence of the theorems above, we can show a result similar to the main theorem of X. Hou (cf. [11]).

Corollary 2. *Let $\Delta = (a_{ij}) \in T_n(S)$ be a matrix with the following properties:*

(i) All diagonal entries of Δ are ones or zeroes;

(ii) If $a_{ii} = a_{jj} = 0$, then $a_{ij} = 0$, where $i, j = 1, \ldots, n$ and $i < j$.

Then, all idempotent triangular matrices over S with only zeroes and ones on the main diagonal are the matrices $E = (x_{ij})$ such that $x_{ii} = a_{ii}$, $i = 1, \ldots, n$, and

$$x_{ij} = a_{ij} + \sum_{k=i+1}^{j-1} a_{ik}a_{kj} + \sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} a_{ik}a_{k\,k_1}a_{k_1\,j} + \cdots + a_{i\,i+1}\ldots a_{j-1\,j}, 1 \le i < j \le n.$$

Proof. If in the proof of Theorem 2 at least one of the idempotents e_i and e_j are equal to 1, it follows that $\delta_{ij} = a_{ij}$. When $e_i = e_j = 0$, we have $\delta_{ij} = 0$. Therefore, the matrix Δ is the same matrix Δ in the proof of Theorem 2 under the given conditions. This result follows from Theorem 3. □

Since the entries of the idempotent matrix in (3) have rather complex structures, we obtain idempotent matrices with the parameters α_{ij} of a special form. Such a matrix is $\begin{pmatrix} e_1 & e_1\alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}$, considered in Example 1. To develop this idea to its conclusion, we construct the matrix $\Gamma = (\gamma_{ij})$, where $\gamma_{ii} = e_i$, $e_i^2 = e_i$ for $i = 1, \ldots, n$ and $\gamma_{ij} = e_i\alpha_{ij}e_j$, $\alpha_{ij} \in S$ for $1 < i < j \le n$. Matrices of the form Γ which are idempotents are called special idempotents. It is not difficult to verify that for $n = 3$, the matrix $\Gamma = \begin{pmatrix} e_1 & e_1\alpha_{12}e_2 & e_1\alpha_{13}e_3 \\ 0 & e_2 & e_2\alpha_{23}e_3 \\ 0 & 0 & e_3 \end{pmatrix}$ is not an idempotent, but the matrix $\Gamma^2 = \begin{pmatrix} e_1 & e_1\alpha_{12}e_2 & e_1\alpha_{13}e_3 + e_1\alpha_{12}e_2\alpha_{23}e_3 \\ 0 & e_2 & e_2\alpha_{23}e_3 \\ 0 & 0 & e_3 \end{pmatrix}$ is an idempotent. Moreover, $\Gamma^2 = \begin{pmatrix} e_1 & e_1\beta_{12}e_2 & e_1\beta_{13}e_3 \\ 0 & e_2 & e_2\beta_{23}e_3 \\ 0 & 0 & e_3 \end{pmatrix}$, where $\beta_{12} = \alpha_{12}$, $\beta_{13} = \alpha_{13} + \alpha_{12}e_2\alpha_{23}$ and $\beta_{23} = \alpha_{23}$. . Thus, for $n = 3$, the matrix Γ^2 is a special idempotent matrix.

Theorem 4. *Let $\Gamma = (\gamma_{ij}) \in T_n(S)$, where $\gamma_{ii} = e_i$, $e_i^2 = e_i$, for $i = 1, \ldots, n$ and $\gamma_{ij} = e_i\alpha_{ij}e_j$, $\alpha_{ij} \in S$ for $1 < i < j \le n$. Then, Γ^{n-1} is a special idempotent matrix.*

Proof. Since $e_i\gamma_{ij} = \gamma_{ij}$ and $\gamma_{ij}e_j = \gamma_{ij}$, it follows that the proof of the statement that Γ^{n-1} is an idempotent matrix is the same as the proof of Theorem 2. Following the proof of this theorem, we obtain that $\Gamma^{n-1} = (\gamma^{(n-1)})$, where

$$\gamma_{ij}^{(n-1)} = \gamma_{ij} + \sum_{k=i+1}^{j-1} \gamma_{ik}\gamma_{kj} + \sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \gamma_{ik}\gamma_{kk_1}\gamma_{k_1j} + \cdots + \gamma_{ii+1}\cdots\gamma_{j-1j} =$$

$$= e_i \left(\alpha_{ij} + \sum_{k=i+1}^{j-1} \alpha_{ik}e_k\alpha_{kj} + \sum_{\substack{k,k_1=i+1 \\ k<k_1}}^{j-1} \alpha_{ik}e_k\alpha_{kk_1}e_{k_1}\alpha_{k_1j} + \right.$$

$$\left. + \cdots + \alpha_{ii+1}e_{i+1}\alpha_{i+1\,i+2}\ldots\alpha_{j-2\,j-1}e_{j-1}\alpha_{j-1j} \right) e_j$$

and this completes the proof. □

The set of special idempotent matrices is denoted by $\mathcal{SP}(S)$. This notation is used in Section 4.

3. Definitions and Results of Idempotents of Additively Idempotent Semiring

Let S be an additively idempotent semiring. Following G. F. Birkenmeier et al. (see [22]), we give the following definition: An idempotent, $\ell \in S$ (*resp.*, $r \in S$), is called left (resp., right) semicentral if $\ell x\ell = x\ell$ (resp., $rxr = rx$) for an arbitrary $x \in S$.

From this definition, we easily have the following.

Proposition 1. *The set of left (resp., right) semicentral idempotents of the semiring S is a multiplicative semigroup with an identity.*

The multiplicative semigroup of the left (resp., right) semicentral idempotents of the semiring S is denoted by $(\mathcal{L}(S), .)$ (resp., $(\mathcal{R}(S), .)$).

For $\ell_1, \ell_2 \in \mathcal{L}(S)$, we consider the Jordan product $\ell_1 \circ \ell_2 = \ell_1\ell_2 + \ell_2\ell_1$. Similarly, for $r_1, r_2 \in \mathcal{R}(S)$, we define $r_1 \circ r_2 = r_1r_2 + r_2r_1$. It is straightforward to prove the following.

Proposition 2. *The semigroup $\mathcal{L}(S)$ (resp., $\mathcal{R}(S)$) is closed under the Jordan product.*

Let $\mathcal{LR}(S)$ be the semigroup generated by $\mathcal{L}(S) \cup \mathcal{R}(S)$. For the products and Jordan products of elements of $\mathcal{LR}(S)$, we easily have the following.

Proposition 3. *Let $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$. Then, we have the following:*

(i) $r\ell$ is an idempotent, but it is neither a left nor a right semicentral idempotent; also, $\ell rx\ell r = r\ell xr\ell$ for all $x \in R$ and then $(\ell r)^2 = r\ell$.

(ii) $(\ell \circ r)^2 = r\ell$.

(iii) $r \circ r\ell = \ell \circ r\ell = r\ell$.

(iv) $\ell \circ \ell r = r \circ \ell r = \ell r \circ r = \ell(\ell \circ r) = \ell \circ (\ell \circ r) = r \circ (\ell \circ r) = \ell \circ r$.

In order to keep this exposition self-contained, we present some definitions very similar to those in [14]. Let $\ell_1, \ell_2 \in \mathcal{L}(S)$. We define

$$\ell_2 \succeq \ell_1 \text{ if and only if } \ \ell_2x\ell_1 = x\ell_1 \ \text{ for all } x \in S.$$

Then, it follows that $1 \succeq \ell \succeq 0$ for $\ell \in \mathcal{L}(S)$. Since $\ell_2 x \ell_1 = \ell_2 \ell_1 x \ell_1$, it follows that, if $\ell_2 \ell_1 = \ell_1$, then $\ell_2 \succeq \ell_1$. On the other hand, if $\ell_2 \succeq \ell_1$, then $\ell_2 \ell_1 = \ell_1$. Hence,

$$\ell_2 \succeq \ell_1 \iff \ell_2 \ell_1 = \ell_1. \tag{4}$$

Let $\ell_0, \ell_1, \ell_2 \in \mathcal{L}(S)$ and $\ell_2 \succeq \ell_1$. From (4), we have $\ell_2 \ell_0 \ell_1 \ell_0 = \ell_2 \ell_1 \ell_0 = \ell_1 \ell_0$. Thus, $\ell_2 \succeq \ell_1 \Rightarrow \ell_2 \ell_0 \succeq \ell_1 \ell_0$. Similarly, for $r_1, r_2 \in \mathcal{R}(S)$, we define

$$r_2 \succeq r_1 \text{ if and only if } \ r_1 x r_2 = r_1 x \ \text{ for all } x \in S.$$

It immediately follows that $1 \succeq r \succeq 0$ for $r \in \mathcal{R}(S)$. Since $r_1 x r_2 = r_1 x r_1 r_2$, it follows that $r_1 r_2 = r_1$, which implies that $r_2 \succeq r_1$. Conversely, if $r_2 \succeq r_1$, we obtain $r_1 r_2 = r_1$. Consequently,

$$r_2 \succeq r_1 \iff r_1 r_2 = r_1. \tag{5}$$

Let $r_0, r_1, r_2 \in \mathcal{L}(S)$ and $r_2 \succeq r_1$. From (5), it follows that $r_0 r_1 r_0 r_2 = r_0 r_1 r_2 = r_0 r_1$, which implies $r_2 \succeq r_1 \Rightarrow r_0 r_2 \succeq r_0 r_1$.

We define an equivalence relation on $\mathcal{L}(R)$ as follows. From the definition, we have the following:

(i) $\ell_1 \succeq \ell_1$ for an arbitrary $\ell_1 \in \mathcal{L}(R)$;

(ii) $\ell_2 \succeq \ell_1$ and $\ell_3 \succeq \ell_2$ implies that $\ell_3 \succeq \ell_1$.

Then, we state that $\ell_1 \sim_{\text{left}} \ell_2$ if and only if $\ell_1 \succeq \ell_2$ and $\ell_2 \succeq \ell_1$. Thus, $\sim_{\text{left}}$ is an equivalence relation on $\mathcal{L}(R)$.

The definition of an equivalence relation on $\mathcal{R}(R)$ is similar. We have the following:

(i) $r_1 \succeq r_1$ for an arbitrary $r_1 \in \mathcal{R}(R)$.

(ii) $r_2 \succeq r_1$ and $r_3 \succeq r_2$ implies that $r_3 \succeq r_1$.

If we define $r_1 \sim_{\text{right}} r_2$ if and only if $r_1 \succeq r_2$ and $r_2 \succeq r_1$, it follows that $\sim_{\text{right}}$ is an equivalence relation on $\mathcal{R}(R)$.

Let $e \in S$ be an idempotent. Since the additively idempotent semiring S is partially ordered ($a + b = a \iff a \geq b$), we can consider two cases:

Case 1. Let $e \leq 1$. Then, e is called left (*resp.*, right) if $ex \geq xe$ (*resp.*, $xe \geq ex$) for an arbitrary $x \in S$ (see D. Vladeva [23]). If e is a left idempotent, it follows that $exe \geq xe$. But, from $e \leq 1$, we have $exe \leq xe$. Thus, $exe = xe$, i.e., e is a left semicentral idempotent. Similarly, if e is a right idempotent, we obtain that it is a right semicentral idempotent.

Note that if e is a left or a right semicentral idempotent, then $ex + xe \geq exe$.

Case 2. Let $e \geq 1$. If e is a left (*resp.*, right) idempotent, it follows that $exe \geq ex \geq xe$ (*resp.*, $exe \geq xe \geq ex$). Therefore, $exe \geq ex + xe$.

The underlying idea of the last inequality is to construct a new specific class of idempotents. An idempotent, $\jmath \in S$, is called Jordan semicentral if we have the following:

(a) $\jmath \geq 1$;

(b) $\jmath x \jmath = \jmath \circ x = \jmath x + x\jmath$ for an arbitrary $x \in S$.

In order to find examples of such idempotents, we consider $1 + e$, where e is an idempotent of S. Since $1 + e$ is an idempotent, it follows that $1 + \ell$ and $1 + r$, where $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$ are idempotents.

We obtain $(1 + \ell)x(1 + \ell) = x + \ell x + x\ell + \ell x \ell = x + \ell x + x\ell = (1 + \ell)x + x(1 + \ell)$ for any $x \in S$ and $\ell \in \mathcal{L}(S)$. Similarly, $(1 + r)x(1 + r) = (1 + r)x + x(1 + r)$ for any $x \in S$ and $r \in \mathcal{R}(S)$. Moreover, if e is an arbitrary idempotent of S, then $1 + e$ is a Jordan semicentral idempotent. Thus, we have enough examples for Jordan semicentral idempotents.

As in ring theory, the idempotent c from the centre of the semiring S is called a central idempotent. If we denote by $(\mathcal{C}(S), .)$ the semigroup of central idempotents, then

$\mathcal{C}(S) = \mathcal{L}(S) \cap \mathcal{R}(S)$. On the other hand, if we denote by $\mathcal{J}(S)$ the set of Jordan semicentral idempotents, it follows that if $c \in \mathcal{C}(S)$ and $c \geq 1$, then $c \in \mathcal{J}(S)$.

Proposition 4. *Let $\jmath \in \mathcal{J}(S)$. If $c \in \mathcal{C}(S)$, then $\jmath c \in \mathcal{J}(S)$.*

Proof. From $\jmath x\jmath = \jmath x + x\jmath$ for all $x \in S$, it follows that $\jmath cx\jmath c = (\jmath cx\jmath)c = (\jmath cx + cx\jmath)c = \jmath cx + x\jmath c$. □

Proposition 5. *Let $\ell \in \mathcal{L}(S)$, $r \in \mathcal{R}(S)$ and $\jmath, \jmath_1 \in \mathcal{J}(S)$. Then, we have the following:*
(1) $(\jmath\ell)^2 = \jmath\ell$; (2) $(\ell\jmath)^2 = \ell \circ \jmath$; (3) $(r\jmath)^2 = r\jmath$; (4) $(\jmath r)^2 = r \circ \jmath$;
(5) $(\jmath \circ \ell)^2 = \jmath \circ \ell$; (6) $(\jmath \circ r)^2 = \jmath \circ r$; (7) $(r\jmath\ell)^2 = r\jmath\ell$;
(8) $(\jmath \circ \ell r)^2 = (\jmath \circ r\ell)^2 = (\jmath \circ r)(\jmath \circ \ell)$;
(9) $((\ell \circ \jmath) \circ r)(\ell \circ (\jmath \circ r)) = (\jmath \circ r)(\jmath \circ \ell)$;
(10) $(\jmath \circ \jmath_1)^2 = \jmath \circ \jmath_1$.

Proof. The proof is routine from these definitions. □

Proposition 6. *Let e_1 and e_2 be idempotents of S. Then, $e_1 + e_2 + e_1 \circ e_2$ is an idempotent in the following cases:*
(a) $e_1e_2 = 0$; (b) $e_1, e_2 \in \mathcal{L}(S)$; (c) $e_1, e_2 \in \mathcal{R}(S)$; (d) $e_1, e_2 \in \mathcal{J}(S)$;
(e) $e_1 \in \mathcal{L}(S), e_2 \in \mathcal{R}(S)$; (f) $e_1 \in \mathcal{L}(S), e_2 \in \mathcal{J}(S)$; (g) $e_1 \in \mathcal{R}(S), e_2 \in \mathcal{J}(S)$.

Proof. The proof is routine from these definitions. □

Proposition 7. *If $\jmath, \jmath_1 \in \mathcal{J}(S)$, then $(\jmath\jmath_1)^2 = (\jmath_1\jmath)^2$.*

Proof. We obtain $(\jmath\jmath_1)^2 = \jmath\jmath_1\jmath\jmath_1 = \jmath(\jmath_1\jmath + \jmath\jmath_1) = \jmath\jmath_1\jmath + \jmath\jmath_1 = \jmath\jmath_1 + \jmath_1\jmath = \jmath \circ \jmath_1$. Since $(\jmath_1\jmath)^2 = \jmath_1 \circ \jmath$, the result follows. □

Let $\jmath, \jmath_1 \in \mathcal{J}(S)$. We write $\jmath \succeq \jmath_1$ if $\jmath x\jmath_1 = \jmath x + x\jmath_1$ for an arbitrary $x \in S$. Thus, when $\jmath \succeq \jmath_1$, we have $\jmath\jmath_1 = \jmath + \jmath_1$ and then $\jmath$ and $\jmath_1$ commute.

We now define $\jmath \sim \jmath_1$ if $\jmath \succeq \jmath_1$ and $\jmath_1 \succeq \jmath$. Note that for Jordan semicentral idempotents, the relation "$\succeq$" is not transitive and the relation "$\sim$" is not an equivalence relation.

From $\jmath \geq 1$, it follows that $\jmath \succeq 1$ and $1 \succeq \jmath$; thus, $\jmath \sim 1$ for any $\jmath \in \mathcal{J}(S)$.

It is easy to see that if $\jmath_1 = 1 + \ell_1$, $\jmath_2 = 1 + \ell_2$, and $\ell_1 \succeq \ell_2$, then $\jmath_1 \succeq \jmath_2$, where $\ell_1, \ell_2 \in \mathcal{L}(S)$. Similarly, if $\jmath_1 = 1 + r_1$, $\jmath_2 = 1 + r_2$ and $r_2 \succeq r_1$, then $\jmath_1 \succeq \jmath_2$, where $r_1, r_2 \in \mathcal{R}(S)$.

Therefore, if $\ell_1 \sim_{\text{left}} \ell_2$ for $\jmath_1 = 1 + \ell_1$ and $\jmath_2 = 1 + \ell_2$, it follows that $\jmath_1 \sim \jmath_2$ and, similarly, if $r_1 \sim_{\text{right}} r_2$, then $\jmath_1 = 1 + r_1$ and $\jmath_2 = 1 + r_2$ implies $\jmath_1 \sim \jmath_2$.

For a fixed $\jmath \in \mathcal{J}(S)$, we consider the set $\mathcal{J}_\jmath = \{\jmath_1 | \jmath_1 \sim \jmath\}$.

Proposition 8. *For any $\jmath \in \mathcal{J}(S)$, the set $\mathcal{J}_\jmath$ is a commutative semigroup.*

Proof. Let $\jmath, \jmath_1 \in \mathcal{J}(S)$ and $\jmath \sim \jmath_1$. Then, for an arbitrary $x \in S$

$$(\jmath + \jmath_1)x(\jmath + \jmath_1) = \jmath x\jmath + \jmath x\jmath_1 + \jmath_1 x\jmath + \jmath_1 x\jmath_1 =$$

$$= \jmath x\jmath + \jmath x + x\jmath_1 + \jmath_1 x + x\jmath + \jmath_1 x\jmath_1 = \jmath x\jmath + \jmath_1 x\jmath_1 = (\jmath + \jmath_1)x + x(\jmath + \jmath_1).$$

Hence, $\jmath\jmath_1 x\jmath\jmath_1 = \jmath\jmath_1 x + x\jmath\jmath_1$. □

Remark 2. *In the next section, we give examples of left semicentral idempotent triangular matrices, ℓ_1 and ℓ_2, such that $\ell_1 \sim_{left} \ell_2$ and there is similar for right and Jordan semicentral idempotent triangular matrices.*

Now, let e_1 and e_2 be arbitrary idempotents of S. It is straightforward to prove the following.

Proposition 9. *If $e_1 \leq 1$, then $e_1 + e_2$ is an idempotent.*

Similarly, it follows that $\sum_{i=1}^{n} e_i$ is an idempotent if $e_1, \ldots, e_n$ are idempotents such that $e_i \leq 1$ for $i = 1, \ldots, n-1$.

Proposition 10. *Let e be an idempotent of the semiring S, with $\ell \in \mathcal{L}(S)$, $r \in \mathcal{R}(S)$, and $\jmath \in \mathcal{J}(S)$. Then, $e\ell e \in \mathcal{L}(eSe)$, $ere \in \mathcal{R}(eSe)$, and $e\jmath e \in \mathcal{J}(eSe)$.*

Proof. The proof is routine from these definitions. □

Let e be a fixed idempotent of the semiring S. We include some basic results related to idempotents of the semiring eS.

(i) $e\ell$ is a left semicentral idempotent of eS for any $\ell \in \mathcal{L}(S)$.

(ii) Since $(er)^2 = ere$ for any $r \in \mathcal{R}(S)$, from Proposition 10, it follows that er is a square root of an idempotent.

(iii) $(er)(e\ell)$ is an idempotent where $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$. Moreover, $e\ell r$ and $er\ell$ are square roots of $(er)(e\ell)$. Similarly, $(er)(e\ell e)$ is an idempotent.

(iv) Since $((e\ell)(ere))^2 = (er)(e\ell e)$, we have that $(e\ell)(ere)$ is a root of an idempotent.

(v) $(e\jmath)(e\ell)$ is an idempotent where $\ell \in \mathcal{L}(S)$ and $\jmath \in \mathcal{J}(S)$. Similarly, $(e\jmath)(e\ell e)$ is an idempotent.

(vi) $(er)(e\jmath e)$ is an idempotent where $r \in \mathcal{R}(S)$ and $\jmath \in \mathcal{J}(S)$.

(vii) $(er)(e\jmath)(e\ell)$ is an idempotent where $\ell \in \mathcal{L}(S)$, $r \in \mathcal{R}(S)$, and $\jmath \in \mathcal{J}(S)$.

(viii) $(e\jmath)^2 = e\jmath e + e\jmath$ and $e\jmath e + e\jmath$ are idempotents where $\jmath \in \mathcal{J}(S)$. Consequently, $(e\jmath)^4 = (e\jmath)^2$.

Now, we describe the dual results related to idempotents of the semiring Se:

(i) re is a right semicentral idempotent of Se for any $r \in \mathcal{R}(S)$.

(ii) Since $(\ell e)^2 = e\ell e$ for any $\ell \in \mathcal{L}(S)$, from Proposition 10, it follows that ℓe is a root of an idempotent.

(iii) $(re)(\ell e)$ is an idempotent where $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$. Moreover, $r\ell e$ and ℓre are square roots of $(re)(\ell e)$. Similarly, $(ere)(\ell e)$ is an idempotent.

(iv) Since $((\ell e)(ere))^2 = (ere)(\ell e)$, we have that $(\ell e)(ere)$ is a root of an idempotent.

(v) $(re)(\jmath e)$ is an idempotent where $r \in \mathcal{R}(S)$ and $\jmath \in \mathcal{J}(S)$. Similarly, $(ere)(\jmath e)$ is an idempotent.

(vi) $(e\jmath e)(\ell e)$ is an idempotent where $\ell \in \mathcal{L}(S)$ and $\jmath \in \mathcal{J}(S)$.

(vii) $(re)(\jmath e)(\ell e)$ is an idempotent where $\ell \in \mathcal{L}(S)$, $r \in \mathcal{R}(S)$, and $\jmath \in \mathcal{J}(S)$.

(viii) $(\jmath e)^2 = \jmath e + e\jmath e$ and $\jmath e + e\jmath e$ are idempotents where $\jmath \in \mathcal{J}(S)$. Consequently, $(\jmath e)^4 = (\jmath e)^2$.

Let e_1 and e_2 be idempotents of S and $e_2 e_1 = 0$. Note that, by Proposition 6a, it follows that $e_1 + e_2 + e_1 e_2$ is an idempotent.

We denote $e_1 \diamond e_2 = e_1 + e_2 + e_1 e_2$. (The reader can obtain the same construction in ring theory, related to non-unital rings, in [24].)

The next proposition motivates the results in APPLICATION A.

Proposition 11. *Let e be an idempotent of the semiring S, with $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$. If $r\ell = 0$, then (a) $\ell \diamond r$ and (b) $e\ell \diamond re$ is an idempotent of S.*

Proof. Part (a) follows immediately from Proposition 6 (a). Since $(re)(el) = re\ell = r\ell e\ell = 0$, (b) holds. □

Remark 3. *In the next section, we will show natural examples of a left semicentral idempotent, ℓ, and a right semicentral idempotent, r, such that $r\ell = 0$. So, it will be interesting to describe the semiring closure (the minimal subsemiring of S) generated by the fixed ℓ and r. The semiring closure consists of the nilpotent ℓr, since $(\ell r)^2 = r\ell = 0$, the square root $\ell + r$, since $(\ell + r)^2 = \ell + r + \ell r$, and five idempotents: ℓ, r, $\ell + \ell r$, $r + \ell r$, and $\ell + r + \ell r$.*

Using a left semicentral idempotent, ℓ, and a right semicentral idempotent, r, such that $r\ell = 0$, we can construct a new Jordan semicentral idempotent.

Proposition 12. *If $\ell \in \mathcal{L}(S)$, $r \in \mathcal{R}(S)$, and $rl = 0$, then it follows that $\jmath = 1 + \ell r$ is a Jordan semicentral idempotent.*

Proof. We obtain $(1 + \ell r)x(1 + \ell r) = x + \ell rx + x\ell r + \ell rx\ell r = (1 + \ell r)x + x(1 + \ell r) + rx\ell$, where $x \in S$. Since $rx\ell = rxr\ell = 0$, we have that $\jmath x\jmath = \jmath x + x\jmath$. □

Proposition 13. *If $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$, then for the Jordan semicentral idempotents $\jmath_\ell = 1 + \ell$ and $\jmath_r = 1 + r$, it follows that $\jmath_\ell \diamond \jmath_r = 1 + \ell \diamond r$.*

Proof. It is easy to check that $1 + e$ is an idempotent for any idempotent e of S. We know that $\jmath_\ell = 1 + \ell$ and $\jmath_r = 1 + r$ are Jordan semicentral idempotents.

Consequently, $\jmath_\ell \diamond \jmath_r = (1 + \ell) \diamond (1 + r) = 1 + \ell + r + \ell r = 1 + \ell \diamond r$. □

We can extend the last result as follows.

Proposition 14. *Let $e \leq 1$ be an idempotent of S, with $\ell \in \mathcal{L}(S)$ and $r \in \mathcal{R}(S)$. Then, it follows that $\jmath_1 = 1 + e\ell$ and $\jmath_2 = 1 + re$ are Jordan semicentral idempotents and $\jmath_1 \diamond \jmath_2 = 1 + e\ell \diamond re$.*

Proof. As in the proof of Proposition 13, we obtain that $(1 + e\ell) \diamond (1 + re) = 1 + e\ell \diamond re$. When $e \leq 1$ for an arbitrary $x \in S$, it follows that $\jmath_1 x \jmath_1 = (1 + e\ell)x(1 + e\ell) = x + e\ell x + xe\ell + e\ell xe\ell = (1 + e\ell)x + x(1 + e\ell) = \jmath_1 x + x\jmath_1$. Similarly, we observe that $\jmath_2 = 1 + re$ is a Jordan semicentral idempotent. □

4. Results on Semicentral Idempotents of Triangular Matrix Semiring

For the proofs of the following two important theorems, we need another lemma (similar to Proposition 3.1 of [14] for trangular matrices over a ring).

Lemma 1. *Let $X = (x_{ij}) \in T_n(S)$ be an arbitrary matrix. If $P = (\pi_{ij}) \in T_n(S)$ is a left (resp., right or Jordan) semicentral idempotent of $T_n(S)$, then π_{ii}, $i = 1, \ldots, n$, are left (resp., right or Jordan) semicentral idempotents of S.*

Proof. We obtain the diagonal entries of the following matrices:

$x_{ii}\pi_{ii}$ of the matrix XP;
$\pi_{ii}x_{ii}$ of the matrix PX;
$\pi_{ii}x_{ii} + x_{ii}\pi_{ii}$ of the matrix $PX + XP$;
$\pi_{ii}x_{ii}\pi_{ii}$ of the matrix PXP for $i = 1, \ldots, n$.

Now, if P is a left semicentral idempotent of $T_n(S)$, we have $\pi_{ii}x_{ii}\pi_{ii} = x_{ii}\pi_{ii}$; if P is a right semicentral idempotent of $T_n(S)$, we obtain $\pi_{ii}x_{ii}\pi_{ii} = \pi_{ii}x_{ii}$; and if P is a Jordan semicentral idempotent of $T_n(S)$, then $\pi_{ii}x_{ii}\pi_{ii} = \pi_{ii}x_{ii} + x_{ii}\pi_{ii}$. Thus, the result follows. □

Theorem 5. *Each left semicentral idempotent triangular $n \times n$ matrix over an additively idempotent semiring, S, without zero divisors is of the form $\ell_k = \begin{pmatrix} \Lambda_k & \Lambda_k A \\ 0 & 0 \end{pmatrix}$, where $\Lambda_k = \operatorname{diag}(\lambda_1, \ldots, \lambda_k)$, $\lambda_i \in \mathcal{L}(S)$, for $i = 1, \ldots, k$, $\lambda_{i-1} \succeq \lambda_i$, $i = 2, \ldots k$, and $A = (\alpha_{ij}) \in M_{k\times(n-k)}$ for $k = 1, \ldots, n-1$, or is of the form $\ell_n = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, where $\lambda_i \in \mathcal{L}(S)$ for $i = 1, \ldots n$ and $\lambda_{i-1} \succeq \lambda_i$ for $i = 2, \ldots, n$.*

Proof. From Lemma 1, it follows that diagonal entries of the left semicentral idempotent matrix Λ are left semicentral idempotents of S. Thus, from the notations in (2) and from (3), it follows that

$$\Lambda = \begin{pmatrix} \lambda_1 & \delta_{12} & \cdots & \delta_{1k} + \sum_1^k * & \cdots & \delta_{1n} + \sum_1^n * \\ 0 & \lambda_2 & \cdots & \delta_{2k} + \sum_2^k * & \cdots & \delta_{2n} + \sum_2^n * \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \lambda_k & \cdots & \delta_{kn} + \sum_k^n * \\ \vdots & \vdots & \cdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & \lambda_n \end{pmatrix},$$

where $\lambda_i \in \mathcal{L}(S)$ for $i = 1, \ldots n$, is a left semicentral idempotent matrix. Note that $\delta_{im} + \sum_i^m *$, $1 \le i \le k < m \le n$ is just the (i, m)-entry of the matrix from (3) for $e_i = \lambda_i$. Since $\Lambda X \Lambda = X\Lambda$ for every triangular matrix, X, we can choose $X = e_{k-1\,k}$, where $e_{k-1\,k}$ is a matrix unit for $1 < k \le n$.

Then, we obtain $X\Lambda = \lambda_k e_{k-1\,k} + \delta_{k\,k+1} e_{k-1\,k+1} + \cdots + (\delta_{kn} + \sum_k^n *) e_{k-1\,n}$ and

$$\Lambda X \Lambda = \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\lambda_k e_{1k} + \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\delta_{k\,k+1} e_{1\,k+1} +$$

$$+ \cdots + \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\left(\delta_{kn} + \sum_k^n *\right) e_{1n} + \cdots +$$

$$+ \delta_{k-2\,k-1}\lambda_k e_{k-2\,k} + \delta_{k-2\,k-1}\delta_{k\,k+1} e_{k-2\,k+1} + \cdots + \delta_{k-2\,k-1}\left(\delta_{kn} + \sum_k^n *\right) e_{k-2\,n} +$$

$$+ \lambda_{k-1}\lambda_k e_{k-1\,k} + \lambda_{k-1}\delta_{k\,k+1} e_{k-1\,k+1} + \cdots + \lambda_{k-1}\left(\delta_{kn} + \sum_k^n *\right) e_{k-1\,n}.$$

Comparing the corresponding elements, we find $\lambda_{k-1}\lambda_k = \lambda_k$ which is $\lambda_{k-1} \succeq \lambda_k$. Therefore, $\lambda_1 \succeq \lambda_2 \succeq \cdots \succeq \lambda_n$.

As a consequence, we have that $\lambda_{k-1}\delta_{k\,k+1} = \delta_{k\,k+1}, \ldots, \lambda_{k-1}(\delta_{kn} + \sum_k^n *) = \delta_{kn} + \sum_k^n *$ are identities for every $k = 2, \ldots, n-1$. Since $\lambda_i \succeq \lambda_j$ for $i < j$, it follows that $\delta_{ij} = \lambda_i\alpha_{ij} + \lambda_i\alpha_{ij}\lambda_j + \alpha_{ij}\lambda_j = \lambda_i\alpha_{ij} + \alpha_{ij}\lambda_j$. If $i < j < k$, we have $\delta_{ij}\lambda_k = (\lambda_i\alpha_{ij} + \alpha_{ij}\lambda_j)\lambda_k = \alpha_{ij}\lambda_k$. From $\left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\lambda_k = 0$, it follows that $\delta_{1\,k-1}\lambda_k = 0$ (since an additively idempotent semiring $a + b = 0$ implies that $a = 0$) and then $\alpha_{1\,k-1}\lambda_k = 0$, where $k \ge 3$. Similarly, from $\left(\delta_{2\,k-1} + \sum_2^{k-1} *\right)\lambda_k = 0$, we find $\alpha_{2\,k-1}\lambda_k = 0$ where $k \ge 4$.

Thus, using $\lambda_1 \succeq \cdots \succeq \lambda_k$, we obtain $\alpha_{ij}\lambda_k = 0$ for $1 \le i < j < k \le n$.

Now, we choose matrix $X = e_{kk}$. Then, $X\Lambda = \lambda_k e_{kk} + \delta_{k\,k+1} e_{k\,k+1} + \cdots + (\delta_{kn} + \sum_k^n *) e_{k\,n}$. Next, we obtain $\Lambda X \Lambda = \left(\delta_{1k} + \sum_1^k *\right)\lambda_k e_{1k} + \left(\delta_{1k} + \sum_1^k *\right)\delta_{k\,k+1} e_{1\,k+1} +$

$$+ \cdots + \left(\delta_{1k} + \sum_1^k *\right)\left(\delta_{kn} + \sum_k^n *\right) e_{1n} + \cdots +$$

$$+ \delta_{k-1\,k}\lambda_k e_{k-1\,k} + \delta_{k-1\,k}\delta_{k\,k+1} e_{k-1\,k+1} + \cdots + \delta_{k-1\,k}\left(\delta_{kn} + \sum_k^n *\right) e_{k-1\,n} +$$

$$+ \lambda_k e_{kk} + \lambda_k \delta_{k\,k+1} e_{k\,k+1} + \cdots + \lambda_k \left(\delta_{kn} + \sum_k^n *\right) e_{kn}.$$

We compare the corresponding elements and find that $\delta_{1k}\lambda_k = 0$ which implies that $\alpha_{1k}\lambda_k = 0$. Similarly, we obtain $\alpha_{2k}\lambda_k = 0, \ldots, \alpha_{k-1\,k}\lambda_k = 0$.

Hence, $\alpha_{ij}\lambda_k = 0$ for $1 \leq i < j \leq k \leq n$. As a consequence, if $k = n$ and $\lambda_n \neq 0$, since there are no zero divisors in S, it follows that all $\alpha_{ij} = 0$ where $1 \leq i < j \leq n$. Thus, $\Lambda = \ell_n = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, where $\lambda_1 \succeq \lambda_2 \succeq \cdots \succeq \lambda_n$.

Now, assume that k is the largest number such that $\lambda_k \neq 0$. Then, all $\alpha_{ij} = 0$ where $1 \leq i < j \leq k$. Since $\lambda_{k+1} = \cdots = \lambda_n = 0$, it follows that the nonzero entries of the matrix Λ are $\lambda_1, \ldots, \lambda_k$ and, generally, the entries of the $k \times (n-k)$ matrix on the right upper corner of Λ. These entries are $\delta_{ij} + \sum_i^j *$ for $i = 1, \ldots, k$ and $j = k+1, \ldots, n$. From $\alpha_{ij} = 0$, for $1 \leq i < j \leq k$, it follows that $\sum_i^j * = 0$. So, the enties of the matrix are $\delta_{ij} = \lambda_i \alpha_{ij} + \alpha_{ij}\lambda_j = \lambda_i \alpha_{ij}$, where $i = 1, \ldots, k$, $j = k+1, \ldots, n$. Hence, $\Lambda = \ell_k$.

Conversely, it is easily checked that the matrix ℓ_k is a left semicentral idempotent. Let $X \in M_{k\times k}$, $Y \in M_{k\times(n-k)}$, and $Z \in M_{(n-k)\times(n-k)}$. Then, $\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}\ell_k = \begin{pmatrix} X\Lambda_k & X\Lambda_k A \\ 0 & 0 \end{pmatrix}$ and $\ell_k \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}\ell_k = \begin{pmatrix} \Lambda_k X \Lambda_k & \Lambda_k X \Lambda_k A \\ 0 & 0 \end{pmatrix}$.

Since the matrix Λ_k is a left semicentral idempotent of $T_k(S)$, it follows that ℓ_k is a left semicentral idempotent of $T_n(S)$, and the result follows. □

The number k, $1 \leq k \leq n$, in Theorem 5 is a type of the left semicentral idempotent ℓ_k. For a fixed k, the set of all left semicentral idempotent matrices of the type k is denoted by $\mathcal{L}_k$.

Remark 4. *Recall that $\mathcal{SP}(S)$ is the set of special idempotent matrices over the semiring S. From Theorem 5, it is easy to see that for an arbitrary number, k, $1 \leq k \leq n$, it follows that $\mathcal{SP}(S) \cap \mathcal{L}_k = 0$. Therefore, $\mathcal{SP}(S) \cap \mathcal{L}(T_n(S)) = 0$.*

Proposition 15. *The set $\mathcal{L}_k$ is a subsemigroup of $\mathcal{L}(T_n(S))$ with an identity.*

Proof. Let ℓ_k with the diagonal entries $\lambda_1, \ldots, \lambda_k \in \mathcal{L}(S)$ and ℓ'_k with the diagonal entries $\lambda'_1, \ldots, \lambda'_k \in \mathcal{L}(S)$ be left semicentral idempotents of the same type. It is easy to verify that

$$\ell_k \ell'_k = \begin{pmatrix} \lambda_1\lambda'_1 & \cdots & 0 & \lambda_1\lambda'_1\alpha_{1\,k+1} & \cdots & \lambda_1\lambda'_1\alpha_{1n} \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & \lambda_k\lambda'_k & \lambda_k\lambda'_k\alpha_{k\,k+1} & \cdots & \lambda_k\lambda'_k\alpha_{kn} \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Thus, for a fixed k, $1 \leq k \leq n$, the set $\mathcal{L}_k$ is a noncommutative semigroup. It is easy to verify that the identity element of $\mathcal{L}_k$ is the matrix $1_k^\ell = \begin{pmatrix} I_k & A \\ 0 & 0 \end{pmatrix}$, where $I_k = \sum_{i=1}^{k} e_{ii}$ and $A \in M_{k\times(n-k)}(S)$. $\square$

The matrix 1_k^ℓ is called a monic left semicentral idempotent of the type k.

In the papers [13,14], the author considered some properties of monic semicentral idempotents.

Note that $\ell_k = \ell_n 1_k^\ell$, where $\ell_n = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, for $1 \leq k \leq n-1$.

Remark 5. *Let $k, 1 \leq k \leq n-1$ be a fixed number and $A, B \in M_{k\times(n-k)}(S)$. The matrices $\ell_A = \begin{pmatrix} I_k & A \\ 0 & 0 \end{pmatrix}$ and $\ell_B = \begin{pmatrix} I_k & B \\ 0 & 0 \end{pmatrix}$ are monic left semicentral idempotent matrices. It is easy to see that $\ell_A \sim_{left} \ell_B$. Thus, 1_k^ℓ is an equivalence class under the relation $\sim_{left}$.*

For right semicentral idempotent triangular matrices, we prove a result quite similar to Theorem 5.

Theorem 6. *Each right semicentral idempotent triangular $n \times n$ matrix over an additively idempotent semiring, S, without zero divisors is of the form $r_k = \begin{pmatrix} 0 & A\mathfrak{R}_k \\ 0 & \mathfrak{R}_k \end{pmatrix}$, where $\mathfrak{R}_k = \operatorname{diag}(\rho_{n-k+1}, \ldots, \rho_n)$, $\rho_i \in \mathcal{R}(S)$, for $i = n-k+1, \ldots, n$, $\rho_{i+1} \succeq \rho_i$, $i = n-k+1, \ldots, n-1$, and $A = (\alpha_{ij}) \in M_{(n-k)\times k}$ for $k = 1, \ldots, n-1$, or is of the form $r_n = \operatorname{diag}(\rho_1, \ldots, \rho_n)$, where $\rho_i \in \mathcal{R}(S)$ for $i = 1, \ldots n$ and $\rho_{i+1} \succeq \rho_i$ for $i = 1, \ldots, n-1$.*

Proof. Again using Lemma 1, we obtain that diagonal entries of the right semicentral idempotent matrix $\mathfrak{R}$ are right semicentral idempotents of S. From the notations in (2) and from (3), it follows that

$$\mathfrak{R} = \begin{pmatrix} \rho_1 & \cdots & \delta_{1\,k-1} + \sum_1^{k-1} * & \delta_{1k} + \sum_1^k * & \cdots & \delta_{1n} + \sum_1^n * \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & \rho_{k-1} & \delta_{k-1\,k} & \cdots & \delta_{k-1\,n} + \sum_{k-1}^n * \\ 0 & \cdots & 0 & \rho_k & \cdots & \delta_{kn} + \sum_k^n * \\ \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \rho_n \end{pmatrix},$$

where $\rho_i \in \mathcal{R}(S)$, for $i = 1, \ldots n$, is a right semicentral idempotent matrix and $\delta_{im} + \sum_i^m *$, $1 \leq i \leq k < m \leq n$, is just the (i,m)-entry of the matrix from (3) for $e_i = \rho_i$.

Since $\mathfrak{R}X\mathfrak{R} = \mathfrak{R}X$ for every triangular matrix, X, we can choose $X = e_{k-1\,k}$, where $e_{k-1\,k}$ is a matrix unit for $1 < k \leq n$.

We obtain $\mathfrak{R}X = \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right) e_{1k} + \cdots + \rho_{k-1} e_{k-1\,k}$ and

$$\mathfrak{R}X\mathfrak{R} = \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\rho_k e_{1k} + \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\delta_{k\,k+1} e_{1\,k+1} +$$

$$+ \cdots + \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\left(\delta_{kn} + \sum_k^n *\right) e_{1n} + \cdots +$$

$$+ \rho_{k-1}\rho_k e_{k-1\,k} + \rho_{k-1}\delta_{k\,k+1} e_{k-1\,k+1} + \cdots + \rho_{k-1}\left(\delta_{kn} + \sum_k^n *\right) e_{k-1\,n}.$$

By comparing the coefficients of $e_{k-1\,k}$, we find $\rho_{k-1}\rho_k = \rho_{k-1}$ that is $\rho_k \succeq \rho_{k-1}$ (see (5)). Therefore, $\rho_n \succeq \rho_{n-1} \succeq \cdots \succeq \rho_1$.

Also, we have that

$$\left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\delta_{k\,k+1} = 0, \left(\delta_{1\,k-1} + \sum_1^{k-1} *\right)\left(\delta_{kn} + \sum_k^n *\right) = 0, \ldots,$$

$$\rho_{k-1}\delta_{k\,k+1} = 0, \ldots, \rho_{k-1}\left(\delta_{kn} + \sum_k^n *\right) = 0.$$

Since $\rho_j \succeq \rho_i$ for $i < j$, it follows that $\delta_{ij} = \rho_i\alpha_{ij} + \rho_i\alpha_{ij}\rho_j + \alpha_{ij}\rho_j = \rho_i\alpha_{ij} + \alpha_{ij}\rho_j$.

Then, if $p < i < j$, we have $\rho_p\delta_{ij} = \rho_p\alpha_{ij}$.

From $\rho_{k-1}(\delta_{kn} + \sum_k^n *) = 0$, it follows that $\rho_{k-1}\alpha_{ij} = 0$ for $1 \le k < i < j \le n$.

Now, for $X = e_{kk}$, we have $\mathfrak{R}X = \left(\delta_{1\,k} + \sum_1^k *\right)e_{1k} + \cdots + \delta_{k-1\,k}e_{k-1\,k} + \rho_k e_{kk}$ and then obtain

$$\mathfrak{R}X\mathfrak{R} = \left(\delta_{1k} + \sum_1^k *\right)\rho_k e_{1k} + \left(\delta_{1k} + \sum_1^k *\right)\delta_{k\,k+1}e_{1\,k+1} +$$

$$+ \cdots + \left(\delta_{1k} + \sum_1^k *\right)\left(\delta_{kn} + \sum_k^n *\right)e_{1n} + \cdots +$$

$$+\delta_{k-1\,k}\rho_k e_{k-1\,k} + \delta_{k-1\,k}\delta_{k\,k+1}e_{k-1\,k+1} + \cdots + \delta_{k-1\,k}\left(\delta_{kn} + \sum_k^n *\right)e_{k-1\,n} +$$

$$+\rho_k e_{kk} + \rho_k\delta_{k\,k+1}e_{k\,k+1} + \cdots + \rho_k\left(\delta_{kn} + \sum_k^n *\right)e_{kn}.$$

It is easy to see that $\left(\delta_{1k} + \sum_1^k *\right)\rho_k = \delta_{1k} + \sum_1^k *, \ldots, \delta_{k-1\,k}\rho_k = \delta_{k-1\,k}$ are identities. It follows that

$$\left(\delta_{1k} + \sum_1^k *\right)\delta_{k\,k+1} = 0, \ldots, \left(\delta_{1k} + \sum_1^k *\right)\left(\delta_{kn} + \sum_k^n *\right) = 0, \ldots, \delta_{k-1\,k}\delta_{k\,k+1} = 0,$$

$$\ldots, \delta_{k-1\,k}\left(\delta_{kn} + \sum_k^n *\right) = 0, \ldots, \rho_k\delta_{k\,k+1} = 0, \ldots, \rho_k\left(\delta_{kn} + \sum_k^n *\right) = 0.$$

Now, $\rho_k\delta_{k\,k+1} = 0$ implies that $\rho_k\alpha_{k\,k+1} = 0$ for all $1 \le k \le n-1$. Thus, if $\rho_1 \neq 0$, we have $\alpha_{12} = 0$, and from $\rho_1\alpha_{ij} = 0$, $1 < i < j \le n-1$, we obtain that $\rho_1\alpha_{ij} = 0$ for all $i < j$. Therefore, $\mathfrak{R} = r_n = \mathrm{diag}(\rho_1, \ldots, \rho_n)$.

Let $\rho_1 = \cdots = \rho_{n-k} = 0$ and $\rho_{n-k+1} \neq 0$. As shown above, it follows that $\alpha_{ij} = 0$ for all $n-k+1 \le i < j \le n$.

Since $\delta_{ij} = 0$ for $1 \le i < j \le n-k$ and also for $n-k+1 \le i < j \le n$, it follows that the (i,j)-entries, where $1 \le i \le n-k$ and $n-k+1 \le j \le n$, of the matrix are equal: $\delta_{ij} = \alpha_{ij}\rho_j$. Hence, $\mathfrak{R} = r_k$.

Conversely, by the same reasoning as in the proof of Theorem 5, we check that r_k is a right semicentral idempotent matrix, and the proof is completed. □

The number k, $1 \le k \le n$, in Theorem 6 is called a type of the right semicentral idempotent r_k. For a fixed k, the set of all right semicentral idempotent matrices of the type k is denoted by $\mathcal{R}_k$.

As in Remark 3, it follows that $\mathcal{SP}(S) \cap \mathcal{R}(T_n(S)) = 0$.

Proposition 16. *The set $\mathcal{R}_k$ is a subsemigroup of $\mathcal{R}(T_n(S))$ with an identity.*

Proof. The proof is similar to that of Proposition 15. □

The identity element of $\mathcal{R}_k$ is the matrix $1_k^r = \begin{pmatrix} 0 & A \\ 0 & I_{n-k+1} \end{pmatrix}$, where $I_{n-k+1} = \sum_{i=n-k+1}^{n} e_{ii}$ and $A \in M_{(n-k)\times k}(S)$. This matrix is called a monic right semicentral idempotent of the type k. In a similar way to in Remark 5, it follows that 1_k^r is an equivalence class under the relation $\sim_{\text{right}}$.

Remark 6. *In spite of some evident similarities with semicentral idempotent matrices over a ring, there is a significant difference. All non-diagonal left and right semicentral idempotent matrices over an additively idempotent semiring are singular.*

Further, we construct the matrix $1_{\ell_k}^J = I + 1_k^\ell = \begin{pmatrix} I_k & A \\ 0 & I_{n-k} \end{pmatrix}$ with only ones on the main diagonal and an arbitrary matrix, $A \in M_{k\times(n-k)}$, in the right upper corner. Then, it follows that $1_{\ell_k}^J$ is a Jordan semicentral idempotent for $k = 1, \ldots, n-1$ (see Section 3). Similarly, the matrix $1_{r_m}^J = I + 1_m^r = \begin{pmatrix} I_{n-m} & A \\ 0 & I_m \end{pmatrix}$ is a Jordan semicentral idempotent for $m = 1, \ldots, n-1$. Then, $1_{r_{n-k}}^J = 1_{\ell_k}^J$. These semicentral idempotents are called monic Jordan semicentral idempotent matrices.

Remark 7. *(i) Assume that k, where $1 \le k \le n-1$ is a fixed integer and $A, B \in M_{k\times(n-k)}(S)$. Now, the matrices $\jmath_A = \begin{pmatrix} I_k & A \\ 0 & I_{n-k} \end{pmatrix}$ and $\jmath_B = \begin{pmatrix} I_k & B \\ 0 & I_{n-k} \end{pmatrix}$ are monic Jordan semicentral idempotent matrices.*

Let $X \in M_{k\times k}$, $Y \in M_{k\times(n-k)}$ and $Z \in M_{(n-k)\times(n-k)}$.

We obtain $\jmath_A \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} = \begin{pmatrix} X & Y+AZ \\ 0 & Z \end{pmatrix}$ and $\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \jmath_B = \begin{pmatrix} X & XB+Y \\ 0 & Z \end{pmatrix}$ and then $\jmath_A \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} + \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \jmath_B = \begin{pmatrix} X & XB+Y+AZ \\ 0 & Z \end{pmatrix} = \jmath_A \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \jmath_B$. Therefore, $\jmath_A \sim \jmath_B$.

(ii) There are no monic Jordan semicentral idempotent matrices that are special idempotent matrices.

The next result shows that there are other Jordan semicentral idempotents.

Proposition 17. *If $\jmath_i \in \mathcal{J}(S)$, $i = 1, \ldots, n$ and $\jmath_i \succeq \jmath_k$ for $i < k$, the matrix $A = \operatorname{diag}(\jmath_1, \ldots, \jmath_n)$ is a Jordan semicentral idempotent.*

Proof. Let $X = (x_{ik}) \in T_n(S)$. Then, it follows that $AX = (\jmath_i x_{ik})$, $XA = (x_{ik}\jmath_k)$ and $AXA = (\jmath_i x_{ik}\jmath_k)$. Since $\jmath_i x_{ik}\jmath_k = \jmath_i x_{ik} + x_{ik}\jmath_k$ for any $i < k$, we have $AXA = AX + XA$. □

Remark 8. *The monic Jordan semicentral idempotent matrices and diagonal matrices considered in the last proposition are particular cases of the matrices $\begin{pmatrix} I_p & 0 & B \\ 0 & C & 0 \\ 0 & 0 & I_q \end{pmatrix}$, where $I_p = \sum_{i=1}^{p} e_{ii}$, $I_q = \sum_{i=n-q+1}^{n} e_{ii}$, $B \in M_{p\times q}(S)$, and $C = \operatorname{diag}(\jmath_{p+1}, \ldots, \jmath_{n-q})$, where $\jmath_i \in \mathcal{J}(S)$, $i = p+1, \ldots, n-q$, and $\jmath_i \succeq \jmath_k$ for $i < k$. When $p = q = 0$, the matrix is diagonal, and when $n = p+q$, all the diagonal entries of the matrix are ones. The proof of this fact is routine.*

In the next example, we describe idempotents of certain triangular matrix semirings.

Example 3. *Let $\mathbb{B} = (\{0,1\}, +, .)$ be a Boolean semiring. We present all idempotents as well as left (right and Jordan) semicentral idempotents, roots of idempotent matrices, and nilpotent matrices in the semiring $T_n(\mathbb{B})$ for $n = 2$ and $n = 3$.*

The matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ are left semicentral idempotents, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ are right semicentral idempotent matrices, and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is a Jordan semicentral idempotent matrix. The matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent. The identity matrix and the zero matrix can be considered a Jordan semicentral idempotent and nilpotent matrix, respectively.

Let $\varepsilon_{ij} = 1$ or $\varepsilon_{ij} = 0$ for $i, j = 1, \ldots, n$, with $i < j$. Then, every matrix of $T_n(\mathbb{B})$ has the form (ε_{ij}). For $n = 3$, it is easy to verify that the matrices $\ell_1 = e_{11} + \varepsilon_{12}e_{12} + \varepsilon_{13}e_{13}$ and $\ell_2 = \ell_1 + e_{22} + \varepsilon_{23}e_{23}$ are left semicentral idempotents. Therefore, we obtain 12 left semicentral idempotent matrices.

Similarly, the right semicentral idempotents are $r_1 = e_{33} + \varepsilon_{23}e_{23} + \varepsilon_{13}e_{13}$ and $r_2 = r_1 + e_{22} + \varepsilon_{12}e_{12}$. The Jordan semicentral idempotents are $\jmath = I + \ell_2 = I + \varepsilon_{12}e_{12} + \varepsilon_{13}e_{13} + \varepsilon_{23}e_{23}$. Thus, we obtain 32 semicentral idempotent matrices.

From Proposition 3, we find that $r_2\ell_2 = e_{22} + \varepsilon_{12}e_{12} + \varepsilon_{13}e_{13} + \varepsilon_{23}e_{23}$ are idempotents. Since $\ell_1 r_1 \leq r_1$, from Proposition 3 again, we obtain that $\ell_1 \circ r_1 = e_{11} + \varepsilon_{12}e_{12} + \varepsilon_{13}e_{13} + \varepsilon_{23}e_{23} + e_{33}$ are idempotent matrices. Therefore, we find 16 idempotent matrices that are not semicentral idempotents.

It is easy to see that $\varepsilon_{12}e_{12} + \varepsilon_{13}e_{13} + \varepsilon_{23}e_{23}$ are strictly nilpotent matrices.

All other matrices are square roots of semicentral idempotents. Thus, $e_{11} + \varepsilon_{12}e_{12} + \varepsilon_{13}e_{13} + e_{23}$ are roots of ℓ_1 and $e_{33} + \varepsilon_{23}e_{23} + \varepsilon_{13}e_{13} + e_{12}$ are roots of r_1.

5. Application A: Decomposition of Idempotent Triangular Matrices into Semicentral Idempotents

Example 4. *In Example 1, we obtain that all idempotent 2×2 matrices over S are $E(e_1, e_2) = \begin{pmatrix} e_1 & e_1\alpha_{12} + e_1\alpha_{12}e_2 + \alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}$, where $e_1, e_2, \alpha_{12} \in S$, and e_1 and e_2 are idempotents.*

Let us consider the monic left semicentral idempotent $1_1^\ell = \begin{pmatrix} 1 & \alpha_{12} \\ 0 & 0 \end{pmatrix}$ and the monic right semicentral idempotent $1_1^r = \begin{pmatrix} 0 & \alpha_{12} \\ 0 & 1 \end{pmatrix}$.

Then, we construct new idempotents as follows: $E_1^\ell = \operatorname{diag}(e_1, e_2)\, 1_1^\ell = \begin{pmatrix} e_1 & e_1\alpha_{12} \\ 0 & 0 \end{pmatrix}$ and $E_1^r = 1_1^r \operatorname{diag}(e_1, e_2) = \begin{pmatrix} 0 & \alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}$. Then, $E_1^\ell E_1^r = \begin{pmatrix} 0 & e_1\alpha_{12}e_2 \\ 0 & 0 \end{pmatrix}$. Therefore, $E(e_1, e_2) = E_1^\ell + E_1^r + E_1^\ell E_1^r = E_1^\ell \diamond E_1^r$.

We can now state another representation. The matrix $1^\jmath = \begin{pmatrix} 1 & \alpha_{12} \\ 0 & 1 \end{pmatrix}$ is a monic Jordan semicentral idempotent. We construct the matrices $E_1^{\jmath\,\text{left}} = \operatorname{diag}(e_1, e_2)\, 1^\jmath = \begin{pmatrix} e_1 & e_1\alpha_{12} \\ 0 & e_2 \end{pmatrix}$ and $E_1^{\jmath\,\text{right}} = 1^\jmath \operatorname{diag}(e_1, e_2) = \begin{pmatrix} e_1 & \alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}$. Thus, we have $E_1^{\jmath\,\text{left}} E_1^{\jmath\,\text{right}} = \begin{pmatrix} e_1 & e_1\alpha_{12}e_2 \\ 0 & e_2 \end{pmatrix}$ and then it follows that $E(e_1, e_2) = E_1^{\jmath\,\text{left}} + E_1^{\jmath\,\text{right}} + E_1^{\jmath\,\text{left}} E_1^{\jmath\,\text{right}} = E_1^{\jmath\,\text{left}} \diamond E_1^{\jmath\,\text{right}}$.

Example 5. *In Example 2, we find that all idempotent matrices of $T_3(S)$ are matrices of the form $E(e_1,e_2,e_3)=\begin{pmatrix} e_1 & \delta_{12} & \delta_{13}+\delta_{12}\delta_{13} \\ 0 & e_2 & \delta_{23} \\ 0 & 0 & e_3 \end{pmatrix}$, where $\delta_{ij}=e_i\alpha_{ij}+e_i\alpha_{ij}e_j+\alpha_{ij}e_j$, $e_i,\alpha_{ij}\in S$, $i,j=1,2,3$, $i<j$, and $e_i^2=e_i$.*

The matrices $1_1^\ell=\begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $1_2^\ell=\begin{pmatrix} 1 & 0 & \alpha_{13} \\ 0 & 1 & \alpha_{23} \\ 0 & 0 & 0 \end{pmatrix}$ are monic left semicentral idempotents. The matrices $1_1^r=\begin{pmatrix} 0 & 0 & \alpha_{13} \\ 0 & 0 & \alpha_{23} \\ 0 & 0 & 1 \end{pmatrix}$ and $1_2^r=\begin{pmatrix} 0 & \alpha_{12} & \alpha_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ are monic right semicentral idempotents, where $\alpha_{12},\alpha_{13},\alpha_{23}\in S$.

Now, we can construct $E_1^\ell=\operatorname{diag}(e_1,e_2,e_3)\,1_1^\ell=\begin{pmatrix} e_1 & e_1\alpha_{12} & e_1\alpha_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $E_2^\ell=\operatorname{diag}(e_1,e_2,e_3)\,1_2^\ell=\begin{pmatrix} e_1 & 0 & e_1\alpha_{13} \\ 0 & e_2 & e_2\alpha_{23} \\ 0 & 0 & 0 \end{pmatrix}$. Similarly, $E_1^r=1_1^r\operatorname{diag}(e_1,e_2,e_3)=\begin{pmatrix} 0 & 0 & \alpha_{13}e_3 \\ 0 & 0 & \alpha_{23}e_3 \\ 0 & 0 & e_3 \end{pmatrix}$ and $E_2^r=1_2^r\operatorname{diag}(e_1,e_2,e_3)=\begin{pmatrix} 0 & \alpha_{12}e_2 & \alpha_{13}e_3 \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}$. Then, $E_1^\ell E_2^r=\begin{pmatrix} 0 & e_1\alpha_{12}e_2 & e_2\alpha_{13}e_3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $E_2^\ell E_1^r=\begin{pmatrix} 0 & 0 & e_1\alpha_{13}e_3 \\ 0 & 0 & e_2\alpha_{23}e_3 \\ 0 & 0 & 0 \end{pmatrix}$. All these matrices are idempotents.

Next, let $\Delta_1=E_1^\ell\diamond E_2^r=\begin{pmatrix} e_1 & \delta_{12} & \delta_{13} \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}$ and $\Delta_2=E_2^\ell\diamond E_1^r=\begin{pmatrix} e_1 & 0 & \delta_{13} \\ 0 & e_2 & \delta_{23} \\ 0 & 0 & e_3 \end{pmatrix}$, which are also idempotents. Then, we have $\Delta_1+\Delta_2=\begin{pmatrix} e_1 & \delta_{12} & \delta_{13} \\ 0 & e_2 & \delta_{23} \\ 0 & 0 & e_3 \end{pmatrix}=\Delta$ and, from Theorem 2, it follows that $E(e_1,e_2,e_3)=(\Delta_1+\Delta_2)^2$.

There is another way of describing the idempotent matrix $E(e_1,e_2,e_3)$. It is easy to see that $(E_1^\ell\diamond E_2^r)(E_2^\ell\diamond E_1^r)+(E_2^\ell\diamond E_1^r)(E_1^\ell\diamond E_2^r)=E(e_1,e_2,e_3)$.

From the monic Jordan semicentral idempotent $1_{\ell_1}^J=\begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, we construct $E_{\ell_1}^{J\,\text{left}}=\begin{pmatrix} e_1 & e_1\alpha_{12} & e_1\alpha_{13} \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}$ and $E_{\ell_1}^{J\,\text{right}}=\begin{pmatrix} e_1 & \alpha_{12}e_2 & \alpha_{13}e_3 \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}$. Then, $E_{\ell_1}^{J\,\text{left}}E_{\ell_1}^{J\,\text{right}}=\begin{pmatrix} e_1 & e_1\alpha_{12}e_2 & e_1\alpha_{13}e_3 \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}$. Therefore, $E_{\ell_1}^{J\,\text{left}}\diamond E_{\ell_1}^{J\,\text{right}}=\Delta_1$.

Similarly, $E_{r_1}^{J\,\text{left}}\diamond E_{r_1}^{J\,\text{right}}=\Delta_2$, where $1_{r_1}^J=\begin{pmatrix} 1 & 0 & \alpha_{13} \\ 0 & 1 & \alpha_{23} \\ 0 & 0 & 1 \end{pmatrix}$ is another monic Jordan semicentral idempotent. Thus, we can represent $E(e_1,e_2,e_3)$ only by the monic Jordan semicentral idempotents.

Theorem 7. *Let $E(e_1,\dots,e_n)$ be an arbitrary idempotent triangular $n\times n$ matrix over an additively idempotent semiring. Then,*

$$E(e_1,\dots,e_n)=\left(\sum_{k=1}^{n-1}E_k^{\ell}\diamond E_{n-k}^{r}\right)^{n-1}, \tag{6}$$

where $E_k^{\ell}=\operatorname{diag}(e_1,\dots,e_n)\,1_k^{\ell}$ and $E_{n-k}^{r}=1_{n-k}^{r}\operatorname{diag}(e_1,\dots,e_n)$, $k=1,\dots,n-1$.

Proof. We know that $1_k^{\ell}=\begin{pmatrix} I_k & A\\ 0 & 0\end{pmatrix}$, where $I_k=\sum_{i=1}^{k}e_{ii}$ and $A\in M_{k\times(n-k)}(S)$. Then, $E_k^{\ell}=\begin{pmatrix} E_k & E_kA\\ 0 & 0\end{pmatrix}$, where $E_k=\operatorname{diag}(e_1,\dots,e_k)$. Similarly, from $1_{n-k}^{r}=\begin{pmatrix} 0 & A\\ 0 & I_{n-k}\end{pmatrix}$, where $I_{n-k}=\sum_{i=k+1}^{n}e_{ii}$, it follows that $E_{n-k}^{r}=\begin{pmatrix} 0 & AE_{n-k}\\ 0 & E_{n-k}\end{pmatrix}$, where $E_{n-k}=\operatorname{diag}(e_{k+1},\dots,e_n)$. Now, we find $E_k^{\ell}E_{n-k}^{r}=\begin{pmatrix} 0 & E_kAE_{n-k}\\ 0 & 0\end{pmatrix}$ and $E_{n-k}^{r}E_k^{\ell}=0$.

Then, $\Delta_k=E_k^{\ell}\diamond E_{n-k}^{r}=I+D_k$, where I is the identity matrix and $D_k=(\delta_{ij})$, $i=1,\dots,k$, $j=k+1,\dots,n$.

Consequently,

$$\sum_{k=1}^{n-1}E_k^{\ell}\diamond E_{n-k}^{r}=\sum_{k=1}^{n-1}\Delta_k=\Delta$$

and by Theorem 2 and Corollary 1, the result follows. □

In a particular case when $E(e_1,\dots,e_n)=\operatorname{diag}(e_1,\dots,e_n)$, the formula in Theorem 7 is an identity. In order to represent the diagonal matrix $E(e_1,\dots,e_n)$ by left and right semicentral idempotents, we prove the next result.

Corollary 3. *The matrix $E(e_1,\dots,e_n)=\operatorname{diag}(e_1,\dots,e_n)$ can be presented in the form*

$$\sum_{i=1}^{n}e_i1_{n-i+1}^{r}1_i^{\ell}=e_1r_n\ell_1\diamond\cdots\diamond e_i1_{n-i+1}^{r}1_i^{\ell}\diamond\cdots\diamond e_nr_1\ell_n.$$

Proof. It follows that the matrix unit e_{ii}, $i=1,\dots,n$, can be presented in the form $1_{n-i+1}^{r}1_i^{\ell}$, where all entries of these semicentral idempotents over the main diagonal are zeroes. Note that $1_n^{r}=1_n^{\ell}=I$. Since $e_i1_{n-i+1}^{r}1_i^{\ell}$ are orthogonal idempotents, the sum is equal to a diamond composition on the right side. □

From the proof of Theorem 7, we obtain a new equality, similar to (6).

Corollary 4. *Let $E(e_1,\dots,e_n)$ be an arbitrary idempotent triangular $n\times n$ matrix over an additively idempotent semiring. Then,*

$$E(e_1,\dots,e_n)=\left(\sum_{k=1}^{n-1}E_{\ell_k}^{J}\diamond E_{r_{n-k}}^{J}\right)^{n-1},$$

where $E_{\ell_k}^{J}=\operatorname{diag}(e_1,\dots,e_n)1_{\ell_k}^{J}$, $E_{r_{n-k}}^{J}=1_{r_{n-k}}^{J}\operatorname{diag}(e_1,\dots,e_n)$ for $k=1,\dots,n-1$.

Proof. From Section 4, we know that $1_{\ell_k}^{J}=I+1_k^{\ell}$ and $1_{r_{n-k}}^{J}=I+1_{n-k}^{r}$ where $k=1,\dots,n-1$ are monic Jordan semicentral idempotents. Both matrices are equal to

$\begin{pmatrix} I_k & A \\ 0 & I_{n-k} \end{pmatrix}$, which has only ones on the main diagonal and a matrix, $A \in M_{k\times(n-k)}(S)$, is in the right upper corner.

Under the notations in the proof of Theorem 7, it follows that $E^J_{\ell_k} = \begin{pmatrix} E_k & E_kA \\ 0 & E_{n-k} \end{pmatrix}$, $E^J_{r_{n-k}} = \begin{pmatrix} E_k & AE_{n-k} \\ 0 & E_{n-k} \end{pmatrix}$ and $E^J_{\ell_k}E^J_{r_{n-k}} = \begin{pmatrix} E_k & E_kAE_{n-k} \\ 0 & E_{n-k} \end{pmatrix}$.

Hence, $E^J_{\ell_k} \diamond E^J_{r_{n-k}} = \Delta_k$, and the result follows. □

6. Application B: Decomposition of Strictly Upper Triangular Matrices into Semicentral Idempotents

Note that strictly upper triangular matrices (i.e., those with zeroes on the main diagonal) over an additively idempotent semiring, S, form a subsemiring of $T_n(S)$.

The following reasonings are very similar to those in [14,25] for triangular matrices over a ring.

By $NT_n(S)$, we denote the ring of strictly upper triangular (or nil-triangular) $n \times n$ matrices over the additively idempotent semiring S.

Example 6. *Let $A \in NT_2(S)$. Then, it follows that*

$$A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 1^\ell_1 1^r_1.$$

Let $A \in NT_3(S)$. As in the proof of Proposition 2.7 (cf. [25]), it follows that

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= 1^\ell_2\begin{pmatrix} 1 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1^\ell_2\begin{pmatrix} 1 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}1^r_2.$$

On the other hand, for $1^\ell_1 = \begin{pmatrix} 1 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $1^r_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, we obtain that $1^\ell_1 1^r_1 = 0$, which implies that $1^\ell_1 \diamond 1^r_1 = 1^\ell_1 + 1^r_1 = \begin{pmatrix} 1 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Therefore, $A = 1^\ell_2(1^\ell_1 + 1^r_1)1^r_2$.

Theorem 8. *Let S be an additively idempotent semirimg, $n \in \mathbb{N}$, and A a strictly upper triangular $n \times n$ matrix over S. Then,*

$$A = \prod_{k=0}^{n-1}\left(1^\ell_{n-1-k} + 1^r_k\right), \tag{7}$$

where $1^\ell_0 = 1^r_0 = 0$.

Proof. We can show that

$$A = \begin{pmatrix} B & C \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_{n-1} & C \\ 0 & 0 \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = 1^\ell_{n-1}\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix},$$

where $B \in NT_{n-1}(S)$ and $C \in M_{(n-1)\times 1}(S)$.

If $B = \prod_k B_k$, where $B_k \in Tr_{n-1}(S)$, then $\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = \prod_k \begin{pmatrix} B_k & 0 \\ 0 & 1 \end{pmatrix}$.

The proof proceeds by induction on n. By $1^{\ell}_k(p)$ (resp., $1^r_k(p)$) we denote a left (resp., right) semicentral idempotent $p \times p$ matrix where $p = 2, \ldots, n-1$.

For $n = 3$, using the first part of Example 4, we obtain

$$\begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} = 1^{\ell}_2(3) \begin{pmatrix} 1^{\ell}_1(2)1^r_1(2) & 0 \\ 0 & 1 \end{pmatrix} = 1^{\ell}_2(3) \begin{pmatrix} 1^{\ell}_1(2) & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1^r_1(2) & 0 \\ 0 & 1 \end{pmatrix} =$$

$$= 1^{\ell}_2(3) \left[\begin{pmatrix} 1^{\ell}_1(2) & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] 1^r_2(3) = 1^{\ell}_2(3)(1^{\ell}_1(3) + 1^r_1(3))1^r_2(3) = \prod_{k=0}^{3} \left(1^{\ell}_{2-k} + 1^r_k \right).$$

We assume that $B = \prod_{k=0}^{n-2} \left(1^{\ell}_{n-2-k}(n-1) + 1^r_k(n-1) \right)$. Then, we find

$$\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = \prod_{k=0}^{n-2} \begin{pmatrix} 1^{\ell}_{n-2-k}(n-1) + 1^r_k(n-1) & 0 \\ 0 & 1 \end{pmatrix} = \prod_{k=0}^{n-2} \left(1^{\ell}_{n-2-k}(n) + 1^r_{k+1}(n) \right).$$

Hence, $A = 1^{\ell}_{n-1}(n) \prod_{k=0}^{n-3} \left(1^{\ell}_{n-2-k}(n) + 1^r_{k+1}(n) \right) 1^r_{n-1}(n)$, which gives the desired conclusion. □

7. Application C: Decomposition of Unitriangular Matrices into Semicentral Idempotents

Recall that a matrix is called unitriangular if it is upper triangular and has only ones on the main diagonal. Each unitriangular matrix has the form $I + A$, where I is an identity matrix and A is a strictly upper triangular matrix. It is easy to see that unitriangular matrices over an additively idempotent semiring, S, form a subsemiring of $T_n(S)$.

First, let us consider the representation of a unitriangular idempotent matrix by left and semicentral idempotents. As a consequence of Theorem 7, we have the following.

Proposition 18. *Let U be a unitriangular idempotent $n \times n$ matrix over an additively idempotent semiring. Then, $U = \left(\sum_{k=1}^{n-1} 1^{\ell}_k \diamond 1^r_{n-k} \right)^{n-1}$.*

For some unitriangular idempotent matrices, which are "near" to the identity matrix, the representation by semicentral idempotents takes an especially simple form.

Proposition 19. *Let $U = (a_{ij}) \in T_n(S)$, where $a_{ii} = 1$, $a_{ij} = 0$ for all $i, j = 1, \ldots, n$, $i < j$, except $a_{i\,i+1}$ if i is an odd integer, and S be an additively idempotent semiring. Then, $U = \sum_{k=1}^{n-1} \left(1^{\ell}_k \diamond 1^r_{n-k} \right)$.*

Proof. It is enough to show that U is an idempotent matrix, and for each $k = 1, \ldots, n-1$, the matrix $1^{\ell}_k \diamond 1^r_{n-k}$ contains a $k \times (n-k)$ matrix which is a submatrix of U with all entries being zeroes except $a_{k\,k+1}$ if k is an odd integer. □

The next example elucidates that there are unitriangular idempotent matrices represented only by a diamond composition of left and right semicentral idempotents.

Example 7. *Let* $A = (a_{ij})$ *where* $a_{ij} \in S$ *is a unitriangular idempotent* 4×4 *matrix. Let* $1_k^\ell = \begin{pmatrix} I_k & B \\ 0 & 0 \end{pmatrix}$, *where* $I_k = \sum_{i=1}^{k} e_{ii}$, $B = (a_{ij}) \in M_{k\times(4-k)}(S)$, *and* B *is a submatrix of* A, *be a monic left semicentral idempotent for* $k = 1, 2, 3$. *Let* $1_{4-k}^r = \begin{pmatrix} 0 & C \\ 0 & I_{4-k} \end{pmatrix}$, *where* $I_{4-k} = \sum_{i=k+1}^{4} e_{ii}$ *and* $C = (a_{ij}) \in M_{(4-k)\times k}(S)$ *and* C *is a submatrix of* A, *be a monic right semicentral idempotent for* $k = 1, 2, 3$. *Then, we have*

$$A = (1_3^\ell \diamond 1_1^r) \diamond (1_2^\ell \diamond 1_2^r) \diamond (1_1^\ell \diamond 1_3^r).$$

Next, we study the notion of a diamond composition of the arbitrary triangular matrices A and B. Thus, $A \diamond B = A + B + AB$ is neither an idempotent matrix nor a nilpotent matrix.

Now, for the arbitrary triangular matrices A and B, it is easy to obtain that $(I + A) \diamond (I + B) = I + (A \diamond B)$, where I is the identity matrix. Consequently, the semiring of unitriangular matrices is closed under a diamond composition.

By induction (and using the associativity of a diamond composition), it follows that $\diamondsuit_k(I + A_k) = I + \diamondsuit_k A_k$, where A_k are arbitrary triangular matrices.

In the text between Remark 5 and Remark 6, we find, for Jordan semicentral idempotents, that $1^J_{\ell_{n-k}} = I + 1^\ell_{n-k}$ and $1^J_{r_k} = I + 1^r_k$.

Therefore, it follows that $1^J_{\ell_{n-k}} \diamond 1^J_{r_k} = I + 1^\ell_{n-k} \diamond 1^r_k$ which implies that $\diamondsuit_{k=1}^{n-1}\left(1^J_{\ell_{n-k}} \diamond 1^J_{r_k}\right) = I + \diamondsuit_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right)$.

Theorem 9. *Let* S *be an additively idempotent semirimg,* $n \in \mathbb{N}$, *and* U *a unitriangular* $n \times n$ *matrix over* S. *Then,*

$$U = \diamondsuit_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right) = \diamondsuit_{k=1}^{n-1}\left(1^J_{\ell_{n-k}} \diamond 1^J_{r_k}\right). \tag{8}$$

Proof. Let A be the strictly upper triangular matrix from Theorem 8. The sum of each two corresponding (with the same number) entries on the main diagonals of the matrices 1^ℓ_{n-k} and 1^r_k is 1. The sum of all left and all right semicentral idempotent matrices (from the representation of A in Theorem 8) contains all entries of A. Moreover, the product $1^\ell_{n-k}1^r_k$ is a submatrix of A (using the reasoning in Section 4 before Lemma 1). Then, we have $\sum_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right) = I + A$.

On the other hand, any product, $\prod_{k=p}^{q}\left(1^\ell_{n-k} \diamond 1^r_k\right)$, $0 \le p < q \le n-1$, is a submatrix of $I + A$. Consequently, $U = I + A = \diamondsuit_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right) = \diamondsuit_{k=1}^{n-1}\left(1^J_{\ell_{n-k}} \diamond 1^J_{r_k}\right)$. □

From the proof of the last theorem, we have the following.

Corollary 5. *Let* 1^ℓ_{n-k} *and* 1^r_k *for* $k = 1, \ldots, n-1$ *be left and right semicentral idempotent matrices. Let all these semicentral idempotents be submatrices of the unitriangular matrix* $A = (a_{ij}) \in T_n(S)$. *Then,*

$$\sum_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right) = \prod_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right) = \diamondsuit_{k=1}^{n-1}\left(1^\ell_{n-k} \diamond 1^r_k\right).$$

D. I. Vladeva (see [26]) considered derivations of the semirings of triangular Toeplitz $n \times n$ matrices over an additively idempotent semiring. For basic facts and many applications of Toeplitz matrices, we refer the reader to R. Gray (see [27]). Note that any triangular Toeplitz $n \times n$ matrix (or diagonal-constant matrix) depends only on the entries $a_{11}, \ldots, a_{1n}$

placed on the diagonals of the matrix. As a consequence of the last theorem and (8), we obtain the following.

Corollary 6. *Let $A = (a_{ij}) \in T_n(S)$ be a Toeplitz matrix, where S is an additively idempotent semiring. If a_{11} is a unit of S, then $A = a_{11}\diamondsuit_{k=1}^{n-1}\left(1_{n-k}^{\ell} \diamond 1_k^r\right)$.*

8. Application D: Nil-Clean Triangular Matrices—Decomposition into Semicentral Idempotents

A classical definition of W. K. Nicholson (see [28,29]) says that a ring, R, is clean if every element of R can be written as a sum of an idempotent and a unit. Using this notion, A.J. Diesl, in [24], introduced nil-clean rings as rings in which every element can be written as the sum of an idempotent and a nilpotent. Diesl's work caught the attention of a number of mathematicians, and in the past ten years, there have been many investigations concerning variants of nil-clean rings (see [30–32]). Inspired by these articles, we introduce a nil-clean additively idempotent semiring as a semiring in which every element can be written as the sum of an idempotent and a nilpotent.

Since the sum of two elements, a and b, in an additively idempotent semiring is $\max\{a, b\}$, we need an example of a nil-clean semiring.

Example 8. *We consider the finite set $\mathcal{C}_n = \{0, 1, \ldots, n-1\}$ and define $x \vee y = \max\{x, y\}$, where $x, y \in \mathcal{C}_n$. Thus, $(\mathcal{C}_n, \vee)$ is a join-semilattice or a commutative idempotent semigroup. The map $\alpha : \mathcal{C}_n \to \mathcal{C}_n$ is called an endomorphism of the finite chain $\mathcal{C}_n$ if $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$. The set of endomorphisms with a fixed point, 0, is a semiring, denoted by $\mathcal{E}_{\mathcal{C}_n}^{(0)}$, with respect to the addition and multiplication defined by the following:*

$(\alpha + \beta)(x) = \alpha(x) \vee \beta(x)$ and $(\alpha\beta)(x) = \beta(\alpha(x))$, where $x \in \mathcal{C}_n$ and $\alpha, \beta \in \mathcal{E}_{\mathcal{C}_n}^{(0)}$.

We denote by $(0, 1, \ldots, n-1)$ and by $(0, 0, \ldots, 0)$ the identity and the zero of $\mathcal{E}_{\mathcal{C}_n}^{(0)}$, respectively. For more information regarding endomorphism semirings, the reader is referred to [17]. In [17], as well as in [18], we consider a semiring which is a subsemiring of the endomorphism semiring $\mathcal{E}_{\mathcal{C}_n}^{(0)}$, consisting of the endomorphisms α such that $\alpha(k) \leq k$ for all $k \in \mathcal{C}_n$. As this semiring is associated with Catalan numbers, we call it the Catalan endomorphism semiring and denote it by $\mathcal{CAT}_n$. We note the following properties:

(i) For an arbitrary $\alpha \in \mathcal{CAT}_n$, it follows that $\alpha \leq (0, 1, \ldots, n-1)$, where $\mathcal{CAT}_n$ is an incline (see [33]). It can be easily checked that this is the maximal subsemiring of $\mathcal{E}_{\mathcal{C}_n}^{(0)}$, which is an incline.

(ii) The order of $\mathcal{CAT}_n$ is the n-th Catalan number C_n. (For the definition and properties of Catalan numbers, the reader is referred to [34].)

(iii) The nilpotent endomorphisms of $\mathcal{E}_{\mathcal{C}_n}^{(0)}$ are the endomorphisms α such that $\alpha^m = (0, 0, \ldots, 0)$ for some positive integer, m, and they also have the property $\alpha(k) < k$ for all $k \in \mathcal{C}_n$. The set of nilpotent endomorphisms is an ideal of $\mathcal{CAT}_n$ of the order of the $(n-1)$-th Catalan number C_{n-1}.

Now, consider an arbitrary endomorphism, $\alpha \in \mathcal{CAT}_n$. If α has no fixed points, it follows that $\alpha(k) < k$ for all $k \in \mathcal{C}_n$. Consequently, α is a nilpotent. Since $\alpha = \alpha + (0, 0, \ldots, 0)$, we have that α is a sum of an idempotent and nilpotent.

Let k be the lowest number which is a fixed point of α. We consider the following possibilities.

Case 1. Let $k = 1$. Assume that $k_1 = k = 1 < k_2 < \cdots < k_s$ are all fixed points of α. Now, if $x \in \mathcal{C}_n$ and $1 < x < k_2$, then $\alpha(x) = 1$. Similarly, if $k_{s-1} < x < k_s$, then $\alpha(x) = k_{s-1}$.

Case 1.1. If $k_s = n - 1$, then α is an idempotent. It is reasonable to assume that $n \geq 3$. Then, the endomorphism $(0, \ldots, 0, 1)$ is a nilpotent. Now, from $\alpha = \alpha + (0, \ldots, 0, 1)$, we have that α is a sum of an idempotent and nilpotent.

Case 1.2. Let $k_s < n-1$. If $\alpha(x) = k_s$ for all x such that $k_s \leq x \leq n-1$, then α is an idempotent. Assume that for some x, $k_s < x \leq n-1$, we have $\alpha(x) = p < x$ where $p \neq k_s$. Now, we construct a new endomorphism, β, such that $\beta(x) = 0$ for all x, $0 \leq x \leq k_s$, and $\beta(x) = \alpha(x)$ for x such that $k_s < x \leq n-1$. Then, β is a nilpotent. Additionally, we construct an endomorphism, γ, such that $\gamma(x) = \alpha(x)$ for all x, such that $0 \leq x \leq k_s$ and $\gamma(x) = k_s$ for x, $k_s \leq x \leq n-1$. Consequently, γ is an idempotent. It is easy to see that $\alpha = \beta + \gamma$.

Case 2. Let k, where $k > 1$, be the smallest fixed point of α. Then, for all x, $1 \leq x \leq k-1$, we have $\alpha(x) < x$. Let $\alpha(k-1) = p < k-1$. Now, we construct an endomorphism, β, such that $\beta(x) = \alpha(x)$ for all x, $0 \leq x \leq k-1$, and $\beta(x) = p$ for all x, $k \leq x \leq n-1$. Since β has no fixed points, it is a nilpotent. Assume that $k_1 = k < k_2 < \cdots < k_s$ are all fixed points of α. Now, for x such that $k < x < k_2$, we have $\alpha(x) = k$. Similarly, if $k_{s-1} < x < k_s$, then $\alpha(x) = k_{s-1}$.

Case 2.1. Let $k_s = n-1$. We construct an endomorphism, γ, where $\gamma(x) = 0$ f0r all x such that $0 \leq x \leq k-1$ and $\gamma(x) = \alpha(x)$ for x, $k \leq x \leq n-1$. Then, γ is an idempotent and $\alpha = \beta + \gamma$.

Case 2.2. Let $k_s < n-1$. We construct an endomorphism, β, such that $\beta(x) = \alpha(x)$ for all x, $0 \leq x \leq k-1$, $\beta(x) = \alpha(k-1)$ for all x, $k \leq x \leq k_s$, and $\beta(x) = \alpha(x)$ for all x, $k_s < x \leq n-1$. Since β has no fixed points, it is a nilpotent. Finally, we construct an endomorphism, γ, such that $\gamma(x) = 0$ for all x such that $0 \leq x \leq k-1$, $\gamma(x) = \alpha(x)$, for x, $k \leq x \leq k_s$, and $\gamma(x) = k_s$ for all x, such that $k_s \leq x \leq n-1$. Then, γ is an idempotent and $\alpha = \beta + \gamma$. Consequently, we prove that $\mathcal{CAT}_n$ is a nil-clean semiring.

Remark 9. *In the example above, we write $\alpha = \alpha + \nu$, where ν is a nilpotent element, for each idempotent α. We call this representation trivial. Are there nontrivial representations in the following sense: $e_1 = e + n$, where e_1 and e are idempotents, $e \neq e_1$, and n is a nilpotent element?*

In order to find such a representation, we consider an additive idempotent semiring, S, where ℓ (resp., r) is a left (resp., right) semicentral idempotent. Assume (as in Section 2) that $r\ell = 0$. Then, ℓr is a nilpotent element and $1 + \ell r$, $\ell + \ell r$ and $r + \ell r$ are nil-clean elements. It is easy to see that $1 + \ell r$, $\ell + \ell r$ and $r + \ell r$ are idempotents (moreover, $1 + \ell r$ is a Jordan semicentral idempotent; see Proposition 4). But, the subsemiring of S, generated by ℓ and r with the property $r\ell = 0$, is not a nil-clean semiring. It is interesting to know if there is a nil-clean semiring with the nontrivial representation of all idempotent elements. Such a nil-clean semiring will be considered in the remark after Proposition 22.

The next result shows why the notion of a nil-clean semiring is relevant to the study of triangular matrices.

Proposition 20. *The semiring $T_n(S)$ is nil-clean, provided that S is a nil-clean semiring.*

Proof. Let $A \in T_n(S)$, where S is a nil-clean semiring. Then, $A = (\varepsilon_{ij} + \eta_{ij})$, where ε_{ij} is an idempotent and η_{ij} is a nilpotent element for $i, j = 1, \ldots, n$, $i \leq j$. It follows that $A = E + N$, where $E = \operatorname{diag}(\varepsilon_{11}, \ldots, \varepsilon_{nn})$, and $N = (\eta_{ij}) + E_1$, where $E_1 = (\varepsilon_{ij})$ is a strictly upper triangular matrix. Since E is an idempotent matrix and N is a nilpotent matrix, it follows that $T_n(S)$ is a nil-clean semiring. □

In the next result, we represent a triangular matrix over a nil-clean semiring by left and right monic semicentral idempotent matrices.

Proposition 21. *Let $A \in T_n(S)$ where S is a nil-clean semiring. Then, there are the matrices $B, C \in T_n(S)$, such that we have the following:*

(i) $A = B + C$;

(ii) $B = \sum_{i=1}^{n} \varepsilon_{ii} 1^r_{n-i+1} 1^\ell_i$, where ε_{ii} are idempotents of S;

(iii) $C^m = \prod_{k=0}^{n-1}\left(1^{\ell}_{n-1-k} + 1^{r}_{k}\right)$ *for some positive integer,* m.

Proof. By the last proposition, it follows that $A = B + C$, where B is an idempotent diagonal matrix and C is a nilpotent matrix. Using Corollary 11, we have that $B = \sum_{i=1}^{n} \varepsilon_{ii} 1^{r}_{n-i+1} 1^{\ell}_{i}$ where ε_{ii} are its diagonal elements.

Since diagonal entries of C are nilpotent elements, there is a positive integer, say, m, such that (according to Theorem 8 and (7)) $C^m = \prod_{k=0}^{n-1}\left(1^{\ell}_{n-1-k} + 1^{r}_{k}\right)$. □

It is important to know if there are nil-clean triangular matrices over S and which entries are not nil-clean elements of S. In a similar vein, J. Šter (see [35]) has shown that $M_n(R)$ is a nil-clean ring if R is a Boolean ring.

Note that in Example 3, we describe all matrices of $T_3(\mathbb{B})$, where $\mathbb{B}$ is the Boolean semiring, as follows: left, right, and Jordan semicentral idempotents, idempotents which are not semicentral, and strictly upper and square roots of semicentral idempotent matrices.

Proposition 22. *The semiring* $T_n(\mathbb{B})$ *is nil-clean where* $\mathbb{B}$ *is the Boolean semiring.*

Proof. The proof is straightforward. □

Remark 10. *Every idempotent matrix,* $A \in T_n(\mathbb{B})$*, is a sum of its main diagonal, which is also an idempotent matrix and strictly upper matrix consisting of all entries over the main diagonal of* A*. Therefore, there is a nontrivial representation of* A *in the sense of Remark 8.*

Now, we represent a matrix in $T_n(\mathbb{B})$ by semicentral idempotent matrices.

Proposition 23. *Let* $A \in T_n(\mathbb{B})$*, where* $\mathbb{B}$ *is the Boolean semiring. Then,*

$$A = \varepsilon_{11} 1^{r}_{n} 1^{\ell}_{1} + \cdots + \varepsilon_{ii} 1^{r}_{n-i+1} 1^{\ell}_{i} + \cdots + \varepsilon_{nn} 1^{r}_{1} 1^{\ell}_{n} + \prod_{k=0}^{n-1}\left(1^{\ell}_{n-1-k} + 1^{r}_{k}\right),$$

where $\varepsilon_{ii} = 1$ *or* $\varepsilon_{ii} = 0$ *for* $i = 1, \ldots, n$.

Proof. The proof is similar to that of Proposition 20. □

By the same reasoning, we prove the next result.

Proposition 24. *Let* S_0 *be a nil-clean subsemiring of* $T_n(S)$ *where* S *is an additively idempotent semiring. Then, for every matrix,* $A \in S_0$*, there are* $B, C \in S_0$ *such that we have the following:*

(i) $A = B + C$.

(ii) B *is an idempotent matrix with the diagonal entries* e_i, $i = 1, \ldots, n$, *and*
$B = \left(\sum_{k=1}^{n-1} E^{\ell}_{k} \diamond E^{r}_{n-k}\right)^{n-1}$, $E^{\ell}_{k} = \mathrm{diag}(e_1, \ldots, e_n) 1^{\ell}_{k}$, $E^{r}_{n-i} = 1^{r}_{n-k} \mathrm{diag}(e_1, \ldots, e_n)$,
$k = 1, \ldots, n-1$.

(iii) $C^m = \prod_{k=0}^{n-1}\left(1^{\ell}_{n-1-k} + 1^{r}_{k}\right)$ *for some positive integer,* m.

There are enough nil-clean subsemirings of $T_n(S)$. Since every semicentral (not necessarily monic) idempotent matrix is nil-clean, we can add to such matrices an arbitrarily strictly upper matrix. Now, the matrices $1^{\ell}_{k} + N_k$ and $1^{r}_{m} + N_m$, where N_k and N_m are strictly upper, are nil-clean matrices. It is easy to see that these matrices form a semiring.

9. Conclusions

In this paper, we obtain the explicit form of an arbitrary idempotent triangular matrix over an additively idempotent semiring. The explicit forms of left and right semicentral

idempotents are given. A new type of semicentral idempotent, called Jordan, is studied. A diamond composition of two idempotent matrices is defined, which plays an important role in decompositions of many triangular matrices.

We consider this paper as a step towards the construction of a linear algebra on additively idempotent semirings, generalizing the idea of well-known max-algebra.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The author wish to tank the reviewers and The editors for helpful comments and suggestions that improved the quality of the article.

Conflicts of Interest: The author declare no conflicts of interest.

References

1. Bistarelli, S. *Semirings for Soft Constraint Solving and Programming*; Springer: Berlin/Heidelberg, Germany, 2004.
2. Brunsch, T.; Hardouin L.; Maiac, C.; Raisc, J. Duality and interval analysis over idempotent semirings. *Linear Algebra Appl.* **2012**, *437*, 2436–2454. [CrossRef]
3. Butkovič, P. *Max-Linear Systems: Theory and Algorithms*; Springer: London, UK, 2010.
4. Gaubert, S.; Katz, R. Reachability problems for products of matrices in semirings. *Int. J. Algebra Comp.* **2006**, *16*, 603–622. [CrossRef]
5. Gaubert, S.; Katz, R. Max-Plus Convex Geometry. In Proceedings of the Conference on Relational Methods in Computer Science, RelMiCS/AKA 2006, Manchester, UK, 29 August–2 September 2006.
6. Grigoriev, D.; Shpilrain, V. Tropical cryptography. *Commun. Algebra* **2014**, *42*, 2624–2632. [CrossRef]
7. Di Nola, A.; Gerla, B. Algebras of Łukasiewicz's Logic and their Semiring Reducts. In *Idempotent Mathematics and Mathematical Physics*; Contemporary Mathematics; American Mathematical Society: Providence, RI, USA, 2005; Volume 377, pp. 131–144.
8. Perri, T.; Rowen, L.H. Kernels in tropical geometry and a Jordan-Holder theorem. *J. Algebra Its Appl.* **2018**, *17*, 1850066. [CrossRef]
9. Drensky, V.S. Idempotents of 2×2 matrix rings over rings of formal power series. *Linear Multilinear Algebra* **2022**, *70*, 5207–5213. [CrossRef]
10. Peirce, B. Linear Associative Algebra. Washington, 1870. *Am. J. Math.* **1870**, *4*, 99–215. Available online: http://www.math.harvard.edu/history/peircealgebra/index.html (accessed on 1 February 2025).
11. Hou, X. Idempotents in triangular matrix rings. *Linear Multilinear Algebra* **2021**, *69*, 296–304. [CrossRef]
12. Wright, S.E. Triangular idempotent matrices over a general ring. *Linear Multilinear Algebra* **2022**, *70*, 1717–1731. [CrossRef]
13. Vladeva, D.I. The role of semicentral idempotents in triangular matrix rings. In *Communications in Algebra*; Taylor & Francis: Abingdon, UK, 2024; Volume53, pp. 1024–1038. [CrossRef]
14. Vladeva, D.I. Semicentral idempotents of upper triangular matrix ring. *J. Algebra Appl.* 2024, *Submitted 02.02.2024, Accepted 24.11. 2024* (to appear).
15. Trendafilov, I.D.; Vladeva, D.I. Idempotent Elements of the Endomorphism Semiring of a Finite Chain. *C. R. l'Académie Bulg. Sci.* **2013**, *66*, 621–628.
16. Chajda, I.; Länger, H. The variety of commutative additively and multiplicatively idempotent semirings. *Semigroup Forum* **2018**, *96*, 409–415. [CrossRef]
17. Vladeva, D.I. Projections on right and left ideals of endomorphism semiring which are derivations. *J. Algebra Appl.* **2020**, *19*, 2050212-1–2050212-26. [CrossRef]
18. Vladeva, D.I. Derivations of some classes of additively idempotent semirings. *Commun. Algebra* **2023**, *51*, 3244–3265. [CrossRef]
19. Golan, J.S. *Semirings and Their Applications*; Kluwer Academic Press: Dordrecht, The Netherlands, 1999.
20. Gantmacher, F.R. *Matrix Theory Vol. 1*; Chelsea: New York, NY, USA, 1959.
21. Jain, S.K.; Goel, V.K.; Kwak, E.K. Nonnegative m th Roots of Nonnegative 0-Symmetric ldempotent Matrices. *Linear Algebra Its Appl.* **1979**, *23*, 37–51. [CrossRef]
22. Birkenmeier, G.F.; Park, J.K.; Rizvi, S.T. *Extensions of Rings and Modules*; Springer: Berlin/Heidelberg, Germany; Birkhäuser: Basel, Switzerland, 2013.
23. Vladeva, D.I. Derivations of skew Ore polynomial semirings. *Commun. Algebra* **2020**, *48*, 4718–4731. [CrossRef]
24. Diesl, A.J. Nil clean rings. *J. Algebra* **2013**, *383*, 197–211. [CrossRef]
25. Alahmadi, A.; Jain, S.K.; Leroy, A.; Sathaye, A. Decompositions into products of idempotents. *Electron. J. Linear Algebra* **2015**, *29*, 74–88. [CrossRef]

26. Vladeva, D.I. Derivatives of triangular, Toeplitz, circulant matrices and of matrices of other forms over semirings. In Proceedings of the 43rd International Conference Applications of Mathematics in Engineering and Economics, Sozopol, Bulgaria, 8–13 June 2017; Volume 1910, pp. 060006-1–060006-12.
27. Gray, R. *Toeplitz and Circulant Matrices: A Review*; Stanford University Press: Stanford, CA, USA, 2006.
28. Nicholson, W.K. Lifting idempotents and exchange rings. *Trans. Am. Math. Soc.* **1977**, *229*, 269–278. [CrossRef]
29. Nicholson, W.K.; Zhou, Y. *Clean Rings: A Survey, Advances in Ring Theory*; World Scientific Publication: Hackensack, NJ, USA, 2005; pp. 181–198.
30. Breaz, S.; Călugăreanu, G.; Danchev, P.; Micu, T. Nil-clean matrix rings. *Linear Algebra Appl.* **2013**, *439*, 3115–3119. [CrossRef]
31. Breaz, S.; Danchev, P.; Zhou, Y. Rings in which every element is either a sum or a difference of a nilpotent and an idempotent. *J. Algebra Appl.* **2016**, *15*, 1650148-1–1650148-13. [CrossRef]
32. Danchev, P.; Garcia, E.; Lozano, M. Decompositions of matrices into diagonalizable and square-zero matrices. *Linear Multilinear Algebra* **2022**, *70*, 4056–4070. [CrossRef]
33. Cao, Z.; Kim, K.; Roush, F. *Incline Algebra and Applications*; John Wiley & Sons: New York, NY, USA, 1984.
34. Stanley, R. *Catalan Numbers*; Cambridge University Press: New York, NY, USA; Cambridge, UK, 2015.
35. Šter, J. On expressing matrices over $\mathbb{Z}_2$ as the sum of an idempotent and a nilpotent. *Linear Algebra Appl.* **2015**, *544*, 339–349. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

On the Equational Theory of Lattice-Based Algebras for Layered Graphs

Zhe Yu [1,†], Hao Zhan [2,†], Yiheng Wang [1], Zhe Lin [2,*] and Fei Liang [3,*]

[1] Department of Philosophy, Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou 510275, China; yuzh28@mail.sysu.edu.cn (Z.Y.); wangyh377@mail2.sysu.edu.cn (Y.W.)
[2] Department of Philosophy, Xiamen University, Xiamen 361005, China; haozhan@stu.xmu.edu.cn
[3] School of Philosophy and Social Development, Institute of Concept and Reasoning, Shandong University, Jinan 250061, China
* Correspondence: pennyshaq@163.com (Z.L.); f.liang@sdu.edu.cn (F.L.)
† These authors contributed equally to this work.

Abstract: Layered algebras are introduced and used to express layered graphs. Layered graphs are considered to be a highly effective abstract tool to manage the difficulty in conceptualizing and reasoning regarding complex systems related to coding in email exchange and access control in security. In the present paper, we study the varieties of several classes of lattice-based layer algebras and show that all these varieties have decidable equational theory via a finite model property.

Keywords: layered algebras; layered graph; residuated groupoid; residuated lattice; equational theory; variety; finite model property; decidability

MSC: 03G10; 06B20; 06B25; 06D30; 06D75

1. Introduction

A binary operation $\cdot$ on an algebra A with a carrier preordered set $(A, \leq)$ is said to be residuated if there exist binary operations $\backslash$ and $/$ on A such that for any $a, b, c \in A$

$$a \cdot b \leq z \iff b \leq a \backslash c \iff a \leq c / b.$$

One refers to $\backslash$ and $/$ by the right and the left residual of $\cdot$, respectively.

A residuated Boolean algebra (r-algebra) is an algebraic structure $\mathrm{A} = (A, \wedge, \vee, \neg, \cdot, \backslash, /)$ such that $(A, \wedge, \vee, \neg)$ is a Boolean algebra and $\cdot$ is a binary operation on A, where $\backslash$ and $/$ are its right and left residuals, respectively. The R-algebras were first introduced by Jósson and Tsinakis [1] as generalizations for relation algebras due to A.Tarski.

The algebraic structures studied under the name of layered algebras by Collinson et al. [2] are the same as those discussed here. The non-commutative and non-associative operation $\cdot$ in groupoids is used to capture the feature of layering in layered graphs. Let G_1, G_2 be directed graphs. The composition of graphs is defined $G_1 \cdot G_2$ if $V(G_1) \cap V(G_2) = \varnothing$, $G_1 \rightsquigarrow G_2$, and $G_2 \not\rightsquigarrow G_1$, where $V(G_i)$ is the set of all vectors of graph G_i ($i \in \{1, 2\}$) and $G_1 \rightsquigarrow G_2$ means that G_2 is reachable from G_1. A graph G is said to be layered if there exist G_1, G_2 such that G_i ($i \in \{1, 2\}$) is a subgraph of G and $G = G_1 \cdot G_2$. The Boolean component and residuated duals of $\cdot$ are used to express properties in the layered graphs.

In the literature [2–4], the layered graph is considered to be a highly effective abstract tool to manage the difficulty in conceptualizing and reasoning about complex systems, including transport systems, IP stacks, email exchange, and access control in security. In

order to describe the subgraph relation in directed graphs, Heyting variants of layered algebras were developed by Docherty and Pym in [4]. A Heyting layered algebra is a combination of a Heyting algebra and a residuated groupoid.

Boolean and Heyting layered algebras are both residuated lattice-ordered groupoids (**RLG**s). This class of algebras was introduced and developed as mathematical tools of categorical grammars for natural language processing; see [5]. A residauted lattice (**RL**) with a carrier preordered set $(A, \leq)$ is an **RLG** in which $\cdot$ admits the associative property, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for any $a, b, c \in A$. The algebras corresponding to logics for querying graphs [6] and bigraphs [7] are residuated lattices. Further, many structures that are well studied already, such as generalized Boolean algebras, Brouwerian algebras, relative Stone algebras, and 'l-groups, are residuated lattices. The class of all residuated lattices will be denoted by $\mathcal{RL}$. Obviously, the residuated property can be captured by equations. Thus, $\mathcal{RL}$ and $\mathcal{RLG}$ are a finitely based variety.

For any algebraic structure A with domain A, an assignment in A is a function μ:**Var** $\rightarrow A$. Every assignment μ in A can be extended homomorphically to the term algebra. Let $\mu(t)$ be the element in A. An algebraic model is a pair (A, μ) where A is an algebraic structure and μ is an assignment in A. We say that (A, μ) satisfies an equation $t_1 \approx t_2$ if $\mu(t_1) = \mu(t_2)$. We write ie_i for the inequalities $t_i \leq t_j$, where $i, j \geq 0$. We say that (A, μ) satisfies a quasi-equation $ie_1 \& \ldots \& ie_n \Rightarrow ie_0$ if (A, μ) satisfies ie_0 whenever it satisfies ie_i $1 \leq i \leq n$. We say an equation e is true in the classes of algebra $\mathcal{A}$ if for any A $\in A$ and any assignment μ, (A, μ) satisfies e. A quasi-equation $e_1 \& \ldots \& ie_n \Rightarrow ie_0$ is said to be true in $\mathcal{A}$ if e_0 is true in $\mathcal{A}$ whenever each e_i $1 \leq i \leq n$ is true in $\mathcal{A}$.

A variety V is said to have a decidable equational theory if there is a computer algorithm that determines whether an equation is true or not in this variety in finite times. Let V be any finitely based variety. If V has the finite model property (FMP), then it has a decidable equational theory. If one replaces equation with quasi-equation, then V has a decidable quasi-equational theory. This problem for quasi-equation is referred to as the word problem for the classes of algebras. It is known that the strong finite model property (SFMP) is equivalent to the finite embeddability property (FEP) over $\mathcal{RLG}$ and $\mathcal{RL}$, which implies the decidability of quasi-equational theory [8].

We mention some FMP and decidability results of the equational and universal theories for classes of algebras closely related to $\mathcal{RLG}$ and $\mathcal{RL}$. The $\mathcal{RG}$ and $\mathcal{DLRG}$ have FEP, so the equational and quasi-equantional theories of them are both decidable (see M. Farulewski [9], W. Buszkowski [5], and Z. Hanikova and R. Horcik [10]). The same holds for the $\mathcal{BRG}$ and $\mathcal{HRG}$ [5] (also see M. Kaminski and N. Francez [11,12] and S. Docerty and D. Pym [4]). For $\mathcal{LRG}$, the undecidability of the universal theory is proved by K. Chvalovsky in [13], whereas the equational theory is proved to be decidable in [14]. The classes of $\mathcal{RL}$ and $\mathcal{RSG}$ have undecidability universal theory [15]; however, the equational theories are both decidable [14,16]. In [12], FMPs are proved for $\mathcal{DRL}$ and $\mathcal{HRL}$ via algebraic and relational semantics, respectively. It follows that the equational theories of the corresponding classes of algebras are decidable. The undecidability of the universal theory of (commutative) $\mathcal{DRL}$ is shown by N. Galatos [17]. Not all varieties of residuated lattices have decidable equational theory. Contractions $\mathcal{RL}$ (assuming $a \cdot a = a$) and $\mathcal{BRL}$ have undecidable equational theories [8].

In the present paper, we consider the decision problem for equational theories of various classes of bounded $\mathcal{DLRG}$ and several classes of commutative and contractive $\mathcal{QBRL}$. We prove that all these classes of algebras have decidable equational theories via showing they have FMPs. The FMP and decidability results are extended to the classes of fusion of associative and non-associative algebras under the same lattice-based algebras, e.g., $\mathcal{QBRL} \oplus \mathcal{QBRLG}$. There are a number of reasons to investigate the equational

theories of these classes of algebras. Firstly, by changing different lattices based in layer algebras, one can increase expressivity of graph properties. For example, a 4-valued and 3-valued sentence can be expressed in a layer graph when the bounded $\mathcal{DLRG}$ is a quasi-Boolean or Kleene algebra, respectively. Secondly, the associative and commutative multiplicative operation may help to reason about the decomposition of graphs into disjoint subgraphs [6,7]. Finally, there are also technical motivations. Although the FMP for bounded $\mathcal{DLRG}$, $\mathcal{HLRG}$, and $\mathcal{BLRG}$ follows from the FEP results, we provide direct proofs for the FMP of these classes of algebras. Further, our proofs cover some new classes of $\mathcal{DLRG}$, which have not been considered before, e.g., $\mathcal{QBLRG}$, $\mathcal{KLRG}$, and so on. Furthermore, we extend our results to several classes of commutative and contractive $\mathcal{QBRL}$, including $\mathcal{BRL}$.

We conclude the introduction by summarizing the contents of the paper. In Section 2, we recall some basic definitions and results of Boolean and Heyting residuated groupoids. In Section 3, we study various $\mathcal{RLG}$s. We prove that all these classes of algebras have finite model properties (FMPs), and their equation theories are decidable. Section 4 extends the results in Section 3 to several quasi-Boolean residuated algebras (including the Boolean one) in which the fusion $\cdot$ admits associative, commutative, and contractive aspects, i.e., $a \cdot a = a$, for some a in the domain of algebras. Further, we argue that the same results hold for several classes of algebras that are fusions of some classes of algebras considered in Sections 3 and 4. In the last section, we conclude our results and list some open problems that we hope will stimulate further research.

2. Layer Algebras

In this section, we recall the basic definitions and properties of (Heyting) layer algebras. These results are obtained from [5]. We assume familiarity with standard lattice theoretic notions, which can be found in [8,18].

Definition 1. *A magma (groupoid)* M *(M,·) is a structure such that M is a set of elements and $\cdot$ is a binary operation on M; i.e., for any $a, b \in M$, $a \cdot b \in M$. If $\cdot$ admits the associative property, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, then* M *is a semigroup.*

Definition 2 ([2])**.** *A layer algebra, first introduced and named residuated algebra, is a structure $(M, \cdot, \backslash, /, \wedge, \vee, \neg, 1, 0)$ such that $(M, \wedge, \vee, \neg, 1, 0)$ is a Boolean algebra and $\cdot, \backslash, /$ are binary operations on carrier set M satisfying that for any $a, b, c \in M$*

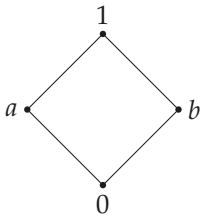
- *(res) $a \cdot b \leq c$ iff $b \leq a \backslash c$ iff $b \leq c / a$*

where $\leq$ is the lattice ordering.

The reduct $\mathrm{Rg} = (G, \cdot, \backslash, /, \leq)$ of a layer algebra is a residuated groupoid. A Heyting layer algebra $\mathrm{H} = (H, \cdot, \backslash, /, \wedge, \vee, \rightarrow, 1, 0)$ is a structure where $(H, \wedge, \vee, \rightarrow, 0, 1)$ is a Heyting algebra and $(H, \cdot, \backslash, /, \leq)$ is a residuated groupoid with the lattice ordering $\leq$. Obviously, a layer algebra is a Heyting layer algebra. In the following, A is used to represent an A algebra, **A** is used to represent a class of A algebras, and $\mathcal{A}$ is used to represent all classes of A algebras. We follow the tradition from [5] and use Boolean (Heyting) residuated groupoids for (Heyting) layer algebras, respectively.

Example 1. *The algebra in Figure 1 is an example of* BRG*s.*

Example 2. *The algebra in Figure 2 is an example of* HRG*s. One has $a \vee \neg a = a \neq 1$.*



	$\neg$
1	0
0	1
a	b
b	a

$\cdot$	0	a	b	1
0	0	a	b	1
a	0	a	b	1
b	0	a	a	a
1	0	a	b	1

$/$	0	a	b	1
0	0	0	0	0
a	a	a	1	a
b	b	b	0	b
1	1	1	1	1

$\backslash$	0	a	b	1
0	0	a	b	1
a	0	a	b	1
b	0	1	0	1
1	0	a	b	1

Figure 1. An example of BRG.



	$\neg$
1	0
0	1
a	0
b	0

$\rightarrow$	0	a	b	1
0	1	1	1	1
a	0	1	1	1
b	0	a	1	1
1	0	a	b	1

$\cdot$	0	a	b	1
0	0	a	1	1
a	0	0	1	1
b	0	0	a	a
1	0	0	a	a

$/$	0	a	b	1
0	0	a	a	a
a	a	a	1	1
b	a	a	1	1
1	1	1	1	1

$\backslash$	0	a	b	1
0	0	a	a	1
a	a	a	a	1
b	a	1	1	1
1	a	1	1	1

Figure 2. An example of HRG.

A layered magma is a structure $(M, \cdot)$ with a partial binary operation $\cdot$ on a carrier set M. The operation is said to be contra-commutative if, for all $m, n \in M$, if $m \cdot n$ is defined, then $n \cdot m$ is undefined. Given a layered magma $(M, \cdot)$, one constructs layered algebras by the following. Let $P(M)$ be the power set of M and $X, Y \in P(W)$. Define

- $X \bullet Y = \{a \cdot b | a \in X \& b \in Y, a \cdot b \text{ is defined}\}$.
- $X \backslash\backslash Y = \{c | \forall a \in X \text{ if } c \cdot a \text{ is defined, and then } c \cdot a \in Y\}$.
- $X // Y = \{c | \forall a \in X \text{ if } a \cdot c \text{ is defined, and then } a \cdot c \in Y\}$.

A layered magma can form a layered algebra by the following way.

Lemma 1. *In a Heyting residuated groupoid* $\mathrm{L} = (L, \cdot, \backslash, /, \wedge, \vee, \neg, 1, 0)$*, for any* $a, b, c \in L$*, if* $a \leq b$*, then* $a \cdot c \leq b \cdot c$ *and* $c \cdot a \leq c \cdot b$*.*

Corollary 1. *In a Heyting residuated groupoid* $\mathrm{L} = (L, \cdot, \backslash, /, \wedge, \vee, \neg, 1, 0)$*, for any* $a, b, c, d \in L$*, if* $a \leq b$ *and* $c \leq d$*, then* $a \cdot c \leq b \cdot d$*.*

Lemma 2. *In a Heyting-residuated groupoid* $\mathrm{L} = (L, \cdot, \backslash, /, \wedge, \vee, \neg, 1, 0)$*, let* $A, B \subseteq L$*, and* $\bigvee A, \bigvee B, \bigwedge A, \bigwedge B$ *exist. Then, the following hold*

- $\bigvee_{a \in A, b \in B} a \cdot b$ *exits and* $\bigvee A \cdot \bigvee B = \bigvee_{a \in A, b \in B} a \cdot b$*.*
- *for any* $c \in L$*,* $\bigwedge_{a \in A} a \backslash c$ *and* $\bigwedge_{b \in B} c \backslash b$ *exist and* $\bigvee A \backslash c = \bigwedge_{a \in A} a \backslash c$*,* $c \backslash \bigwedge B = \bigwedge_{b \in B} c \backslash b$*.*

Recall that Boolean (Heyting) residuated groupoids NRGs (HRGs) form varieties, which are studied from logic point of view in [5]. Gentzen systems are present for the logics of BRGs and HRGs based on sequents, which are pairs of trees of formulas. Here,

we describe the algebraic version of Gentzen system for BRGs and RRGs by adapting the denotation from [8]. Let **Var** be a set of countably many variables $x_1, x_2, \ldots$ in the languages.

Definition 3. *The set of terms Te is defined inductively as follows:*

$$Te \ni t ::= x \in \mathbf{Var} \mid 1 \mid 0 \mid t \wedge t \mid t \vee t \mid t \to t \mid t \cdot t \mid t \backslash t \mid t / t$$

Define $\neg t = t \to 0$.

Definition 4. *A tree over a finite set of terms is a structure such that all leaves of tree are terms in T and connected by connective* $\cdot$.

Example 3. *Let* $T = \{t_1, t_2, t_3\}$. *Then,* $(t_1 \cdot t_2) \cdot (t_2 \cdot t_3)$ *and* $(t_1 \cdot t_3) \cdot t_1$ *are all trees over T.*

Obviously, all tree are terms. In the following, we use $\overline{t}, \overline{s}, \overline{q}, \ldots$ to denote trees when emphasized.

Definition 5. *A context is a structure generated from a tree* $\overline{t}[-]$ *with a designated position* $[-]$ *that can be filled with a tree. In particular, a single position* $[-]$ *is a context. Let* $\overline{t}[\overline{t'}]$ *be a tree obtained from* $\overline{t}[-]$ *by substituting* $\overline{t'}$ *for* $[-]$.

Example 4. *Let expression* $\overline{t}[-] = (- \cdot \neg t_1) \cdot t_2 \wedge t_3)$ *be a context. If we replace the tree* $\overline{t'} = t_4 \backslash t_5$ *for the position* $-$ *in* $\overline{t}[-]$, *then we obtain the term* $\overline{t}[\overline{t'}] = ((t_4 \backslash t_5) \cdot \neg t_1) \cdot t_2 \wedge t_3$. *If we replace the tree* $t_4 \cdot t_5$ *for the position* $-$ *in* $\overline{t}[-]$, *then we obtain the term* $\overline{t}[\overline{t'}] = ((t_4 \cdot t_5) \cdot \neg t_1) \cdot t_2 \wedge t_3$.

Definition 6. *An algebraic Gentzen system is a finite set* **GS** *of quasi-inequalities in the following form*

$$t_{11} \leq t_{12} \& \ldots \& t_{n1} \leq t_{n2} \Rightarrow t_{01} \leq t_{02}$$

where t_{ij} $0 \leq i, j \leq n$ *are terms.*

Definition 7. *We define* $\mathbf{GS_{HRG}}$ *to be the finite set of quasi-inequalities given in the following*

- $\Rightarrow t \leq t$ *(refl)*
  $\Rightarrow t_1 \wedge (t_2 \vee t_3) \leq (t_1 \wedge t_2) \vee (t_1 \wedge t_3)$ *(dist)*
  $\Rightarrow t \leq 1$ *(g1)*
  $\Rightarrow 0 \leq t$ *(l0)*
- $t_1 \leq t_2 \& \overline{t_3}[t_2] \leq t_4 \Rightarrow \overline{t_3}[t_1] \leq t_4$ *(tran)*
- $t_1 \leq t_2 \& t_3 \leq t_4 \Rightarrow t_1 \cdot t_3 \Rightarrow t_2 \cdot t_4$ *($\cdot R$)*
- $t_1 \leq t_2 \& \overline{t_3}[t_4] \leq t_5 \Rightarrow \overline{t_3}[t_1 \cdot t_2 \backslash t_4] \leq t_5$ *($\backslash L$)*
  $t_1 \cdot t_2 \leq t_3 \Rightarrow t_2 \leq t_1 \backslash t_3$ *($\backslash R$)*
- $t_1 \leq t_2 \& \overline{t_3}[t_4] \leq t_5 \Rightarrow \overline{t_3}[t_4 / t_2 \cdot t_1] \leq t_5$ *($/L$)*
  $t_2 \cdot t_1 \leq t_3 \Rightarrow t_2 \leq t_3 / t_1$ *($/R$)*
- $\overline{t_1}[t_2] \leq t_3 \& \overline{t_1}[t_4] \leq t_3 \Rightarrow \overline{t_1}[t_2 \vee t_4] \leq t_3$ *($\vee L$)*
  $t_1 \leq t_2 \Rightarrow t_1 \leq t_2 \vee t_3$ *($\vee R$)*
  $t_1 \leq t_2 \Rightarrow t_1 \leq t_3 \vee t_2$ *($\vee R$)*
- $\overline{t_1}[t_2] \leq t_3 \Rightarrow \overline{t_1}[t_2 \wedge t_4] \leq t_3$ *($\wedge L$)*
  $\overline{t_1}[t_2] \leq t_3 \Rightarrow \overline{t_1}[t_4 \wedge t_2] \leq t_3$ *($\wedge L$)*
  $t_1 \leq t_2 \& t_1 \leq t_3 \Rightarrow t_1 \leq t_2 \wedge t_3$*($\wedge R$)*
- $t_1 \leq t_2 \& \overline{t_3}[t_4] \leq t_5 \Rightarrow \overline{t_3}[t_1 \wedge t_2 \to t_4] \leq t_5$ *($\to L$)*
  $t_1 \wedge t_2 \leq t_3 \Rightarrow t_2 \leq t_1 \backslash t_3$ *($\to R$)*

  Define $\mathbf{GS_{BRG}} = \mathbf{GS_{HRG}} \cup \{\Rightarrow 1 \leq t \vee \neg t \quad (\mathrm{em})\}$.

Recall that the definitions of rooted trees and Genzten are provable.

Definition 8. *A rooted tree is a poset with a least element, called the root, and, for each element, the set of all elements below it is linearly ordered.*

Definition 9. *A proof-tree in a* **GS** *is a finite rooted tree in which each element is an inequality, which is an instance of a member of* **GS**.

Definition 10. *An inequality $t_1 \leq t_2$ is said to be Gentzen-provable in* **GS** *denoted by $\vdash_{\mathbf{GS}} t_1 \leq t_2$ if there exists a proof-tree in* **GS** *with this inequality as the root.*

Let T be the terms of algebras defined in Definition 2. Write T(W) for the term algebra of term T with variables in the set W. Let $\mu : W \mapsto A$, where A is the carrier domain of an A-algebra. Obviously, μ can be extended to a unique homomorphism $\mu' : T \mapsto H$.

Definition 11. *A* $\mathbf{GS_A}$ *is called sound with respect to all classes of algebra $\mathcal{A}$ if for any inequality $s \leq t$. If $\vdash_{\mathbf{GS_A}} s \leq t$, then, for any $\mathrm{A} \in \mathcal{A}$ with carrier domain A, there is a μ defined as above such that $\mu(s) \leq \mu(t)$ holds in* A.

Definition 12. *A* $\mathbf{GS_A}$ *is called complete with respect to all classes of algebra $\mathcal{A}$ if for any inequality $s \leq t$. If $\nvdash_{\mathbf{GS_A}} s \leq t$, then there is $\mathrm{A} \in \mathcal{A}$ with carrier domain A and a μ defined as above such that $\mu(s) \leq \mu(t)$ fails in* A.

Theorem 1. $\mathbf{GS_{BRG}}$ *and* $\mathbf{GS_{HRG}}$ *are sound and complete with respect to $\mathcal{BRG}$ and $\mathcal{HRG}$.*

The soundness can be shown by proving that all quasi-inequalities are valid in $\mathcal{BRG}$ ($\mathcal{HRG}$). The completeness follows directly from the proof of FMP in the next section. Details of proofs are included in [4,5,11,12].

Definition 13. *Let* VA *be the variety of* **A***-algebras. VA is said to have the finite model property (FMP) if for any $s, t \in T$ there is an* A *and a μ, satisfying that $\mu(s) \leq \mu(t)$ implies $\pi(s) \leq \pi(t)$ for some finite* A′ *and π.*

The FMP can be equivalently defined by the Genzten systems.

Definition 14. *Let* VA *be a variety of* **A***-algebras and* $\mathbf{GS_A}$ *be its corresponding Genzten system. VA is said to have finite model property if for any $s, t \in T \nvdash_{\mathbf{GS_A}} s \leq t$; then, there is an* A *and a μ such that $\mu(s) \leq \mu(t)$ does not hold in* A.

Theorem 2. *The varieties of $\mathcal{BRG}$ and $\mathcal{HRG}$ have FMPs and decidable equational theory.*

3. Bounded Distributive Lattice-Ordered Residuated Groupoid and Semigroup

Definition 15. *A bounded distributive lattice-ordered residuated groupoid (DLRG)* $\mathrm{A} = (A, \cdot, \backslash, /, \wedge, \vee, 1, 0)$ *is a structure where $(A, \wedge, \vee, 0, 1)$ is a bounded distributive lattice and $(A, \cdot, \backslash, /, \leq)$ is a residuated groupoid with lattice ordering $\leq$.*

Proposition 1. *The following equations are satisfied by every DLRG:*

1 $a \cdot (b \vee c) = (a \cdot b) \vee (a \cdot c)$;
2 $a\backslash(b \wedge c) \leq (a\backslash c) \wedge (a\backslash c)$;
3 $(a \wedge b)/c \leq (a/c) \wedge (b/c)$.

The DLRG extensions are DLRGs enriched with unary operation $\neg$ or binary operation $\rightarrow$ satisfying some conditions in the following definition. In the following, we write DLRG$_n$s and DLRG$_i$s, meaning DLRGs enriched with $\neg$ and $\rightarrow$, respectively.

Definition 16. *In a DLRG with carrier domain A, the following conditions are considered for any $a, b, c \in A$:*

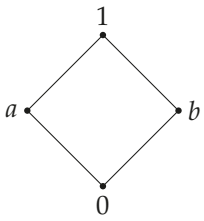
(t) *$a \leq b$ implies $\neg b \leq \neg a$;*
(dn) *$a = \neg\neg a$;*
(ko) *$(a \wedge \neg a) \vee b \leq b \vee \neg b$;*
(k) *$(a \wedge \neg a) \vee b \leq b$;*
(b) *$a \vee \neg a = 1$ & $a \wedge \neg a = 0$;*
(h) *$a \wedge b \leq c$ iff $b \leq a \rightarrow c$.*

Definition 17. *Various extensions of DLRG based on conditions in Definition 16 are listed as follows:*

QBLRG: quasi-Boolean residuated groupoid is DLRG$_n$ s.t. (d), (t), and (dn) hold.
KLRG: Kleene residuated groupoid is QBLRG s.t. (k) holds (this class of algebra is considered in [19]).
KoLRG: Kleene ordered residuated groupoid is QBLRG s.t. (ko) holds (this class of algebra is considered in [20,21]).
BRG: Boolean residuated groupoid is DLRG$_n$ s.t. (b) holds.
HRG: Heyting residuated groupoid is DLRG$_i$ s.t. (d) and (h) hold.

Defining $\cdot, \backslash, /$ similar to Examples 2 and 3 on different lattices, one obtains different examples of the corresponding algebras. Here, we present an example of QBLRG. Others can be treated similarly.

Example 5. *The algebra in Figure 3 is an example of QBLRG. One has $(a \wedge \neg a) \vee b = 1 \not\leq b = b \vee \neg b$, $(a \wedge \neg a) \vee b = 1 \not\leq b$ $a \vee \neg a \neq 1$, and $a \wedge \neg a \neq 0$.*



	$\neg$
1	0
0	1
a	a
b	b

$\cdot$	0	a	b	1
0	0	a	b	1
a	0	a	b	1
b	0	a	a	a
1	0	a	b	1

$/$	0	a	b	1
0	0	0	0	0
a	a	a	1	a
b	b	b	0	b
1	1	1	1	1

$\backslash$	0	a	b	1
0	0	a	b	1
a	0	a	b	1
b	0	1	0	1
1	0	a	b	1

Figure 3. An example of QBLRG.

Definition 18. *We define $\mathbf{GS_{DLRG}}$ to be the finite set of quasi-inequalities given in the following*

- $\Rightarrow t \leq t$ *(refl)*
  $\Rightarrow t_1 \wedge (t_2 \vee t_3) \leq (t_1 \wedge t_2) \vee (t_1 \wedge t_3)$ *(dist)*
  $\Rightarrow t \leq 1$ *(g1)*
  $\Rightarrow 0 \leq t$ *(l0)*
- $t_1 \leq t_2 \& \overline{t_3}[t_2] \leq t_4 \Rightarrow \overline{t_3}[t_1] \leq t_4$ *(tran)*
- $t_1 \leq t_2 \& t_3 \leq t_4 \Rightarrow t_1 \cdot t_3 \Rightarrow t_2 \cdot t_4$ *($\cdot$R)*

- $t_1 \leq t_2 \& \overline{t_3}[t_4] \leq t_5 \Rightarrow \overline{t_3}[t_1 \cdot t_2 \backslash t_4] \leq t_5$ $(\backslash L)$
  $t_1 \cdot t_2 \leq t_3 \Rightarrow t_2 \leq t_1 \backslash t_3$ $(\backslash R)$
- $t_1 \leq t_2 \& \overline{t_3}[t_4] \leq t_5 \Rightarrow \overline{t_3}[t_4 / t_2 \cdot t_1] \leq t_5$ $(/L)$
  $t_2 \cdot t_1 \leq t_3 \Rightarrow t_2 \leq t_3 / t_1$ $(/R)$
- $\overline{t_1}[t_2] \leq t_3 \& \overline{t_1}[t_4] \leq t_3 \Rightarrow \overline{t_1}[t_2 \vee t_4] \leq t_3$ $(\vee L)$
  $t_1 \leq t_2 \Rightarrow t_1 \leq t_2 \vee t_3$ $(\vee R)$
  $t_1 \leq t_2 \Rightarrow t_1 \leq t_3 \vee t_2$ $(\vee R)$
- $\overline{t_1}[t_2] \leq t_3 \Rightarrow \overline{t_1}[t_2 \wedge t_4] \leq t_3$ $(\wedge L)$
  $\overline{t_1}[t_2] \leq t_3 \Rightarrow \overline{t_1}[t_4 \wedge t_2] \leq t_3$ $(\wedge L)$
  $t_1 \leq t_2 \& t_1 \leq t_3 \Rightarrow t_1 \leq t_2 \wedge t_3 (\wedge R)$

Obviously, $\mathbf{GS_{DLRG}} \cup \{(\rightarrow \text{ L}), (\rightarrow \text{ R})\} = \mathbf{GS_{HRG}}$. *Define* $\mathbf{GS_{QBLRG}}$, $\mathbf{GS_{KLRG}}$, $\mathbf{GS_{KoLRG}}$ *as follows:*

- $\mathbf{GS_{QBLRG}} = \mathbf{GS_{DLRG}} \cup \{s \leq t \Rightarrow \neg t \leq \neg s (trpo), \quad \neg\neg s = s (doubn)\}$;
- $\mathbf{GS_{KLRG}} = \mathbf{GS_{QBLRG}} \cup \{\Rightarrow (s \wedge \neg s) \vee t \leq t (kleene)\}$;
- $\mathbf{GS_{KoLRG}} = \mathbf{GS_{QBLRG}} \cup \{(s \wedge \neg s) \vee t \leq t \vee \neg t (kleeno)\}$.

Definition 19. *A residuated semigroup (RSG)* G $(G, \cdot, \backslash, /, \leq)$ *is a structure such that* $(G, \cdot)$ *is a semigroup and* $\cdot, \backslash, /$ *are binary operations on* G *satisfying (res).*

Definition 20. *A commutative and contractive residuated semigroup (RSG)* G $(G, \cdot, \backslash, /, \leq)$ *is an RSG such that* $\cdot$*, satisfying the following*

- *(com)* $a \cdot b = b \cdot a$;
- *(con)* $a \cdot a = a$.

for any $a, b \in G$.

Definition 21. *An associative, commutative, and contractive residuated quasi-Boolean algebra* G $(G, \cdot, \backslash, /, \wedge, \vee, \neg)$ *such that* $(G, \wedge, \vee, \neg)$ *is a quasi-Boolean algebra and* $(G, \cdot, \backslash, /, \leq)$ *is a commutative and contractive residuated semigroup where* $\leq$ *is the lattice order. If* $(G, \wedge, \vee, \neg)$ *is Kleene (order) or Boolean algebra, then* G *is an associative, commutative and contractive residuated Kleene (order) or Boolean algebra.*

Proposition 2. *The following equation are satisfied by every associative, commutative, and contractive residuated quasi-Boolean algebra.*

1 $a \cdot (b \rightarrow_\# c) \leq (a \cdot b) \rightarrow_\# c$;
2 $a \rightarrow_\# b \leq (a \cdot c) \rightarrow_\# (b \cdot c)$;
3 $(a \rightarrow_\# b) \cdot (b \rightarrow_\# c) \leq (a \rightarrow_\# c)$;
4 $a \rightarrow_\# (b \cdot c) \leq (a \rightarrow_\# c) \rightarrow_\# b$;
5 $(a \rightarrow_\# c) \rightarrow_\# b \leq a \rightarrow_\# (b \cdot c)$;
6 $(a \rightarrow_\# a) \cdot a \leq a$;
7 $a \leq (a \rightarrow_\# a) \cdot a$;
8 $a \rightarrow_\# (b \wedge c) \leq (a \rightarrow_\# b) \wedge (a \rightarrow_\# c)$;
9 $(a \rightarrow_\# b) \wedge (a \rightarrow_\# c) \leq a \rightarrow_\# (b \wedge c)$;
10 $a \rightarrow_\# (b \rightarrow_\# c) \leq b \rightarrow_\# (a \rightarrow_\# c)$;
11 $b \rightarrow_\# (a \rightarrow_\# c) \leq a \rightarrow_\# (b \rightarrow_\# c)$;
12 $a \rightarrow_\# (a \rightarrow_\# b) \leq a \rightarrow_\# b$;
13 $a \rightarrow_\# b \leq a \rightarrow_\# (a \rightarrow_\# b)$.

The proof refers to Proposition 1.4.4 in [8] and Lemma 11.

Let $\mathcal{CC}xRA$, where $x \in \{\mathcal{QB}, \mathcal{K}, \mathcal{K}o, \mathcal{B}\}$ are the classes of associative, commutative, and contractive residuated x algebras. Since the commutative holds in $\mathcal{CC}x\mathcal{RG}$, $a \backslash b = a / b$

for any $a, b \in G$, in the following, we write $\rightarrow_{\#}$, and we mean $\backslash$ and $/$. and recall the definition of terms.

Definition 22. *The set of terms Te are defined inductively as follows:*

$$Te \ni t ::= x \in \mathbf{Var} \mid 1 \mid 0 \mid t \wedge t \mid \neg t \mid t \cdot t \mid t \rightarrow_{\#} t$$

Define $t \vee t = \neg(\neg t \wedge \neg t)$.

Definition 23. *We define* $\mathbf{GS_{CCQBRA}}$ *to be the finite set of quasi-inequalities s.t.* $\mathbf{GS_L} \cup \{(t), (dn)\} \subseteq \mathbf{GS_{AL}}$ *and the following*

- $\overline{t_1}[\overline{t_2} \cdot \overline{t_3}] \leq t_4 \Leftrightarrow \overline{t_1}[\overline{t_2} \cdot \overline{t_3}] \leq t_4$ *(com);*
- $\overline{t_1}[\overline{t_2}] \leq t_3 \Leftrightarrow \overline{t_1}[\overline{t_2} \cdot \overline{t_2}] \leq t_3$ *(con);*
- $\overline{t_1}[(\overline{t_2} \cdot \overline{t_3}) \cdot \overline{t_4}] \leq t_5 \Leftrightarrow \overline{t_1}[\overline{t_2} \cdot (\overline{t_3} \cdot \overline{t_4})] \leq t_5$ *(ass).*

Define $\mathbf{GS_{CCKRA}} = \mathbf{GS_{CCQBRA}} \cup \{(kln)\}$, $\mathbf{GS_{CCKoRA}} = \mathbf{GS_{CCQBRA}} \cup \{(klno)\}$, *and* $\mathbf{GS_{CCBRA}} = \mathbf{GS_{CCQBRA}} \cup \{(em), \Rightarrow a \wedge \neg a = 1(lc)\}$

Let $\mathbf{GS} \in \{\mathbf{GS_{DLRG}}, \mathbf{GS_{QBRG}}, \mathbf{GS_{KRG}}, \mathbf{GS_{KoRG}}, \mathbf{GS_{CCQBRA}}, \mathbf{GS_{CCKRA}}, \mathbf{GS_{CCKoRA}}, \mathbf{GS_{CCBRA}}\}$, and $\mathcal{A}_{\mathcal{GS}}$ be the classes of its corresponding algebras.

Proposition 3. $\vdash_{\mathbf{GS}} t \cdot s \leq q$ *iff* $\vdash_{\mathbf{GS}} t \leq s \rightarrow_{\#} q$ *iff* $\vdash_{\mathbf{GS}} s \leq t \rightarrow_{\#} q$.

Theorem 3. $\mathbf{GS}$ *is sound and complete with respect to* $\mathcal{A}_{\mathcal{GS}}$.

The soundness can be shown by proving that all quasi-inequalities are valid in $\mathcal{A}_{\mathcal{GS}}$. The completeness follows directly from the proof of FMP in the next section.

4. Finite Model Property and Decidability

In this section, we show the FMPs of all algebras considered in Sections 2 and 3. Let $\mathbf{LG} \in \{\mathbf{GS_{DLRG}}, \mathbf{GS_{QBRG}}, \mathbf{GS_{KRG}}, \mathbf{GS_{KoRG}}, \mathbf{GS_{HRG}}, \mathbf{GS_{BRG}}\}$. In the following, we always assume that T is a finite set of terms and $\{1, 0\} \subseteq T$. Define $\neg T = \{\neg t | t \in T\}$, $d(T)$ as the $\wedge, \vee$ closure of T and $d'(T)$ as the $\wedge, \vee, \neg$ closure of T. Let T^* be $d(T)$ when $\mathbf{LG} \in \{\mathbf{GS_{DLRG}}, \mathbf{GS_{HRG}}\}$. Otherwise, $T^* = d'(T)$. Let $T^!$ be the set of trees over T^*.

Definition 24. *We define* $\leq_{\mathcal{T}}$ *on* $T^!$ *as follows: for* $\overline{t_1}, \overline{t_2} \in T^!$, $\overline{t_1} \leq_{\mathcal{T}} \overline{t_2}$ *iff for term* $s \in T^*$, *if* $\vdash_{\mathbf{LG}} \overline{t_2} \leq s \Rightarrow \overline{t_1} \leq s$.

Let $\overline{t_1} \approx_{\mathcal{T}} \overline{t_2}$ be $\overline{t_1} \leq_{\mathcal{T}} \overline{t_2}$ and $\overline{t_2} \leq_{\mathcal{T}} \overline{t_1}$, and then $\approx_{\mathcal{T}}$ is an equivalence relation. Let $[s]_{\mathcal{T}} = \{\bar{t} \mid s \approx_{\mathcal{T}} \bar{t} \ \& \bar{t} \in T^!\}$ for any $s \in T^*$. Let $[T^*] = \{[s]_{\mathcal{T}} \mid s \in T^*\}$.

Definition 25. *A term t is called a disjunction normal form with respect to the set of terms T if it is the disjunction of conjunction of some terms in* $T \cup \neg T$.

Since distributive of lattices and the De Morgan properties are always assumed here, for any $s \in T^*$, there is a term $dnf_{\mathcal{T}}(s)$ in disjunction normal form such that $s \approx_{\mathcal{T}} dnf_{\mathcal{T}}(s)$. Clearly, $\{dnf_{\mathcal{T}}(s) | s \in T^*\}$ is finite since T is finite. Due to $[s]_{\mathcal{T}} = [dnf_{\mathcal{T}}(s)]_{\mathcal{T}}$ and the number of $[dnf_{\mathcal{T}}(s)]_{\mathcal{T}}$ is finite, $[T^*]$ is finite.

Lemma 3. *For any* $\bar{t} \in T^!$, *there is a* $s \in dnf(T^*)$ *such that* $\bar{t} \approx_{\mathcal{T}} s$.

Proof. Let $s = \bigwedge\{dnf_{\mathcal{T}}(s_i) | \vdash_{\mathbf{LG}} \bar{t} \leq s_i, s_i \in T^*\}$. Assume that $\vdash_{\mathbf{LG}} \bar{t} \leq s'$ for some $s' \in T^*$. Then, there is an i such that $s_i = s'$. Clearly, $\vdash_{\mathbf{LG}} s \leq s'$. Thus, $s \leq_{\mathcal{T}} \bar{t}$. In the opposite

direction, since $\vdash_{\mathbf{LG}} \bar{t} \leq s_i$, by ($\wedge$R), one obtains $\vdash_{\mathbf{LG}} \bar{t} \leq s$. Suppose that $\vdash_{\mathbf{LG}} s \leq q$ for some $q \in T^*$. By applying (tran) to $\vdash_{\mathbf{LG}} s \leq q$ and $\vdash_{\mathbf{LG}} t \leq s$, one obtains $\vdash_{\mathbf{LG}} t \leq q$. Thus, $t \leq_{\mathcal{T}} s$. $\square$

Remark 1. *Note that, for any $t \in T^!$, $\vdash_{\mathbf{LG}} t \leq 1$. Thus, $\{dnf_{\mathcal{T}}(s_i) | \vdash_{\mathbf{LG}} t \leq s_i, s_i \in T^*\}$ is not empty. Further, this set is finite. Hence, s always exists. If one considers the algebras without the greatest element 1, for instance* **rg***s or* **dlrg***s as in [5], then one needs more complex set of theoretic construction with the help of closure operator and interpolant proof theory, as in the result in [5].*

Definition 26. *Let $\mathcal{Q} = ([T^*], \wedge^*, \vee^*, \neg^*, \cdot^*, \backslash^*, /^*, 0^*, 1^*)$ be the quotient algebra of $[T^*]$, where all operations are defined as follows: for any $[s]_{\mathcal{T}}, [q]_{\mathcal{T}} \in [T^*]$,*

(1) $1^* = [1]_{\mathcal{T}}$;
(2) $0^* = [0]_{\mathcal{T}}$;
(3) $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} = [s \wedge q]_{\mathcal{T}}$;
(4) $[s]_{\mathcal{T}} \vee^* [q]_{\mathcal{T}} = [s \vee q]_{\mathcal{T}}$;
(5) $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} = [w]_{\mathcal{T}}$ *s.t.* $w \approx_{\mathcal{T}} s \cdot q$;
(6) $[s]_{\mathcal{T}} \backslash^* [q]_{\mathcal{T}} = [w_1 \vee \ldots \vee w_n]_{\mathcal{T}}$ *s.t.* $[s]_{\mathcal{T}} \cdot^* [w_i]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$ *for any* $i \in \{1, \ldots, n\}$;
(7) $[s]_{\mathcal{T}} /^* [q]_{\mathcal{T}} = [w_1 \vee \ldots \vee w_n]_{\mathcal{T}}$ *s.t.* $[w_i]_{\mathcal{T}} \cdot^* [s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$ *for any* $i \in \{1, \ldots, n\}$;
(8) $\neg^* [s]_{\mathcal{T}} = [\neg s]_{\mathcal{T}}$;

We define $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$ as $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} = [s]_{\mathcal{T}}$.

If $\mathbf{LG} = \mathbf{GS_{DLRG}}$, then $\mathcal{Q}$ is constructured as in 26 by excluding item (8).

Definition 27. *Let $\mathcal{Q} = ([T^*], \wedge^*, \vee^*, \rightarrow^*, \cdot^*, \backslash^*, /^*, 0^*, 1^*)$ be the quotient algebra of $[T^*]$, where all operations except $\rightarrow^*$ and $\leq^*$ are defined as in Definition 26 and $\rightarrow^*$ is defined as follows.*

(9) $[s]_{\mathcal{T}} \rightarrow^* [q]_{\mathcal{T}} = [w_1 \vee \ldots \vee w_n]_{\mathcal{T}}$ *s.t.* $[s]_{\mathcal{T}} \wedge^* [w_i]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$ *for any* $i \in \{1, \ldots, n\}$;

Lemma 4. *The following conditions are equivalent for all $s, q \in T^*$:*

(1) $s \leq_{\mathcal{T}} q$;
(2) $\vdash_{\mathbf{LG}} s \leq q$;
(3) $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$

Proof. Let us show (1) implies (2). Let $s \leq_{\mathcal{T}} q$. By (relf), $\vdash_{\mathbf{LG}} q \leq q$. Thus, by Definition 24, one obtains $\vdash_{\mathbf{LG}} s \leq q$.

Let us show (2) implies (3). It suffices to prove $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} = [s]_{\mathcal{T}}$. By Definition 26. $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} = [s \wedge q]_{\mathcal{T}}$. Assume that $\vdash_{\mathbf{LG}} s \leq q$. Clearly, by (relf) $\vdash_{\mathbf{LG}} s \leq s$. By ($\wedge$ R), one obtains $\vdash_{\mathbf{LG}} s \leq s \wedge q$. Obviously, $s \leq_{\mathcal{T}} s \wedge q$. Conversely, $\vdash_{\mathbf{LG}} s \wedge q \leq s$. Thus, $s \wedge q \leq_{\mathcal{T}} s$. Therefore, $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$.

Let us show (3) implies (1). Assume that $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$. Thus, $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} = [s \wedge q]_{\mathcal{T}} = [s]_{\mathcal{T}}$. Thus, $s \wedge q \approx_{\mathcal{T}} s$. Therefore, $s \leq_{\mathcal{T}} s \wedge q$. Thus, $\vdash_{\mathbf{LG}} s \leq s \wedge q$. Clearly, $\vdash_{\mathbf{LG}} s \wedge q \leq q$. By (trans), $\vdash_{\mathbf{LG}} s \leq q$. Let $\vdash_{\mathbf{LG}} q \leq w$ for some $w \in T^*$. Thus, by (trans), $\vdash_{\mathbf{LG}} s \leq w$. Hence, $s \leq_{\mathcal{T}} q$. $\square$

Lemma 5. *All the operations defined in Definition 26 are well defined.*

Proof. $\wedge, \vee$ (or $\wedge, \vee, \neg$) are well defined since T^* is closed under these operations. We provide the proof for operation $\cdot$. Then, by the functional definition, $\backslash$, / ($\rightarrow$) are all well defined. Let $[s]_{\mathcal{T}} = [q]_{\mathcal{T}}$. It suffices to show $[w]_{\mathcal{T}} \cdot^* [s]_{\mathcal{T}} = [w]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}}$. Let $[w]_{\mathcal{T}} \cdot^* [s]_{\mathcal{T}} = [w_1]$ s.t. $w_1 \approx_{\mathcal{T}} w \cdot s$ and $[w]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} = [w_1]$ s.t. $w_2 \approx_{\mathcal{T}} w \cdot q$. Obviously, $\vdash_{\mathbf{LG}} w_1 \leq w_1$. Then, by Definition 24, $\vdash_{\mathbf{LG}} w \cdot s \leq w_1$. Clearly, $\vdash_{\mathbf{LG}} q \leq s$. Thus, by (trans), $\vdash_{\mathbf{LG}} w \cdot q \leq w_1$. Then, by by Definition 24, $\vdash_{\mathbf{LG}} w_2 \leq w_1$. So, by Lemma 4, $[w_1]_{\mathcal{T}} \leq^* [w_2]_{\mathcal{T}}$. Similarly,

one proves $[w_2]_{\mathcal{T}} \leq^* [w_1]_{\mathcal{T}}$. Thus, $[w]_{\mathcal{T}} \cdot^* [s]_{\mathcal{T}} = [w]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}}$. Similarly, $[s]_{\mathcal{T}} \cdot^* [w]_{\mathcal{T}} = [q]_{\mathcal{T}} \cdot^* [w]_{\mathcal{T}}$ Hence, $\cdot$ is well defined. □

Lemma 6. *For any* $[s]_{\mathcal{T}}, [q]_{T^*}, [w]_{\mathcal{T}} \in [T^*]$ *in* $\mathcal{Q}$ *according to Definitions 26 and 27,* $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$ *iff* $[q]_{\mathcal{T}} \leq^* [s]_{\mathcal{T}} \backslash^* [w]_{\mathcal{T}}$ *iff* $[s]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}} /h^* [q]_{\mathcal{T}}$.

Proof. Let us show $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$ implies $[q]_{\mathcal{T}} \leq^* [s]_{\mathcal{T}} \backslash^* [w]_{\mathcal{T}}$. Let $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} = [r]_{\mathcal{T}}$ and $[s]_{\mathcal{T}} \backslash^* [w]_{\mathcal{T}} = [u]_{\mathcal{T}} = [\bigvee \{dnf_{\mathcal{T}}(u_i) | [s]_{\mathcal{T}} \cdot^* [u_i]_{\mathcal{T}} \leq [w]_{\mathcal{T}}\}]_{\mathcal{T}}$. Assume that $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$. Then, there is a u_i such that $u_i = q$. Then, by (refl) and ($\vee$R), $\vdash_{\mathbf{LG}} q \leq u$. Thus, by Lemma 4, $[q]_{\mathcal{T}} \leq [u]_{\mathcal{T}}$. Therefore, $[q]_{\mathcal{T}} \leq^* [s]_{\mathcal{T}} \backslash^* [w]_{\mathcal{T}}$.

Let us show the opposite direction. Assume that $[q]_{\mathcal{T}} \leq^* [s]_{\mathcal{T}} \backslash^* [w]_{\mathcal{T}}$. By Lemma 4, $\vdash_{\mathbf{LG}} q \leq u$ Thus, $\vdash_{\mathbf{LG}} s \cdot u_i \leq w$. So, $\vdash_{\mathbf{LG}} s \cdot dnf_{\mathcal{T}}(u_i) \leq w$. By ($\vee$L), $\vdash_{\mathbf{LG}} s \cdot u \leq w$. Hence, by (trans), $\vdash_{\mathbf{LG}} s \cdot q \leq w$. Hence, $\vdash_{\mathbf{LG}} r \leq w$. So, $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$.

Similarly, one proves $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$ iff $[s]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}} /h^* [q]_{\mathcal{T}}$. □

Corollary 2. *For any* $[s]_{\mathcal{T}}, [q]_{\mathcal{T}}, [w]_{\mathcal{T}} \in [T^*]$ *in* $\mathcal{Q}$ *according to Definition 27,* $[s]_{\mathcal{T}} \wedge^* [q]_{\mathcal{T}} \leq^* [w]_{\mathcal{T}}$ *iff* $[q]_{\mathcal{T}} \leq^* [s]_{\mathcal{T}} \rightarrow^* [w]_{\mathcal{T}}$.

Lemma 7. *For any* $[s]_{\mathcal{T}}, [q]_{\mathcal{T}}, [w]_{\mathcal{T}} \in [T^*]$, *the following hold*

(1) $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$ *implies* $\neg [q]_{\mathcal{T}} \leq^* \neg [s]_{\mathcal{T}}$ *if* **LG** *contains (QB);*
(2) $[s]_{\mathcal{T}} =^* \neg^* \neg^* [s]_{\mathcal{T}}$ *if* **LG** *contains (QB);*
(3) $([s]_{\mathcal{T}} \wedge^* \neg^* [s]_{\mathcal{T}}) \vee^* [q]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}} \vee^* \neg^* [q]_{\mathcal{T}}$ *if* **LG** *contains (Ko);*
(4) $([s]_{\mathcal{T}} \wedge^* \neg^* [s]_{\mathcal{T}}) \vee^* b \leq^* b$ *if* **LG** *contains (K);*
(5) $[s]_{\mathcal{T}} \vee^* \neg^* [s]_{\mathcal{T}} =^* 1^*$ & $[s]_{\mathcal{T}} \wedge^* \neg^* [s]_{\mathcal{T}} = 0^*$ *if* **LG** *contains (B).*

Proof. We only provide the details for (1). Others can be proved similarly. Assume that $[s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$. By Lemma 4, $\vdash_{\mathbf{LG}} s \leq q$. Then, by (QB), one obtains $\vdash_{\mathbf{LG}} \neg q \leq \neg s$. Again, by Lemma 4, $\neg [q]_{\mathcal{T}} \leq^* \neg [s]_{\mathcal{T}}$. □

Lemma 8. $\mathcal{Q}$ *is a finite iRG where* $i \in \{DL, QB, K, Ko, B, H\}$ *if* **LG** *contains (i) axioms.*

Proof. Immediately follows from Lemmas 6 and 7 and Corollary 2. □

Lemma 9. *The following conditions hold for* $\mathcal{Q}$*: for any* $s, q \in T$,

(1) *If* $s \cdot q \in \mathcal{T}$, *then* $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} = [s \cdot q]_{\mathcal{T}}$.
(2) *If* $s \backslash q \in \mathcal{T}$, *then* $[s]_{\mathcal{T}} \backslash^* [q]_{\mathcal{T}} = [s \backslash q]_{\mathcal{T}}$.
(3) *If* $s / q \in \mathcal{T}$, *then* $[s]_{\mathcal{T}} /^* [q]_{\mathcal{T}} = [s / q]_{\mathcal{T}}$.
(4) *If* $s \rightarrow q \in \mathcal{T}$, *then* $[s]_{\mathcal{T}} \rightarrow^* [q]_{\mathcal{T}} = [s \rightarrow q]_{\mathcal{T}}$.

Proof. Let us show (1). Let $[s]_{\mathcal{T}} \cdot^* [q]_{\mathcal{T}} = [w]_{\mathcal{T}}$. Then, $w \approx_{\mathcal{T}} s \cdot q$. Thus, $\vdash_{\mathbf{LG}} w \leq s \cdot q$ and $\vdash_{\mathbf{LG}} s \cdot q \leq w$. By Lemma 4, $[w]_{\mathcal{T}} = [s \cdot q]_{\mathcal{T}}$.

Let us show (2). Let $[s]_{\mathcal{T}} \backslash^* [q]_{\mathcal{T}} = [w]_{\mathcal{T}}$. Let $w = \bigvee \{w_i | \vdash_{\mathbf{LG}} s \cdot w_i \leq q\}$. By ($\vee$L), one obtains $\vdash_{\mathbf{LG}} s \cdot w \leq q$. Thus, (\R) $\vdash_{\mathbf{LG}} w \leq s \backslash q$. Furthermore, $\vdash_{\mathbf{LG}} s \cdot s \backslash \leq q$. Thus, there is a $w_i = s \backslash q$ for some i. So, $\vdash_{\mathbf{LG}} s \backslash q \leq w$. □

Lemma 10. *Let* T^* *be set of terms generated from* s, q *in Definition 22. If* $\nvdash_{\mathbf{LG}} s \leq q$, *then there is* $\mathcal{A}_{\mathcal{LG}}$ $\mathcal{Q}$ *and an assignment* σ, *satisfying that* $\not\models_{\mathcal{Q}} [s]_{\mathcal{T}} \leq^* [q]_{\mathcal{T}}$.

Proof. Recall that T is the smallest set containing all the terms in $Sub(s) \cup Sub(q) \cup \{0, 1\}$. Let T^* be defined as above. Clearly, T^* is finitely based. Assume that $\nvdash_{\mathbf{LG}} s \leq q$. Construct $\mathcal{Q}$ as in Definition 26 or Definition 27 with respect to **LG**. Let $\sigma : \mathbf{Var}(T) \mapsto [T^*]$ such that

$\sigma(p) = [p]_{\mathcal{T}}$. σ can be simply extended to $\hat{\sigma}$ satisfying that $\hat{\sigma}(w) = [w]_{\mathcal{T}}$ for any $w \in T^*$. Assume that $\sigma\hat{(}s) \leq \sigma\hat{(}q)$. Then, $[s]_{\mathcal{T}} \leq [q]_{\mathcal{T}}$. By Lemma 4 and Lemma 16, one obtains $\vdash_{\mathbf{LG}} s \leq q$, which yields contradiction. □

Theorem 4 (FMP and Decidability)**.** LG *has FMP and thus is decidable.*

Proof. Suppose $\nvdash_{\mathsf{LG}} s \leq t$ By Lemma 10, there is a finite counter-algebra $\mathcal{Q}$ such that $\not\models_{\mathcal{Q}} s \leq t$. Thus, $\not\models_{\mathbf{A_{LG}}} s \Rightarrow t$. □

Remark 2. *The proof result can be extended to the Galois connection extensions of distributive lattices, De Morgan algebras, Heyting algebras, and Boolean algebras. The Galois operators are a pair of modal operators denoted by* $\Diamond, \Box$ *that usually satisfy the following properties.*

- $\Diamond a \leq b$ *iff* $a \leq \Box b$ *(gs)*

A pair of Galois connection operators are essentially a unary version of fusion $\cdot$ *and its residual duals* $\backslash, /$*. However, if we consider more complex algebraic structures, such as requiring the modal operators to satisfy transitivity like the 4 axiom, then the construction presented here will not hold, and more sophisticated constructions and analytical proofs will be necessary.*

Let $\mathbf{AG} \in \{\mathbf{GS_{CCQBRA}}, \mathbf{GS_{CCKRA}}, \mathbf{GS_{CCKoRA}}, \mathbf{GS_{CCBRA}}\}$. Define T be a set of finite terms containing $\{0, 1\}$. Let $c(T)$ be the $\wedge$ $\rightarrow_{\#}$ closure of T. Let T' be the $\wedge, \neg$ closure of $c(T)$ and $T^?$ be the set of trees over T'.

Lemma 11. *The following hold in* **AG***:*

(1) $\vdash_{\mathbf{AG}} s \cdot t_1 \leq q \& s \cdot t_2 \leq q \Rightarrow s \cdot t_1 \vee t_2 \leq q$;
(2) $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \wedge q) = (s \rightarrow_{\#} t) \wedge (s \rightarrow_{\#} q)$;
(3) $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \rightarrow_{\#} q) = t \rightarrow_{\#} (s \rightarrow_{\#} q)$;
(4) $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (s \rightarrow_{\#} t) = s \rightarrow_{\#} t$.

Proof. Let us show (1). Let $\vdash_{\mathbf{AG}} s \cdot t_1 \leq q$ and $\vdash_{\mathbf{AG}} s \cdot t_2 \leq q$. By $(\rightarrow_{\#})$, $\vdash_{\mathbf{AG}} t_i \leq s \rightarrow_{\#} q$. By (trpo), $\vdash_{\mathbf{AG}} \neg(s \rightarrow_{\#} q) \leq \neg t_1$ and $\vdash_{\mathbf{AG}} \neg(s \rightarrow_{\#} q) \leq \neg t_2$. By ($\wedge$R), $\vdash_{\mathbf{AG}} \neg(s \rightarrow_{\#} q) \leq \neg t_1 \wedge \neg t_2$. By (trpo) (doubn) and (trans), $\vdash_{\mathbf{AG}} \neg(\neg t_1 \wedge \neg t_2) \leq s \rightarrow_{\#} q$. Thus, $\vdash_{\mathbf{AG}} s \cdot \neg(\neg t_1 \wedge \neg t_2) \leq q$, whence $\vdash_{\mathbf{AG}} s \cdot t_1 \vee t_2 \leq q$.

Let us show (2). Obviously, $\vdash_{\mathbf{AG}} \Rightarrow s \leq s$ and $\vdash_{\mathbf{AG}} t \wedge q \leq q$. By $(\rightarrow_{\#}\mathrm{L})$, $\vdash_{\mathbf{AG}} \Rightarrow s \cdot s \rightarrow_{\#} (t \wedge q) \leq q$. Hence, $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \wedge q) \leq (s \rightarrow_{\#} q)$. Similarly, $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \wedge q) \leq (s \rightarrow_{\#} q)$. By ($\wedge$R), $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \wedge q) \leq (s \rightarrow_{\#} t) \wedge (s \rightarrow_{\#} q)$. For the other direction, clearly $\vdash_{\mathbf{AG}} \Rightarrow s \cdot s \rightarrow_{\#} t \leq t$ and $\vdash_{\mathbf{AG}} \Rightarrow s \cdot s \rightarrow_{\#} q \leq q$. By ($\wedge$R) $\vdash_{\mathbf{AG}} \Rightarrow s \cdot (s \rightarrow_{\#} t) \wedge (s \rightarrow_{\#} q) \leq t \wedge q$. Hence, $\vdash_{\mathbf{AG}} \Rightarrow (s \rightarrow_{\#} t) \wedge (s \rightarrow_{\#} q) \leq s \rightarrow_{\#} (t \wedge q)$.

Let us show (3). Obviously, $\vdash_{\mathbf{AG}} q \leq q$. Then, by $(\rightarrow_{\#} L)$ twice, $\vdash_{\mathbf{AG}} s \cdot t \cdot s \rightarrow_{\#} (t \rightarrow_{\#} q) \leq q$. By (com), one obtains $\vdash_{\mathbf{AG}} t \cdot s \cdot s \rightarrow_{\#} (t \rightarrow_{\#} q) \leq q$. Therefore, by $(\rightarrow_{\#}\mathrm{R})$ twice, one obtains $\vdash_{\mathbf{AG}} \Rightarrow s \rightarrow_{\#} (t \rightarrow_{\#} q) \leq t \rightarrow_{\#} (s \rightarrow_{\#} q)$. The opposite direction can be proved similarly.

Let us show (4). Obviously, $\vdash_{\mathbf{AG}} t \leq t$. Then, by $(\rightarrow_{\#} L)$ twice, $\vdash_{\mathbf{AG}} s \cdot s \cdot s \rightarrow_{\#} (s \rightarrow_{\#} t) \leq t$. Then, by (con), one obtains $\vdash_{\mathbf{AG}} s \cdot s \rightarrow_{\#} (s \rightarrow_{\#} t) \leq t$. Then, by $(\rightarrow_{\#})$, one obtains $\vdash_{\mathbf{AG}} s \rightarrow_{\#} (s \rightarrow_{\#} t) \leq s \rightarrow_{\#} t$. For the opposite direction, since $\vdash_{\mathbf{AG}} t \leq t$, by $(\rightarrow_{\#})$ $\vdash_{\mathbf{AG}} s \cdot s \rightarrow_{\#} t \leq t$. By (con), $\vdash_{\mathbf{AG}} s \cdot s \cdot s \rightarrow_{\#} t \leq t$. By $(\rightarrow_{\#}\mathrm{R})$ twice, $\vdash_{\mathbf{AG}} s \rightarrow_{\#} t \leq s \rightarrow_{\#} (s \rightarrow_{\#} t)$. □

Lemma 12. *For any* $\overline{t_1}, \overline{t_2} \in T^?$ *and* $s \in T'$ *if* $\vdash_{\mathbf{AG}} \overline{t_1} \cdot \overline{t_2} \leq s$*, then there is a* $w \in c(T)$ *such that* $\vdash_{\mathbf{AG}} \overline{t_1} \cdot \overline{t_2} \leq w$ *and* $\vdash_{\mathbf{AG}} w \leq s$

Proof. We proceed the proof by induction on the derivation in **AG**. Let $\overline{t_1} \cdot \overline{t_2} \leq s$ be the ended inequalities obtained by rule (R). Assume that $\overline{t_1} \cdot \overline{t_2}$ is not introduced by (R). Then, the claim holds by induction hypothesis. For instance, suppose that $\overline{t_1} \cdot \overline{t_2} \leq s$ is obtained by $\overline{t_1} \cdot \overline{t_2} \leq q$ and $q \leq s$ by (trans). Then, by induction hypothesis, there is a $w \in c(T)$ s.t. $\overline{t_1} \cdot \overline{t_2} \leq w$ and $w \leq q$. By (trans), $w \leq s$. Thus, w is the required term for $\overline{t_1} \cdot \overline{t_2}$.

Assume that $\overline{t_1} \cdot \overline{t_2}$ is introduced by (R). If (R) is (·R), then $s = s_1 \cdot s_2$ for some s_1, s_2. Clearly, $s \in T'$. So, $s \in c(T)$. Hence, s is the required term for $\overline{t_1} \cdot \overline{t_2}$. Otherwise, suppose that $\overline{t_1} \cdot \overline{t_2} \leq s$ is obtained by $\overline{t_1} \cdot q \leq s$ and $\overline{t_2} \leq q$ by (trans). Then, by induction hypothesis, there is a $w \in c(T)$ s.t. $\overline{t_1} \cdot q \leq w$ and $w \leq s$. Hence, by (trans), $\overline{t_1} \cdot \overline{t_2} \leq w$. So, w is the required term for $\overline{t_1} \cdot \overline{t_2}$. □

According to Lemma 11, by omitting repetitions, $c(T)$ is finite up to equivalent in **AG** when T is finite. $\leq_{T'}$ and $\approx_{T'}$ are defined similarly as in Definition 24 with respect to **AG**. $[s]_{T'}$ for some $s \in T'$; [c(T)] and $[T']$ are defined naturally. Since quasi-Boolean of lattice is assumed, then $\wedge, \neg$ closure of terms is finite up to equivalent. Thus, both $[c(T)]$ and $[T']$ are finite.

Lemma 13. *For any $\overline{t_1} \cdot \overline{t_2} \in T^?$, there is $s \in c(T)$ such that $\overline{t} \approx_T s$.*

Let $\mathcal{Q}' = ([T'], \wedge', \neg', \cdot', \to'_\#, 0', 1')$ be the quotient algebra of $[T']$ and $\leq'$ defined as in Definition 26.

Lemma 14. *The following conditions are equivalent for all $s, q \in T^*$:*

(1) $s \leq_{T'} q$;
(2) $\vdash_{\mathbf{AG}} s \leq q$;
(3) $[s]_{T'} \leq' [q]_{T'}$

The proof is quite similar to Lemma 4. Consequently, all operations in $\mathcal{Q}'$ are well defined. Define $[s]_T \vee' [t]_T = \neg'(\neg'[s]_T \wedge' \neg'[t]_T)$.

Lemma 15. *For any $[s]_{T'}, [q]_{T'}, [w]_{T'} \in [T']$ in $\mathcal{Q}'$, the following hold:*

(1) $[s]_{T'} \cdot' [q]_{T'} \leq' [w]_{T'}$ *iff* $[q]_{T'} \leq' [s]_{T'} \to'_\# [w]_{T'}$;
(2) $[s]_{T'} \leq' [q]_{T'}$ *implies* $\neg'[q]_{T'} \leq' \neg'[s]_{T'}$;
(3) $[s]_{T'} =^* \neg'\neg'[s]_{T'}$;
(4) $([s]_{T'} \wedge' \neg'[s]_{T'}) \vee' [q]_{T'} \leq' [q]_{T'} \vee' \neg'[q]_{T'}$ *if* **AG** *contains (Ko);*
(5) $([s]_{T;} \wedge' \neg'[s]_{T'}) \vee' [q]_{T'} \leq' [q]_{T'}$ *if* **AG** *contains (K);*
(6) $[s]_{T'} \vee' \neg'[s]_{T'} =' 1'$ & $[s]_{T'} \wedge' \neg'[s]_{T'} =' 0'$ *if* **AG** *contains (B);*
(7) $([s]_{T'} \cdot' [t]_{T'}) \cdot' [q]_{T'} = [s]_{T'} \cdot' ([t]_{T'} \cdot' [q]_{T'})$;
(8) $[s]_{T'} \cdot' [t]_{T'} = [t]_{T'} \cdot' [s]_{T'}$;
(9) $[s]_{T'} \cdot' [s]_{T'} = [s]_{T'}$.

Proof. The proof is quite similar to Lemmas 6 and 7 except (7)–(9). (8) and (9) are easy. We provide the details for (7).

Let $([s]_{T'} \cdot' [t]_{T'}) \cdot' [q]_{T'} = [r_1]_{T'}$ and $[s]_{T'} \cdot' ([t]_{T'} \cdot' [q]_{T'}) = [r_2]_{T'}$. Let $[s]_{T'} \cdot' [t]_{T'} = [w_1]_{T'}$ and $[t]_{T'} \cdot' [q]_{T'} = [w_2]_{T'}$. Hence, $[r_1]_{T'} = [w_1 \cdot q]_{T'}$ and $[r_2]_{T'} = [s \cdot w_2]_{T'}$. It suffices to show $[r_1]_{T'} =' [r_2]_{T'}$.

Let $\vdash_{\mathbf{AG}} r_1 \leq w$. Then, $\vdash_{\mathbf{AG}} w_1 \cdot q \leq w$. Further, $\vdash_{\mathbf{AG}} s \cdot t \leq w_1$. Thus, by (trans), $\vdash_{\mathbf{AG}} (s \cdot t) \cdot q \leq w$. By ($ass_1$), $\vdash_{\mathbf{AG}} s \cdot (t \cdot q) \leq w$. By Lemma, there is $e \in c(T)$ such that $\vdash_{\mathbf{AG}} s \cdot (t \cdot q) \leq e$ and $\vdash_{\mathbf{AG}} e \leq w$. Then, $\vdash_{\mathbf{AG}} t \cdot q \leq s \to_\# e$, where $s \to_\# e \in c(T)$. Hence, $\vdash_{\mathbf{AG}} w_2 \leq s \to_\# e$. Then, $\vdash_{\mathbf{AG}} s \cdot w_2 \leq e$. Thus, $\vdash_{\mathbf{AG}} r_2 \leq e$. By (trans), $\vdash_{\mathbf{AG}} r_2 \leq w$. By Lemma $[r_1]_{T'} \leq' [r_2]_{T'}$. Similarly, $[r_2]_{T'} \leq' [r_1]_{T'}$. □

Lemma 16. *The following conditions hold for $\mathcal{Q}'$: for any,*

(1) *If $s \cdot q \in T'$, then $[s]_{T'} \cdot' [q]_{T'} = [s \cdot q]_{T'}$;*
(2) *If $s \to'_{\#} q \in T'$, then $[s]_{T'} \to'_{\#} [q]_{T'} = [s \to_{\#} q]_{T'}$.*

Lemma 17. *Let T' be set of terms generated from s, q. If $\nvdash_{\mathbf{AG}} s \leq q$, then there is $\mathcal{A}_{\mathcal{AG}}$ $\mathcal{Q}'$ and an assignment σ that is extended to σ' as above, satisfying $\not\models_{\mathcal{Q}'} \sigma(s) \leq' \sigma(t)$.*

Theorem 5 (FMP and Decidability)**. AG** *has FMP and is thus decidable.*

Remark 3. *In the finiteness proof delineated above, Lemma 11 is contingent on the properties of contraction and commutativity. The demonstration of Lemma 12, which serves as the cornerstone for constructing finite-quotient algebras, inherently relies on the validity of Lemma 11. Consequently, our proof does not extend to scenarios where fusion $\cdot$ fails to satisfy contraction and commutativity but still adheres to associativity.*

Moreover, this method does not work for the cases such that fusion $\cdot$ only admits associativity and weakening property too.

5. Conclusions

In this paper, we considered different lattice variants of layered algebras. We defined new graph-theoretical operations on layered graphs, thereby enhancing their expressivity. We demonstrated that any class of algebras belonging to $\{\mathcal{DLRG}, \mathcal{QBRG}, \mathcal{KRG}, \mathcal{KoRG}, \mathcal{HRG}, \mathcal{BRG}, \mathcal{CCQBRA}, \mathcal{CCKRA}, \mathcal{CCKoRA}, \mathcal{CCBRA}\}$ has FMP and decidable equational theory. We extended the results in [5] to more classes of algebras. We restricted the classes of algebras considered here to be bounded, which leads to a more simple proof. Moreover, by using special interpolation properties (Lemma 12), we expanded the FMP and decidability results to some classes of associative, commutative, and contractive algebras successfully.

Layered graph algebras offer a novel approach to analyzing complex systems that are prevalent in these fields. Specifically, they enable more rigorous verification of key properties, such as security and error resilience. In cryptography, this framework can be used to analyze and identify weaknesses in cryptographic systems that rely on layered security measures. In coding theory, it can help to design new error-correcting codes that are better suited for environments with limited resources or prone to communication disruptions. Essentially, this framework bridges algebraic theory with real-world problems to ensure secure and reliable data transmission.

For further research, we are also interested in the complexity problems closely related to the results presented in this paper. In [22], it is shown that the bounded distributive residuated groupoid (denoted $\mathcal{DLRG}$ here) has an EXPTIME-complete quasi-equational theory and thus the EXPTIME upper bound for the equational theory of $\mathcal{DLRG}$. The same complexity results for quasi-equational theory $\mathcal{BRG}$ are proved in [23], while $\mathcal{BRG}$ has a PSPACE-complete equational theory [24]. Lastly, the complexity of the equational theories of other algebras considered here, to the best of our knowledge, has not been settled.

Moreover, we are interested in exploring extended questions of the finite model property for layered graph algebras over non-distributive lattices. Utilizing logical methods, we can demonstrate the cut-elimination property for the sequent calculus system corresponding to the considered algebra. Based on this result, by proving that the derivation tree is finite, we can establish the decidability of the corresponding logic. Consequently, this allows us to address the decidability problem of equations for the corresponding non-distributive layered graph algebras. However, proving the finite model property is considerably more challenging. In [8], the most basic non-distributive layered graph

algebras (under the name non-distributive lattice-ordered residuated groupoid) and some of their negation extensions were shown to possess the finite model property. Nevertheless, the finite model property for many extensions remains an open problem, such as non-distributive layered graph algebras with De Morgan negation, Boolean negation extensions, and others.

The strong finite model property is another issue that we intend to focus on in the future. It is known that this problem is closely related to the word problem for classes of algebras, a topic that has been extensively studied. Moreover, since the classes of algebras we investigate are varieties, they all satisfy the HSP (homomorphic image, subalgebra, and product) property. As indicated in [8], for a class of algebras satisfying this property, the strong finite model property implies that the class has the finite embeddability property. Therefore, the strong finite model property is also a subject of our forthcoming research endeavors.

Author Contributions: Conceptualization, Z.L., F.L. and Z.Y.; methodology, Z.L.; validation, Z.L., F.L. and Z.Y.; formal analysis, Z.L.; investigation, Z.L.; writing—original draft preparation, Z.L., H.Z., Z.Y. and Y.W.; writing—review and editing, Z.L., F.L., Z.Y., H.Z. and Y.W.; supervision, Z.L. and F.L.; project administration, Z.L. and Z.Y.; funding acquisition, Z.Y., F.L. and H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The research was funded by the Key Project of Chinese Ministry of Education (22JJD720021) and the Chinese Ministry of Education of Humanities and Social Science Project (23YJC72040003).

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Jónsson, B.; Tsinakis, C. Relation algebras as residuated Boolean algebras. *Algebra Universalis* **1993**, *30*, 469–478. [CrossRef]
2. Collinson, M.; McDonald, K.; Pym, D. A substructural logic for layered graphs. *J. Log. Comput.* **2014**, *24*, 953–988. [CrossRef]
3. Collinson, M.; McDonald, K.; Pym, D. Layered graph logic as an assertion language for access control policy models. *J. Log. Comput.* **2017**, *27*, 41–80. [CrossRef]
4. Docherty, S.; Pym, D. Intuitionistic layered graph logic: Semantics and proof theory. *Log. Methods Comput. Sci.* **2018**, *14*.. [CrossRef]
5. Buszkowski, W. Interpolation and FEP for logics of residuated algebras. *Log. J. IGPL* **2011**, *19*, 437–454. [CrossRef]
6. Cardelli, L.; Gardner, P.; Ghelli, G. A spatial logic for querying graphs. In *Automata, Languages and Programming: 29th International Colloquium, ICALP 2002 Málaga, Spain, 8–13 July 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 597–610.
7. Conforti, G.; Macedonio, D.; Sassone, V. Spatial logics for bigraphs. In *Proceeding ICAP '05, LNCS 3580*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 766–778.
8. Galatos, N.; Jipsen, P.; Kowalski, T.; Ono, H. *Residuated Lattices: An Algebraic Glimpse at Substructural Logics*; Studies in Logic and The Foundations of Mathematics 151; Elsevier: Amsterdam, The Netherlands, 2007.
9. Farulewski, M. Finite Embeddabilty Property for Residuated Groupoids. *Rep. Math. Log.* **2008**, *43*, 25–42.
10. Hanikova, Z.; Horcık, R. The finite embeddability property for residuated groupoids. *Algebra Universalis* **2014**, *72*, 1–13.
11. Kaminski, M.; Francez, N. Relational semantics of the Lambek calculus extended with classical propositional logic. *Stud. Log.* **2014**, *102*, 479–497.
12. Kaminski, M.; Francez, N. The Lambek calculus extended with intuitionistic propositional logic. *Stud. Log.* **2016**, *104*, 1051–1082. [CrossRef]
13. Chvalovsk'y, K. Undecidability of the consequence relation in full nonassociative Lambek Calculus. *J. Symb. Log.* **2015**, *80*, 567–586. [CrossRef]
14. Girard, J.Y. Linear logic. *Theor. Comp. Sci.* **1987**, *50*, 1–101. [CrossRef]
15. Buszkowski, W. Some decision problems in the theory of syntactic categories. *Math. Log. Q.* **1982**, *28*, 539–548.
16. Lambek, J. The Mathematics of Sentence Structure. *Am. Math. Mon.* **1958**, *65*, 154–170. [CrossRef]
17. Galatos, N. The undecidability of the word problem for distributive residuated lattices. In *Ordered Algebraic Structures*; Martínez, J., Ed.; Kluwer Academic Publishers: Dordrecht, The Netherlands, 2002; pp. 231–243.

18. Metcalfe, G.; Paoli, F.; Tsinakis, C. *Residuated Structures in Algebra and Logic*; American Mathematical Society: Providence, RI, USA, 2023; Volume 277.
19. Kleene, S.C. *Introduction to Metamathematics*; Literary Licensing, LLC: Whitefish, MT, USA, 1952.
20. Dunn, J.M. A Kripke-style semantics for R-mingle using a binary accessibility relation. *Stud. Log.* **1976**, *35*, 163–172. [CrossRef]
21. Rivieccio, U. An infinity of super-Belnap logics. *J. Appl. Non-Class. Logics* **2012**, *22*, 319–335.
22. Shkatov, D.; Van Alten, C.J. Complexity of the universal theory of bounded residuated distributive lattice-ordered groupoids. *Algebra Univers.* **2019**, *80*, 36.
23. Placzek, P. Complexity of Nonassociative Lambek Calculus with classical logic. *Electron. Proc. Theor. Comput. Sci.* **2024**, *415*, 150–164.
24. Lin, Z.; Ma, M. On the complexity of the equational theory of residuated boolean algebras. In *Logic, Language, Information, and Computation;* Väänänen, J., Hirvonen, Å., de Queiroz, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; pp. 265–278.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

An Investigation into Bipolar Fuzzy Hoop Algebras and Their Applications

Tahsin Oner [1,†], Rajesh Neelamegarajan [2,†], Ravi Kumar Bandaru [3,*,†] and Hashem Bordbar [4,*,†]

[1] Department of Mathematics, Faculty of Science, Ege University, 35100 Izmir, Türkiye; tahsin.oner@ege.edu.tr
[2] Department of Mathematics, Rajah Serfoji Government College, Thanjavur 613005, Tamil Nadu, India; nrajesh_topology@yahoo.co.in
[3] Department of Mathematics, School of Advanced Sciences, VIT-AP University, Amaravati 522237, Andhra Pradesh, India
[4] Centre for Information Technologies and Applied Mathematics, University of Nova Gorica, 5000 Nova Gorica, Slovenia
* Correspondence: ravimaths83@gmail.com (R.K.B.); hashem.bordbar@ung.si (H.B.); Tel.: +386-070-614-786 (H.B.)
† These authors contributed equally to this work.

Abstract: This paper introduces bipolar fuzzy sub-hoops and bipolar fuzzy filters within hoop algebras, extending fuzzy logic to incorporate both positive and negative membership degrees. We define these structures, explore their algebraic properties, and establish their interplay through rigorous theorems. Key results include characterizations of bipolar fuzzy filters via level sets and conditions under which they become implicative filters. These findings enhance the theoretical framework of many-valued logic and offer practical applications in decision-making, image processing, and spatial reasoning under uncertainty. Our work provides a foundation for advanced fuzzy systems handling complex, contradictory information.

Keywords: hoop; bipolar fuzzy sub-hoop; bipolar fuzzy ideal

MSC: 20N05; 94D05; 03H72

1. Introduction

The notion of a *hoop* was introduced by Bosbach [1,2] as a foundational algebraic structure for examining many-valued logical systems, where the truth values of propositions are represented within a lattice framework. Hoops serve as a valuable mathematical tool for modeling systems in which logical propositions assume a continuum of values, typically within the interval $[0, 1]$, rather than being limited to binary truth values. This makes them especially suitable for reasoning in fuzzy logic contexts, where truth is viewed as partial and gradual rather than absolute.

Algebraically, a hoop is a bounded distributive lattice equipped with an additional binary operation, commonly referred to as *implication* or *residuation*, that satisfies specific axioms. This structure is particularly significant in fuzzy set theory, where it supports reasoning and decision-making under uncertainty. The implication operation enables the flexible manipulation of fuzzy relations and logical constructs, offering a more expressive framework than classical Boolean logic.

Hoops can be regarded as a generalization of Heyting algebras, extending the semantics of classical logic to accommodate degrees of truth. Their structural properties make

hoop algebras indispensable in formalizing the semantics of fuzzy sets and logics and they are widely used in applications such as spatial reasoning, image processing, and decision support systems.

Since Bosbach's initial formulation, hoop theory has been the subject of extensive research (see [3–11]). These studies have deepened our understanding of hoop structures, their properties, and their relevance to many-valued logic systems, particularly within the framework of fuzzy logic.

In 1994, Zhang [12] introduced the concept of *bipolar fuzzy sets* as a generalization of traditional fuzzy sets [13]. Unlike classical fuzzy sets where membership degrees range from 0 to 1, bipolar fuzzy sets assign degrees within the interval $[-1, 1]$. In this setting, a degree of 0 indicates irrelevance to the property in question, values between 0 and 1 suggest partial satisfaction, while values between -1 and 0 indicate the partial satisfaction of a counter-property. Although bipolar fuzzy sets share some conceptual similarities with intuitionistic fuzzy sets, they differ fundamentally in structure and interpretation. The distinction between positive and negative information is crucial in many real-world scenarios; positive information reflects what is considered possible, while negative information captures what is regarded as impossible.

To manage bipolar information, both fuzzy and possibilistic frameworks have been proposed. These approaches are particularly relevant in areas such as image processing and spatial reasoning, where bipolarity naturally arises. For instance, in determining an object's position, positive information may represent plausible locations, while negative information may signify locations that are definitively excluded. In spatial relation modeling, concepts like "left" and "right" are not mere negations of one another but represent symmetric opposites. This symmetry introduces a middle ground, positions that are neither clearly to the left nor the right, emphasizing the inherent indeterminacy and demonstrating that the union of positive and negative information does not exhaust the entire space.

This paper introduces and investigates the concepts of *bipolar fuzzy sub-hoops* and *bipolar fuzzy filters*, examining their algebraic properties in depth. It explores the interactions between these two structures, providing a detailed analysis of their relationship. Additionally, it establishes formal characterizations for both bipolar fuzzy sub-hoops and bipolar fuzzy filters, offering new insights into their underlying structure and contributing to their theoretical development within the broader context of fuzzy logic and many-valued reasoning.

The novelty of this work lies in introducing bipolar fuzzy sub-hoops and filters, which generalize fuzzy logic to incorporate both positive and negative information within hoop algebras. Our contributions include defining these structures, proving their algebraic properties, and characterizing their interrelationship, notably that every BFF is a BFSH (Theorem 4). A key technical difficulty was ensuring that bipolar fuzzy sets respect the hoop algebra's operations while handling dual membership degrees, which we addressed through new conditions and theorems (e.g., Theorems 3 and 6) that align with classical algebraic structures.

The list of acronyms is given in Table 1.

Table 1. List of acronyms.

Acronyms	Representation
BFF	bipolar fuzzy filter
IBFF	implicative bipolar fuzzy filter
BFS	bipolar fuzzy set
BFSH	bipolar fuzzy sub-hoop
BF_S	bipolar fuzzy structure

2. Preliminaries

Bipolar fuzzy sets, introduced by Zhang [12], extend traditional fuzzy sets by incorporating negative membership degrees, enabling the modeling of both positive and negative information.

Definition 1 ([12]). *Let $\mathcal{X}$ be a non-empty set. A bipolar fuzzy set (briefly, BFS) $\mathcal{B}$ in $\mathcal{X}$ is defined as $\mathcal{B} = \{(\mathfrak{x}, \Omega^-(\mathfrak{x}), \Omega^+(\mathfrak{x})) \mid \mathfrak{x} \in \mathcal{X}\}$, where $\Omega^+ : \mathcal{X} \to [0,1]$ and $\Omega^- : \mathcal{X} \to [-1,0]$ are two functions. The positive membership degree $\Omega^+(\mathfrak{x})$ represents the degree to which element $\mathfrak{x}$ satisfies the property associated with the BFS $\mathcal{B}$, while the negative membership degree $\Omega^-(\mathfrak{x})$ represents the degree to which $\mathfrak{x}$ satisfies an implicit counter-property related to $\mathcal{B}$. If $\Omega^+(\mathfrak{x}) \neq 0$ and $\Omega^-(\mathfrak{x}) = 0$, this indicates that x fully satisfies the positive property of B. Conversely, if $\Omega^+(\hbar_{\mathfrak{a}_1}) = 0$ and $\Omega^-(\mathfrak{x}) \neq 0$, this suggests that x does not meet the property of $\mathcal{B}$ but partially satisfies its counter-property. It is also possible that $\Omega^+(\mathfrak{x}) = 0$ and $\Omega^-(\mathfrak{x}) = 0$, which occurs when the membership functions for the property and its counter-property overlap over some subset of $\mathcal{X}$. For simplicity, we denote the BFS $\mathcal{B} = \{(\mathfrak{x}, \Omega^-(\mathfrak{x}), \Omega^+(\mathfrak{x})) \mid \mathfrak{x} \in \mathcal{X}\}$ as $\Omega = (\Omega^+, \Omega^-)$.*

Hoop algebras, defined by Bosbach [1,2], provide a lattice-based framework for many-valued logic, with operations $\odot$ and $\to$ supporting fuzzy reasoning. They generalize Heyting algebras and are central to our bipolar fuzzy extensions.

Definition 2 ([4]). *A hoop (or hoop algebra) is an algebraic structure denoted as $(\mathcal{H}, \odot, \to, 1)$, where $(\mathcal{H}, \odot, 1)$ forms a commutative monoid, and the following properties hold:*

- *(H1)* $\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1} = 1$,
- *(H2)* $\hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) = \hbar_{\mathfrak{a}_2} \odot (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_1})$,
- *(H3)* $\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) = (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to z$ *for all* $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}$.

Next, we define a relation $\leq_{\mathcal{H}}$ on a hoop $\mathcal{H}$ as follows:

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H})(\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \Leftrightarrow \hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} = 1). \tag{1}$$

It is straightforward to verify that $(\mathcal{H}, \leq_{\mathcal{H}})$ forms a partially ordered set.

Sub-hoops preserve the algebraic structure of hoops, forming the basis for our bipolar fuzzy sub-hoops, which extend this concept to fuzzy settings.

Definition 3 ([8]). *A non-empty subset $\mathcal{S}$ of a hoop algebra $\mathcal{H}$ is called a sub-hoop of $\mathcal{H}$ if it satisfies the following condition:*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{S})(\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2} \in \mathcal{S} \quad \text{and} \quad \hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} \in \mathcal{S}). \tag{2}$$

Additionally, every sub-hoop must include the element 1.

Proposition 1 ([8]). *Let $(\mathcal{H}, \odot, \to, 1)$ be a hoop algebra. For any $\hbar_{\mathfrak{a}}, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}$, the following conditions hold:*
(a1) $(\mathcal{H}, \leq_{\mathcal{H}})$ is a meet-semilattice with $\hbar_{\mathfrak{a}_1} \wedge \hbar_{\mathfrak{a}_2} = \hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})$;
(a2) $\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_3}$ if and only if $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}$;
(a3) $\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}$, and $\hbar_{\mathfrak{a}_1}^{\mathfrak{n}} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1}$ for any $\mathfrak{n} \in N$;
(a4) $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_1}$;
(a5) $1 \to \hbar_{\mathfrak{a}} = \hbar_{\mathfrak{a}}$ and $\hbar_{\mathfrak{a}} \to 1 = 1$;
(a6) $\hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1} \wedge \hbar_{\mathfrak{a}_2} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}$;
(a7) $\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} \leq_{\mathcal{H}} (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3})$;

(a8) $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2}$ *implies* $\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_3} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \odot \hbar_{\mathfrak{a}_3}, \hbar_{\mathfrak{a}_3} \to \hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_3} \to \hbar_{\mathfrak{a}_2}$, *and* $\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}$;
(a9) $\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) = \hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3})$.

Filters in hoop algebras capture upward-closed subsets, essential for defining bipolar fuzzy filters that refine fuzzy information.

Definition 4 ([8]). *A non-empty subset $\mathcal{F}$ of a hoop algebra $\mathcal{H}$ is referred to as a filter of $\mathcal{H}$ if the following conditions are satisfied:*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H})(\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{F} \Rightarrow \hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2} \in \mathcal{F}), \tag{3}$$
$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H})(\hbar_{\mathfrak{a}_1} \in \mathcal{F}, \hbar_{\mathfrak{a}_1} \leq \hbar_{\mathfrak{a}_2} \Rightarrow \hbar_{\mathfrak{a}_2} \in \mathcal{F}). \tag{4}$$

Implicative filters strengthen filter conditions, motivating our definition of implicative bipolar fuzzy filters (IBFFs) for advanced fuzzy logic applications.

Definition 5 ([9]). *A non-empty subset $\mathcal{F}$ of a hoop algebra $\mathcal{H}$ is termed an implicative filter of $\mathcal{H}$ if it satisfies the following conditions:*

$$1 \in \mathcal{F}, \tag{5}$$
$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H})(\hbar_{\mathfrak{a}_1} \to ((\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) \to \hbar_{\mathfrak{a}_2}) \in \mathcal{F}, \hbar_{\mathfrak{a}_1} \in \mathcal{F} \Rightarrow \hbar_{\mathfrak{a}_2} \in \mathcal{F}). \tag{6}$$

It is important to note that the conditions in (3) and (4) indicate that the subset $\mathcal{F}$ is closed under the operation $\odot$ and upward-closed, respectively. Furthermore, a subset $\mathcal{F}$ of a hoop algebra $\mathcal{H}$ is a filter if and only if it satisfies condition (5) along with the following additional condition:

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H})(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} \in \mathcal{F}, \hbar_{\mathfrak{a}_1} \in \mathcal{F} \Rightarrow \hbar_{\mathfrak{a}_2} \in \mathcal{F}). \tag{7}$$

3. Bipolar Fuzzy Hoop Algebras

Definition 6. *A BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ within a hoop $\mathcal{H}$ is termed a bipolar fuzzy sub-hoop (briefly, BFSH) of $\mathcal{H}$ if the following conditions hold:*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \quad \begin{pmatrix} \Omega^+(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\}, \\ \Omega^-(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\} \end{pmatrix}. \tag{8}$$

Here, $\bullet$ represents either $\odot$ or $\to$.

Example 1. *Let $\mathcal{H} = \{0, 1, 2, 3, 4, 5, 6\}$ be a set equipped with two binary operations, $\cdot$ and $\to$, whose values are provided in the following Tables 2 and 3.*

Then, $(\mathcal{H}, \odot, \to, 1)$ is a hoop algebra. Let $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ be a BFS in $\mathcal{H}$, given by Table 4.

It is straightforward to verify that the BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ within the hoop $\mathcal{H}$ qualifies as a BFSH of $\mathcal{H}$.

Table 2. Cayley table of the binary operation $\to$.

$\to$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	1	1	2	1	1	1	1
1	0	1	2	3	4	5	6
2	1	1	1	1	1	1	1
3	0	1	2	1	1	5	6
4	0	1	2	3	1	5	6
5	0	1	2	1	1	1	6
6	1	2	1	1	1	1	1

Table 3. Cayley table of the binary operation $\odot$.

$\odot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	2	0	0	0	0
1	0	1	2	3	4	5	6
2	2	2	2	2	2	2	2
3	0	3	2	3	3	5	6
4	0	4	2	3	4	5	6
5	0	5	2	5	5	5	6
6	0	6	2	6	6	6	0

Table 4. Tabular representation of $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$.

$\mathcal{H}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
$\Omega^-(\hbar_\mathfrak{a})$	-0.8	-0.8	-0.8	-0.7	-0.7	-0.7	-0.8
$\Omega^+(\hbar_\mathfrak{a})$	0.8	0.8	0.8	0.7	0.8	0.8	0.8

Proposition 2. *For any BFSH $\Omega = (\Omega^+, \Omega^-)$ of $\mathcal{H}$, the following holds:*

$$(\forall \hbar_\mathfrak{a} \in \mathcal{H}) \quad \begin{pmatrix} \Omega^+(1) \geq \Omega^+(\hbar_\mathfrak{a}), \\ \Omega^-(1) \leq \Omega^-(\hbar_\mathfrak{a}) \end{pmatrix}. \tag{9}$$

Proof. Since $\hbar_\mathfrak{a} \to \hbar_\mathfrak{a} = 1$ for all $\hbar_\mathfrak{a} \in \mathcal{H}$, it is straightforward by (8). □

Proposition 3. *Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be a homomorphism of a hoop algebra $\mathcal{X}$ into a hoop algebra $\mathcal{Y}$ and $\Omega = (\mathcal{Y}, \Omega^-, \Omega^+)$ be a BFSH of $\mathcal{Y}$. Then, the inverse image $\vartheta^{-1}(\Omega)$ of Ω is a BFSH of $\mathcal{X}$.*

Proof. For any $\bullet \in \{\odot, \to\}$ and $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{X}$. Then,

$$\begin{aligned} \Omega^+_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) &= \Omega^+(\vartheta(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2})) \\ &= \Omega^+(\vartheta(\hbar_{\mathfrak{a}_1}) \bullet \vartheta(\hbar_{\mathfrak{a}_2})) \\ &\geq \min\{\Omega^+(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^+(\vartheta(\hbar_{\mathfrak{a}_2}))\} \\ &= \min\{\Omega^+_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_1}), \Omega^+_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_2})\}, \end{aligned}$$

and

$$\begin{aligned} \Omega^-_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) &= \Omega^-(\vartheta(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2})) \\ &= \Omega^-(\vartheta(\hbar_{\mathfrak{a}_1}) \bullet \vartheta(\hbar_{\mathfrak{a}_2})) \\ &\leq \max\{\Omega^-(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^-(\vartheta(\hbar_{\mathfrak{a}_2}))\} \\ &= \max\{\Omega^-_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_1}), \Omega^-_{\vartheta^{-1}(\Omega)}(\hbar_{\mathfrak{a}_2})\}. \end{aligned}$$

□

Definition 7. *A BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ within a hoop algebra $\mathcal{H}$ is said to possess the sup-inf property if for any subset $\mathcal{T} \subset \mathcal{H}$, there exists an element $t_0 \in \mathcal{T}$ such that $\Omega^+(t_0) = \sup_{t \in \mathcal{T}} \Omega^+(t)$ and $\Omega^-(t_0) = \inf_{t \in \mathcal{T}} \Omega^+(t)$.*

Proposition 4. *Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be a homomorphism from a hoop algebra $\mathcal{X}$ to a hoop algebra $\mathcal{Y}$ and let $\Omega = (\mathcal{A}, \Omega^-, \Omega^+)$ be a BFSH of $\mathcal{X}$ that satisfies the sup-inf property. Then, the image $\vartheta(\Omega)$ under the homomorphism is a BFSH of $\mathcal{Y}$.*

Proof. For any $\bullet \in \{\odot, \to\}$ and $\mathfrak{u}, \mathfrak{v} \in \mathcal{Y}$; let $\hbar_{\mathfrak{a}_1} \in \alpha^{-1}(\mathfrak{u})$ and $\hbar_{\mathfrak{a}_2} \in \alpha^{-1}(\mathfrak{v})$ such that

$$\Omega^+(\hbar_{\mathfrak{a}_1}) = \sup_{t \in \vartheta^{-1}(\mathfrak{u})} \Omega^+(t), \quad \Omega^+(\hbar_{\mathfrak{a}_2}) = \sup_{t \in \vartheta^{-1}(\mathfrak{v})} \Omega^+(t)$$

and

$$\Omega^-(\hbar_{\mathfrak{a}_1}) = \inf_{t \in \vartheta^{-1}(\mathfrak{u})} \Omega^-(t), \quad \Omega^-(\hbar_{\mathfrak{a}_2}) = \inf_{t \in \vartheta^{-1}(\mathfrak{v})} \Omega^-(t).$$

Then, by the definition of $\Omega^+_{\vartheta(\Omega)}$, we have

$$\begin{aligned}
\Omega^+_{\vartheta(\Omega)}(\mathfrak{u} \bullet \mathfrak{v}) &= \sup_{t \in \vartheta^{-1}(\mathfrak{u} \bullet \mathfrak{v})} \Omega^+(t) \\
&\geq \Omega^+(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \\
&\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\} \\
&= \min\{\sup_{t \in \alpha^{-1}(\mathfrak{u})} \Omega^+(t), \sup_{t \in \alpha^{-1}(\mathfrak{v})} \Omega^+(t)\} \\
&= \min\{\Omega^+_{\vartheta(\Omega)}(\mathfrak{u}), \Omega^+_{\vartheta(\Omega)}(\mathfrak{v})\}
\end{aligned}$$

and

$$\begin{aligned}
\Omega^-_{\vartheta(\Omega)}(\mathfrak{u} \bullet \mathfrak{v}) &= \inf_{t \in \vartheta^{-1}(\mathfrak{u} \bullet \mathfrak{v})} \Omega^-(t) \\
&\leq \Omega^-(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \\
&\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\} \\
&= \max\{\inf_{t \in \vartheta^{-1}(\mathfrak{u})} \Omega^-(t), \inf_{t \in \vartheta^{-1}(v)} \Omega^-(t)\} \\
&= \max\{\Omega^-_{\vartheta(\Omega)}(\mathfrak{u}), \Omega^-_{\vartheta(\Omega)}(\mathfrak{v})\}.
\end{aligned}$$

Hence, $\vartheta(\Omega)$ is a BFSH of $\mathcal{Y}$. □

Definition 8. *A BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ within a hoop algebra $\mathcal{H}$ is considered to be a bipolar fuzzy filter (briefly, BFF) of $\mathcal{H}$ if for every $\bullet \in \{\odot, \to\}$, the following conditions hold:*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \Omega^+(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\} \\ \Omega^-(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\} \end{pmatrix}, \tag{10}$$

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \quad \Rightarrow \\ \begin{cases} \Omega^+(\hbar_{\mathfrak{a}_1}) \leq \Omega^+(\hbar_{\mathfrak{a}_2}) \\ \Omega^-(\hbar_{\mathfrak{a}_1}) \geq \Omega^-(\hbar_{\mathfrak{a}_2}) \end{cases} \end{pmatrix}. \tag{11}$$

Example 2. *Let $(\mathcal{H}, \odot, \to, 1)$ be a hoop algebra, given in Example 1. Let $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ be a BFS in $\mathcal{H}$, given by Table 5.*

It can be readily verified that the BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ within the hoop algebra $\mathcal{H}$ qualifies as a BFF of $\mathcal{H}$.

Table 5. Tabular representation of $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$.

$\mathcal{H}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
$\Omega^-(\hbar_{\mathfrak{a}})$	-0.6	-0.8	-0.6	-0.7	-0.8	-0.7	-0.6
$\Omega^+(\hbar_{\mathfrak{a}})$	0.7	0.8	0.7	0.7	0.8	0.7	0.7

The following theorem provides an alternative characterization of bipolar fuzzy filters (BFFs) by replacing the monotonicity condition with a condition involving the implication operation, simplifying their verification in hoop algebras.

Theorem 1. *A BFS $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies* (9) *and*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \Omega^+(\hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} \\ \Omega^-(\hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} \end{pmatrix}. \tag{12}$$

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of $\mathcal{H}$. Since $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} 1$ for all $\hbar_{\mathfrak{a}_1} \in \mathcal{H}$, it follows from Equation (11) that Equation (9) holds. For any $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$, we obtain the inequality

$$\hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2}.$$

By utilizing Equations (10) and (11), we derive the following bounds:

$$\Omega^+(\hbar_{\mathfrak{a}_2}) \geq \Omega^+(\hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}$$

and

$$\Omega^-(\hbar_{\mathfrak{a}_2}) \leq \Omega^-(\hbar_{\mathfrak{a}_1} \odot (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\},$$

which establishes Equation (12).

Conversely, suppose that the BFS $\Omega = (\Omega^+, \Omega^-)$ satisfies both Equations (9) and (12). Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$. Since

$$\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2})) = (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) = 1,$$

it follows from the assumptions (9) and (12) that

$$\begin{aligned} \Omega^+(\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) &\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \Omega^+(\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}))\} \\ &\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2})))\}\} \\ &= \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(1)\}\} \\ &= \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \Omega^+(\hbar_{\mathfrak{a}_1})\} \end{aligned}$$

and

$$\begin{aligned} \Omega^-(\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) &\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \Omega^-(\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}))\} \\ &\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2})))\}\} \\ &= \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(1)\}\} \\ &= \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \Omega^-(\hbar_{\mathfrak{a}_1})\}. \end{aligned}$$

Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$ be such that $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2}$. Then, $\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} = 1$, and so

$$\Omega^+(\hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} = \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(1)\} = \Omega^+(\hbar_{\mathfrak{a}_1}),$$

$$\Omega^-(\hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} = \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(1)\} = \Omega^-(\hbar_{\mathfrak{a}_1}).$$

Therefore, $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

Theorem 2. *In the context of a hoop algebra $\mathcal{H}$, every BFF is a BFSH.*

Proof. To prove that every BFF is a BFSH in a hoop algebra $\mathcal{H}$, we show that a BFS $\Omega = (\Omega^+, \Omega^-)$ satisfying Definition 13 (BFF) also satisfies Definition 6 (BFSH). By Definition 8, a BFF Ω satisfies

$$\Omega^+(\hbar_{a_1} \bullet \hbar_{a_2}) \geq \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_2})\}, \quad \Omega^-(\hbar_{a_1} \bullet \hbar_{a_2}) \leq \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_2})\}$$

for all $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$ and $\bullet \in \{\odot, \to\}$, and the monotonicity condition:

$$\text{If } \hbar_{a_1} \leq_{\mathcal{H}} \hbar_{a_2}, \text{ then } \Omega^+(\hbar_{a_1}) \leq \Omega^+(\hbar_{a_2}), \quad \Omega^-(\hbar_{a_1}) \geq \Omega^-(\hbar_{a_2}).$$

Definition 6 requires only the first condition for $\bullet \in \{\odot, \to\}$. Since this condition is identical in both definitions, it is immediately satisfied by any BFF. The additional monotonicity condition in Definition 8 is not required for a BFSH, so every BFF automatically satisfies the BFSH conditions. Hence, every BFF is a BFSH. □

The converse of Theorem 2 does not necessarily hold, as demonstrated by the following example.

Example 3. *Consider the hoop algebra $(\mathcal{H}, \odot, \to, 1)$, as defined in Example 1, and the BFSH $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$, presented in the same example. However, $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ does not qualify as a BFF of $\mathcal{H}$, as evidenced by the following inequalities:*

$$\begin{aligned} \Omega^-(3) = -0.7 \not\leq -0.8 &= \max\{-0.8, -0.8\} \\ &= \max\{\Omega^-(1), \Omega^-(2)\} \\ &= \max\{\Omega^-(2 \to 3), \Omega^-(2)\} \end{aligned}$$

and

$$\begin{aligned} \Omega^+(3) = 0.7 \not\geq 0.8 &= \min\{0.8, 0.8\} \\ &= \min\{\Omega^+(1), \Omega^+(2)\} \\ &= \min\{\Omega^+(2 \to 3), \Omega^+(2)\}. \end{aligned}$$

The following theorem establishes that a bipolar fuzzy set is a BFF if its level sets are filters, bridging fuzzy logic with classical algebraic structures. The proof relies on the definitions of level sets and filter properties in hoop algebras.

Theorem 3. *Let $\mathcal{H}$ be a hoop algebra. The BF_S $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if for all $(\mathfrak{t}, \mathfrak{s}) \in [0,1] \times [0,1]$ with $\mathfrak{t} + \mathfrak{s} \leq 1$, the non-empty level sets $\mathcal{U}(\Omega^+, \mathfrak{t})$ and $\mathcal{L}(\Omega^-, \mathfrak{s})$ are filters of $\mathcal{H}$.*

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. Let $(\mathfrak{t}, \mathfrak{s}) \in [0,1] \times [0,1]$ be such that $\mathfrak{t} + \mathfrak{s} \leq 1$, and suppose that $\mathcal{U}(\Omega^+, \mathfrak{t})$ and $\mathcal{L}(\Omega^-, \mathfrak{s})$ are non-empty. It is evident that $1 \in \mathcal{U}(\Omega^+, \mathfrak{t}) \cap \mathcal{L}(\Omega^-, \mathfrak{s})$.

Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$ be such that $\hbar_{\mathfrak{a}_1} \in \mathcal{U}(\Omega^+, \mathfrak{t}) \cap \mathcal{L}(\Omega^-, \mathfrak{s})$ and $\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2} \in \mathcal{U}(\Omega^+, \mathfrak{t}) \cap \mathcal{L}(\Omega^-, \mathfrak{s})$. By the properties of Ω, we have $\Omega^+(\hbar_{\mathfrak{a}_1}) \geq \mathfrak{t}$, $\Omega^-(\hbar_{\mathfrak{a}_1}) \leq \mathfrak{s}$, $\Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \geq \mathfrak{t}$ and $\Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \leq s$.

From Equation (12), it follows that

$$\Omega^+(\hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} \geq t$$

and

$$\Omega^-(\hbar_{a_2}) \leq \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\} \leq s.$$

Hence, $\hbar_{a_2} \in \mathcal{U}(\Omega^+, t) \cap \mathcal{L}(\Omega^-, s)$, which implies that $\mathcal{U}(\Omega^+, t)$ and $\mathcal{L}(\Omega^-, s)$ are filters of $\mathcal{H}$.

Conversely, assume that the non-empty level sets $\mathcal{U}(\Omega^+, t)$ and $\mathcal{L}(\Omega^-, s)$ are filters of $\mathcal{H}$ for all $(t, s) \in [0,1] \times [0,1]$ with $t + s \leq 1$. For any $\hbar_{a_1} \in \mathcal{H}$, let $\Omega^+(\hbar_{a_1}) = t_1$ and $\Omega^-(\hbar_{a_1}) = s_1$. Since $1 \in \mathcal{U}(\Omega^+, t_1) \cap \mathcal{L}(\Omega^-, s_1)$, we have $\Omega^+(1) \geq t_1 = \Omega^+(\hbar_{a_1})$ and $\Omega^-(\hbar_{a_1}) \leq s_1$.

For any $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$, let $t_1, t_2, s_1, s_2 \in [0,1]$ be such that $\Omega^+(\hbar_{a_1}) = t_1$, $\Omega^+(\hbar_{a_1} \to \hbar_{a_2}) = t_2$, $\Omega^-(\hbar_{a_1}) = s_1$ and $\Omega^-(\hbar_{a_1} \to \hbar_{a_2}) = s_2$. Take $t = \min\{t_1, t_2\}$ and $s = \max\{s_1, s_2\}$. Then, both $\hbar_{a_1}$ and $\hbar_{a_1} \to \hbar_{a_2}$ belong to $\mathcal{U}(\Omega^+, t) \cap \mathcal{L}(\Omega^-, s)$. Consequently, $\hbar_{a_2} \in \mathcal{U}(\Omega^+, t) \cap L(\Omega^-, s)$ and, thus,

$$\Omega^+(\hbar_{a_2}) \geq t = \min\{t_1, t_2\} = \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_1} \to \hbar_{a_2})\}$$

and

$$\Omega^-(\hbar_{a_2}) \leq s = \max\{s_1, s_2\} = \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}.$$

Therefore, $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

The following theorem characterizes BFFs through conditions on their positive and negative membership functions, enhancing their applicability in fuzzy reasoning systems. The proof uses the algebraic properties of hoop operations to ensure consistency.

Theorem 4. *A BF$_S$ $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies Equation* (9) *and the following condition:*

$$(\forall \hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}) \quad \begin{cases} \Omega^+(\hbar_{a_1} \odot \hbar_{a_2}) = \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_2})\}, \\ \Omega^-(\hbar_{a_1} \odot \hbar_{a_2}) = \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_2})\}. \end{cases} \tag{13}$$

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ and let $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$. Since $\hbar_{a_1} \odot \hbar_{a_2} \leq_{\mathcal{H}} \hbar_{a_1}$ and $\hbar_{a_1} \odot \hbar_{a_2} \leq_{\mathcal{H}} \hbar_{a_2}$, it follows from Equation (11) that

$$\Omega^+(\hbar_{a_1} \odot \hbar_{a_2}) \leq \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_2})\}, \Omega^-(\hbar_{a_1} \odot \hbar_{a_2}) \geq \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_2})\}.$$

Since $\hbar_{a_1} \leq_{\mathcal{H}} \hbar_{a_2} \to (\hbar_{a_1} \odot \hbar_{a_2})$, we also have

$$\Omega^+(\hbar_{a_1} \odot \hbar_{a_2}) \geq \min\{\Omega^+(\hbar_{a_2}), \Omega^+(\hbar_{a_2} \to (\hbar_{a_1} \odot \hbar_{a_2}))\} \geq \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_2})\}$$

and

$$\Omega^-(\hbar_{a_1} \odot \hbar_{a_2}) \leq \max\{\Omega^-(\hbar_{a_2}), \Omega^-(\hbar_{a_2} \to (\hbar_{a_1} \odot \hbar_{a_2}))\} \leq \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_2})\}.$$

Thus, by Equations (12) and (11), we prove (13).

Conversely, suppose that $\Omega = (\Omega^+, \Omega^-)$ satisfies both Equation (9) and condition (13). Since $\hbar_{a_1} \odot (\hbar_{a_1} \to \hbar_{a_2}) \leq_{\mathcal{H}} \hbar_{a_2}$ for all $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$, it follows from (9) and (13) that

$$\Omega^+(\hbar_{a_2}) \geq \Omega^+(\hbar_{a_1} \odot (\hbar_{a_1} \to \hbar_{a_2})) = \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_1} \to \hbar_{a_2})\}$$

and

$$\Omega^-(\hbar_{a_2}) \leq \Omega^-(\hbar_{a_1} \odot (\hbar_{a_1} \to \hbar_{a_2})) = \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}.$$

Therefore, by Theorem 1, we conclude that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

The following theorem provides a necessary condition for a bipolar fuzzy set to be a BFF, offering a practical test for filter properties. The proof exploits the interplay between positive and negative memberships under hoop operations.

Theorem 5. *A BF_S $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies Equation* (9) *and the following condition:*

$$(\forall \hbar_{a_1}, \hbar_{a_2}, \hbar_{a_3} \in \mathcal{H}) \begin{cases} \Omega^+(\hbar_{a_1} \to \hbar_{a_3}) \geq \min\{\Omega^+(\hbar_{a_1} \to y), \Omega^+(\hbar_{a_2} \to \hbar_{a_3})\}, \\ \Omega^-(\hbar_{a_1} \to \hbar_{a_3}) \leq \max\{\Omega^-(\hbar_{a_1} \to \hbar_{a_2}), \Omega^-(\hbar_{a_2} \to \hbar_{a_3})\}. \end{cases} \tag{14}$$

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ and let $\hbar_{a_1}, \hbar_{a_2}, \hbar_{a_3} \in \mathcal{H}$. Since $(\hbar_{a_1} \to \hbar_{a_2}) \odot (\hbar_{a_2} \to \hbar_{a_3}) \leq_{\mathcal{H}} \hbar_{a_1} \to \hbar_{a_3}$, it follows from Equations (11) and (13) that

$$\begin{aligned} \Omega^+(\hbar_{a_1} \to \hbar_{a_3}) &\geq \Omega^+((\hbar_{a_1} \to \hbar_{a_2}) \odot (y \to \hbar_{a_3})) \\ &= \min\{\Omega^+(\hbar_{a_1} \to \hbar_{a_2}), \Omega^+(\hbar_{a_2} \to \hbar_{a_3})\} \end{aligned}$$

$$\begin{aligned} \Omega^-(\hbar_{a_1} \to \hbar_{a_3}) &\leq \Omega^-((\hbar_{a_1} \to \hbar_{a_2}) \odot (\hbar_{a_2} \to \hbar_{a_3})) \\ &= \max\{\Omega^-(\hbar_{a_1} \to \hbar_{a_2}), \Omega^-(\hbar_{a_2} \to \hbar_{a_3})\} \end{aligned}$$

This proves Equation (14).

Conversely, suppose that $\Omega = (\Omega^+, \Omega^-)$ satisfies both Equation (9) and condition (14). If we set $\hbar_{a_1} = 1$ in (14), we recover Equation (12). Thus, by Theorem 1, we conclude that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

The following theorem refines the characterization of BFFs by introducing additional conditions on membership degrees, strengthening their theoretical foundation. The proof combines hoop algebra axioms with bipolar fuzzy set constraints.

Theorem 6. *A BF_S $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies Equation* (9) *and the following condition:*

$$(\forall \hbar_{a_1}, \hbar_{a_2}, \hbar_{a_3} \in \mathcal{H}) \begin{cases} \Omega^+(\hbar_{a_2} \odot \hbar_{a_3}) \geq \min\{\Omega^+(\hbar_{a_1} \odot \hbar_{a_3}), \Omega^+(\hbar_{a_1} \to \hbar_{a_2})\}, \\ \Omega^-(\hbar_{a_2} \odot \hbar_{a_3}) \leq \max\{\Omega^-(\hbar_{a_1} \odot \hbar_{a_3}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}. \end{cases} \tag{15}$$

Proof. Let us assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ and consider arbitrary elements $\hbar_{a_1}, \hbar_{a_2}, \hbar_{a_3} \in \mathcal{H}$. It is noted that $(\hbar_{a_3} \odot \hbar_{a_1}) \odot (\hbar_{a_1} \to \hbar_{a_2}) = \hbar_{a_3} \odot (\hbar_{a_1} \odot (\hbar_{a_1} \to \hbar_{a_2})) \leq_{\mathcal{H}} \hbar_{a_3} \odot \hbar_{a_2}$. Applying Equations (11) and (13), we obtain the following inequalities:

$$\begin{aligned} \Omega^+(\hbar_{a_3} \odot \hbar_{a_2}) &\geq \Omega^+((\hbar_{a_3} \odot \hbar_{a_1}) \odot (\hbar_{a_1} \to \hbar_{a_2})) \\ &= \min\{\Omega^+(\hbar_{a_3} \odot \hbar_{a_1}), \Omega^+(\hbar_{a_1} \to \hbar_{a_2})\} \end{aligned}$$

and

$$\begin{aligned} \Omega^-(\hbar_{a_3} \odot \hbar_{a_2}) &\leq \Omega^-((\hbar_{a_3} \odot \hbar_{a_1}) \odot (\hbar_{a_1} \to \hbar_{a_2})) \\ &= \max\{\Omega^-(\hbar_{a_3} \odot \hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}. \end{aligned}$$

This proves Equation (15).

Conversely, suppose that $\Omega = (\Omega^+, \Omega^-)$ satisfies both Equation (9) and condition (15). Setting $\hbar_{\mathfrak{a}_3} = 1$ in (15) leads to Equation (12). Therefore, by Theorem 1, we conclude that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

Theorem 7. *A BF_S $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies the following condition:*

$$(\forall \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}) \left(\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3} \Rightarrow \begin{cases} \Omega^+(\hbar_{\mathfrak{a}_3}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\}, \\ \Omega^-(\hbar_{\mathfrak{a}_3}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\}. \end{cases} \right) \tag{16}$$

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ and let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}$ such that $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}$. Since $\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) = 1$, it follows that

$$\begin{aligned} \Omega^+(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) &\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}))\} \\ &= \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(1)\} \\ &= \Omega^+(\hbar_{\mathfrak{a}_1}) \end{aligned}$$

and

$$\begin{aligned} \Omega^-(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) &\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}))\} \\ &= \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(1)\} \\ &= \Omega^-(\hbar_{\mathfrak{a}_1}), \end{aligned}$$

which follows from Equation (12). Consequently, we obtain the inequalities

$$\Omega^+(\hbar_{\mathfrak{a}_3}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \Omega^+(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})\} \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\}$$

and

$$\Omega^-(\hbar_{\mathfrak{a}_3}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \Omega^-(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})\} \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\}.$$

Conversely, suppose that $\Omega = (\Omega^+, \Omega^-)$ satisfies both Equation (9) and condition (16). Since for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$, we have $\hbar_{\mathfrak{a}_1} \leq_{\mathcal{H}} (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}$, it follows from (16) that

$$\Omega^+(y) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}, \Omega^-(y) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}.$$

Thus, by Theorem 1, we conclude that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

Theorem 8. *A BF_S $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$ if and only if it satisfies* (9) *and the following condition:*

$$(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}) \left(\begin{array}{l} \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) \geq \min\{\Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3}), \Omega^+(\hbar_{\mathfrak{a}_2})\}, \\ \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) \leq \max\{\Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3}), \Omega^-(\hbar_{\mathfrak{a}_2})\}. \end{array} \right) \tag{17}$$

Proof. Let us assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. By definition, for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}$, the following holds: Since $(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}$, for any $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}$,

the condition $\hbar_{\mathfrak{a}_2} \odot ((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3}) \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_2} \odot (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_3} \leq_{\mathcal{H}} \hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}$ holds. Therefore, we have the following inequalities:

$$\begin{aligned} \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) &\geq \Omega^+(\hbar_{\mathfrak{a}_3}) \\ &\geq \Omega^+(\hbar_{\mathfrak{a}_2} \odot (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})) \\ &= \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \Omega^+(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})\} \\ &\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2}), \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3})\} \end{aligned}$$

and, similarly for the negative part,

$$\begin{aligned} \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) &\leq \Omega^-(\hbar_{\mathfrak{a}_3}) \\ &\leq \Omega^-(\hbar_{\mathfrak{a}_2} \odot (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})) \\ &= \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \Omega^-(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3})\} \\ &\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2}), \Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_3})\}. \end{aligned}$$

This confirms that the structure Ω satisfies the condition in (17).

Conversely, assume that $\Omega = (\Omega^+, \Omega^-)$ satisfies both (9) and (17). By substituting $\hbar_{\mathfrak{a}_1} = 1$ in (17), we obtain the condition in (12). Thus, by applying Theorem 1, we conclude that $\Omega = (\Omega^+, \Omega^-)$ is indeed a BFF of $\mathcal{H}$. □

Definition 9. *A BF_S $\Omega = (\Omega^+, \Omega^-)$ is called an implicative bipolar fuzzy filter (briefly, IBFF) of a hoop algebra $\mathcal{H}$ if it satisfies the condition given by Equation* (9) *and*

$$(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}) \left(\begin{array}{l} \Omega^+(\hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(x \to ((\hbar_{\mathfrak{a}_2} \to z) \to y))\} \\ \Omega^-(\hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(x \to ((\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}) \to \hbar_{\mathfrak{a}_2}))\} \end{array} \right). \tag{18}$$

Example 4. *Let $\mathcal{H} = \{0, 1, 2, 3, 4, 5, 6\}$ be a set with the binary operations $\cdot$ and $\to$ given in the following Tables 6 and 7.*

Then, $(\mathcal{H}, \odot, \to, 1)$ is a hoop algebra. Let $\Omega = (\ \mathcal{H}\ , \Omega^-, \Omega^+)$ be a BFS in $\mathcal{H}$ given by Table 8.

Then, it is easy to check that the BFS $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ in $\mathcal{H}$ is an IBFF of $\mathcal{H}$.

Table 6. Cayley table of the binary operation $\to$.

$\to$	**0**	**1**	**2**	**3**	**4**	**5**
0	1	1	1	4	4	5
1	0	1	2	3	4	5
2	0	1	1	3	4	5
3	1	1	1	1	1	5
4	0	1	1	0	1	5
5	1	1	1	1	1	1

Table 7. Cayley table of the binary operation $\odot$.

$\odot$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	3	3	5
1	0	1	2	3	4	5
2	0	2	2	3	4	5
3	3	3	3	3	3	5
4	3	4	4	3	4	5
5	5	5	5	5	5	5

Table 8. Tabular representation of $\Omega = (\ \mathcal{H}\ , \Omega^-, \Omega^+)$.

$\mathcal{H}$	**0**	**1**	**2**	**3**	**4**	**5**
$\Omega^-(\hbar_{\mathfrak{a}})$	-0.83	-0.83	-0.83	-0.83	-0.83	-0.7
$\Omega^+(\hbar_{\mathfrak{a}})$	0.7	0.7	0.7	0.7	0.7	0.6

The following theorem introduces implicative bipolar fuzzy filters (IBFFs) as a specialized subset of BFFs, enriching the filter hierarchy.

Theorem 9. *Every IBFF is a BFF.*

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be an IBFF of $\mathcal{H}$. If we take $\hbar_{\mathfrak{a}_3} = 1$ in Equation (18) and use Proposition 1 (a5), then we obtain (12). Therefore, by Theorem 1, $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

The converse of Theorem 9 may not be true, as seen in the following example.

Example 5. *Consider the BFF $\Omega = (\mathcal{H}, \Omega^-, \Omega^+)$ of a hoop algebra $(\mathcal{H}, \odot, \to, 1)$ in Example 2. However, it is not an IBFF of $\mathcal{H}$ since*

$$\begin{aligned} \Omega^-(5) = -0.7 \not\leq -0.8 &= \max\{-0.8, -0.8\} \\ &= \max\{\Omega^-(1), \Omega^-(2)\} \\ &= \max\{\Omega^-(4), \Omega^-(4 \to ((5 \to 0) \to 5))\} \end{aligned}$$

and

$$\begin{aligned} \Omega^+(5) = 0.7 \not\geq 0.8 &= \min\{0.8, 0.8\} \\ &= \max\{\Omega^-(1), \Omega^-(2)\} \\ &= \min\{\Omega^+(1), \Omega^+(1 \to ((5 \to 6) \to 5))\}. \end{aligned}$$

Proposition 5. *Every IBFF $\Omega = (\Omega^+, \Omega^-)$ of $\mathcal{H}$ satisfies the following assertions.*

$$(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \leq \Omega^+(\hbar_{\mathfrak{a}_1}) \\ \Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \geq \Omega^-(\hbar_{\mathfrak{a}_1}) \end{pmatrix}. \tag{19}$$

$$(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) = \Omega^+(1) \\ \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) = \Omega^-(1) \end{pmatrix}. \tag{20}$$

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be an IBFF of a hoop algebra H. If we set $\hbar_{\mathfrak{a}_2} = \hbar_{\mathfrak{a}_1}$, $\hbar_{\mathfrak{a}_1} = 1$ and $\hbar_{\mathfrak{a}_3} = \hbar_{\mathfrak{a}_2}$ in Equation (18) and use Proposition 1 (a5) and (9), then we obtain (19). Using (19), Definition 2 (H1), Proposition 1 (a5), (a7), (a9), and (11), we obtain

$$\begin{aligned} &\Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \\ &\geq \Omega^+(((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to (((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1})) \\ &= \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to ((((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1})) \\ &\geq \Omega^+(((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})) \\ &\geq \Omega^+(\hbar_{\mathfrak{a}_1} \to (((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1})) \\ &= \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1})) \\ &= \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to 1) \\ &= \Omega^+(1) \end{aligned}$$

and

$$
\begin{aligned}
&\Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1})\\
&\leq \Omega^-(((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to (((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}))\\
&= \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to (((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}))\\
&\leq \Omega^-(((((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\\
&\leq \Omega^-(\hbar_{\mathfrak{a}_1} \to (((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to x))\\
&= \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}))\\
&= \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to 1)\\
&= \Omega^-(1),
\end{aligned}
$$

for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$. It follows from (9) that we have (20). □

Proposition 6. *Let $\mathcal{H}$ be a bounded hoop algebra. Then, every IBFF $\Omega = (\Omega^+, \Omega^-)$ of $\mathcal{H}$ satisfies the following assertions:*

$$
(\forall\, \hbar_{\mathfrak{a}_1} \in \mathcal{H}) \begin{pmatrix} \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) = \Omega^+(1) \\ \Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) = \Omega^-(1) \end{pmatrix} \tag{21}
$$

$$
(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}) \begin{pmatrix} \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \geq \Omega^+((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}) \\ \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \leq \Omega^-((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}) \end{pmatrix} \tag{22}
$$

$$
(\forall\, \hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2}, \hbar_{\mathfrak{a}_3} \in \mathcal{H}) \begin{pmatrix} \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}), \Omega^+(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_3} \to \hbar_{\mathfrak{a}_2}))\} \\ \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_3}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_3}), \Omega^-(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_3} \to \hbar_{\mathfrak{a}_2}))\} \end{pmatrix}. \tag{23}
$$

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be an IBFF of a bounded hoop algebra $\mathcal{H}$. Then, by Theorem 9, $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$.

If we take $\hbar_{\mathfrak{a}_2} = 0$ in Equation (20), then

$$
\Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \Omega^+(((\hbar_{\mathfrak{a}} \to 0) \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}_1}) = \Omega^+(1),
$$

$$
\Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \Omega^-(((\hbar_{\mathfrak{a}} \to 0) \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}_1}) = \Omega^-(1)
$$

for all $\hbar_{\mathfrak{a}} \in \mathcal{H}$.

Note that $\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \leq_{\mathcal{H}} (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})$ for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$. It follows from Definition 2 (H3) and Equation (11) that

$$
\Omega^+((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}) = \Omega^+(\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})) \leq \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})),
$$

$$
\Omega^-((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}) = \Omega^-(\hbar_{\mathfrak{a}_2} \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})) \geq \Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})). \tag{24}
$$

Combining Proposition 1 (a5) and Equations (9), (18) and (24), we obtain

$$
\begin{aligned}
\Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) &\geq \min\{\Omega^+(1), \Omega^+(1 \to (((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to 0) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})))\}\\
&= \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to 0) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\\
&= \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\\
&\geq \Omega^+((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2})
\end{aligned}
$$

and

$$\begin{aligned}\Omega^-(\hbar_{a_1}\to\hbar_{a_2}) &\le \max\{\Omega^-(1),\Omega^-(1\to(((\hbar_{a_1}\to\hbar_{a_2})\to 0)\to(\hbar_{a_1}\to\hbar_{a_2})))\}\\ &= \Omega^-(((\hbar_{a_1}\to\hbar_{a_2})\to 0)\to(\hbar_{a_1}\to\hbar_{a_2}))\\ &= \Omega^-((\hbar_{a_1}\to\hbar_{a_2})\to(\hbar_{a_1}\to\hbar_{a_2}))\\ &\le \Omega^-((\hbar_{a_1}\odot\hbar_{a_2})\to\hbar_{a_2}).\end{aligned}$$

This proves Equation (22).

Using (HP3) and Equations (14) and (22), we have

$$\begin{aligned}\Omega^+(\hbar_{a_1}\to\hbar_{a_3}) &\ge \Omega^+((\hbar_{a_1}\odot\hbar_{a_3})\to\hbar_{a_3})\\ &\ge \min\{\Omega^+((x\odot z)\to\hbar_{a_2}),\Omega^+(\hbar_{a_2}\to\hbar_{a_3})\}\\ &= \min\{\Omega^+(\hbar_{a_1}\to(\hbar_{a_3}\to\hbar_{a_2})),\Omega^+(\hbar_{a_2}\to\hbar_{a_3})\}\end{aligned}$$

and

$$\begin{aligned}\Omega^-(\hbar_{a_1}\to\hbar_{a_3}) &\le \Omega^-((\hbar_{a_1}\odot\hbar_{a_3})\to\hbar_{a_3})\\ &\le \max\{\Omega^-((\hbar_{a_1}\odot\hbar_{a_3})\to\hbar_{a_2}),\Omega^-(\hbar_{a_2}\to\hbar_{a_3})\}\\ &= \max\{\Omega^-(\hbar_{a_1}\to(\hbar_{a_3}\to\hbar_{a_2})),\Omega^-(\hbar_{a_2}\to\hbar_{a_3})\},\end{aligned}$$

which proves Equation (23). □

Theorem 10. *Let $\mathcal{H}$ be a hoop algebra. The BF_S $\Omega=(\Omega^+,\Omega^-)$ is an IBFF of $\mathcal{H}$ if and only if its nonempty bipolar fuzzy level sets $\mathcal{U}(\Omega^+,t)$ and $\mathcal{L}(\Omega^-,s)$ are implicative filters of $\mathcal{H}$ for all $(t,s)\in[0,1]\times[0,1]$ with $t+s\le 1$.*

Proof. The proof follows similarly to that of Theorem 3. □

We provide conditions under which a BFF is an IBFF.

Theorem 11. *If a BFF $\Omega=(\Omega^+,\Omega^-)$ of $\mathcal{H}$ satisfies condition* (20)*, then it is an IBFF of $\mathcal{H}$.*

Proof. Let $\hbar_{a_1},\hbar_{a_2},\hbar_{a_3}\in\mathcal{H}$. Then, we have

$$\begin{aligned}\Omega^+(\hbar_{a_2}) &\ge \min\{\Omega^+(((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\to\hbar_{a_2}),\Omega^+((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\}\\ &= \min\{\Omega^+(1),\Omega^+((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\}\\ &= \Omega^+((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\\ &\ge \min\{\Omega^+(\hbar_{a_1}),\Omega^+(\hbar_{a_1}\to((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2}))\}\end{aligned}$$

and

$$\begin{aligned}\Omega^-(\hbar_{a_2}) &\le \max\{\Omega^-(((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\to\hbar_{a_2}),\Omega^-((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\}\\ &= \max\{\Omega^-(1),\Omega^-((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2})\}\\ &= \Omega^-((\hbar_{a_2}\to z)\to\hbar_{a_2})\\ &\le \max\{\Omega^-(\hbar_{a_1}),\Omega^-(\hbar_{a_1}\to((\hbar_{a_2}\to\hbar_{a_3})\to\hbar_{a_2}))\}.\end{aligned}$$

This follows from (9), (12) and (20). Therefore, $\Omega=(\Omega^+,\Omega^-)$ is an IBFF of $\mathcal{H}$. □

Theorem 12. *If a BFF $\Omega=(\Omega^+,\Omega^-)$ of $\mathcal{H}$ satisfies condition* (19)*, then it is an IBFF of $\mathcal{H}$.*

Proof. Let $\Omega=(\Omega^+,\Omega^-)$ be a BFF of $\mathcal{H}$ that satisfies (19). As shown in Proposition 5, (19) implies (20). Thus, by Theorem 11, $\Omega=(\Omega^+,\Omega^-)$ is an IBFF of $\mathcal{H}$. □

Theorem 13. *If a BFF $\Omega=(\Omega^+,\Omega^-)$ of $\mathcal{H}$ satisfies condition* (21)*, then it is an IBFF of $\mathcal{H}$.*

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of $\mathcal{H}$ that satisfies (21). Note that for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{H}$,

$$(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1} \leq ((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}.$$

By using (9), (11) and (21), we obtain the following:

$$\begin{aligned} \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) &\leq \Omega^+(1) \\ &= \Omega^+((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \\ &\leq \Omega^+(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \end{aligned}$$

and

$$\begin{aligned} \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) &\geq \Omega^-(1) \\ &= \Omega^-((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}) \\ &\geq \Omega^-(((\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_1}) \to \hbar_{\mathfrak{a}_1}). \end{aligned}$$

Thus, (20) holds and, therefore, $\Omega = (\Omega^+, \Omega^-)$ is an IBFF of $\mathcal{H}$ by Theorem 11. □

Theorem 14. *If a BFF $\Omega = (\Omega^+, \Omega^-)$ of $\mathcal{H}$ satisfies condition* (22)*, then it is an IBFF of $\mathcal{H}$.*

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of $\mathcal{H}$ that satisfies condition (22). For any $\hbar_{\mathfrak{a}} \in \mathcal{H}$, we have the following:

$$\begin{aligned} \Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) &\leq \Omega^+(1) \\ &= \Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to (\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}})) \\ &= \Omega^+((\hbar_{\mathfrak{a}} \to x) \to \hbar_{\mathfrak{a}}) \\ &\leq \Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \end{aligned}$$

and, similarly,

$$\begin{aligned} \Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) &\geq \Omega^-(1) \\ &= \Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to (\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}})) \\ &= \Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \\ &\geq \Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}). \end{aligned}$$

These inequalities follow from Definition 2 (H1), (H3), (9), and (22). Therefore, (21) holds and, thus, by Theorem 13, $\Omega = (\Omega^+, \Omega^-)$ is an IBFF of $\mathcal{H}$. □

Theorem 15. *If a BFF $\Omega = (\Omega^+, \Omega^-)$ of $\mathcal{H}$ satisfies condition* (23)*, then it is an IBFF of $\mathcal{H}$.*

Proof. Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of $\mathcal{H}$ that satisfies condition (23). Condition (23) implies that

$$\begin{aligned} \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) &\geq \min\{\Omega^+(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_2}), \Omega^+(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_2}))\} \\ &= \min\{\Omega^+(1), \Omega^+((x \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2})\} \\ &= \Omega^+((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}) \end{aligned}$$

and, similarly,

$$\begin{aligned}\Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}) &\leq \max\{\Omega^-(\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_2}), \Omega^-(\hbar_{\mathfrak{a}_1} \to (\hbar_{\mathfrak{a}_2} \to \hbar_{\mathfrak{a}_2}))\} \\ &= \max\{\Omega^-(1), \Omega^-((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2})\} \\ &= \Omega^-((\hbar_{\mathfrak{a}_1} \odot \hbar_{\mathfrak{a}_2}) \to \hbar_{\mathfrak{a}_2}).\end{aligned}$$

Thus, (22) is valid and, therefore, by Theorem 14, $\Omega = (\Omega^+, \Omega^-)$ is an IBFF of $\mathcal{H}$. □

Theorem 16. *Let $\Omega = (\Omega^+, \Omega^-)$ and $\varrho = (\varrho^+, \varrho^-)$ be BFFs of a hoop algebra $\mathcal{H}$ such that*

$$\Omega^+(1) = \varrho^+(1), \quad \Omega^-(1) = \varrho^-(1), \tag{25}$$

$$\Omega^+(\hbar_{\mathfrak{a}}) \leq \varrho^+(\hbar_{\mathfrak{a}}), \quad \Omega^-(\hbar_{\mathfrak{a}}) \geq \varrho^-(\hbar_{\mathfrak{a}}), \tag{26}$$

for all $\hbar_{\mathfrak{a}} \in \mathcal{H}$. If $\Omega = (\Omega^+, \Omega^-)$ is an IBFF of $\mathcal{H}$, then $\varrho = (\varrho^+, \varrho^-)$ is also an IBFF of $\mathcal{H}$.

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is an IBFF of $\mathcal{H}$. By Theorem 9, this implies that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$.

For any $\hbar_{\mathfrak{a}} \in \mathcal{H}$, we have

$$\Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \geq \Omega^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \Omega^+(1) = \varrho^+(1)$$

and

$$\Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \leq \Omega^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \Omega^-(1) = \varrho^-(1),$$

where the equalities follow from (25), (26), and (21).

Since $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$, we know from (9) that

$$\varrho^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \leq \varrho^+(1) \quad \text{and} \quad \varrho^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) \geq \varrho^-(1).$$

Thus, for all $\hbar_{\mathfrak{a}} \in \mathcal{H}$, we conclude

$$\varrho^+((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \varrho^+(1) \quad \text{and} \quad \varrho^-((\hbar_{\mathfrak{a}} \to \hbar_{\mathfrak{a}}) \to \hbar_{\mathfrak{a}}) = \varrho^-(1).$$

This shows that $\varrho = (\varrho^+, \varrho^-)$ satisfies the conditions of an IBFF of $\mathcal{H}$. Therefore, by Theorem 13, $\varrho = (\varrho^+, \varrho^-)$ is an IBFF of $\mathcal{H}$. □

Proposition 7. *If $\Omega_{\mathfrak{k}} = (\Omega^+_{\mathfrak{k}}, \Omega^-_{\mathfrak{k}})$ for all $\mathfrak{k} \in \Gamma$ is a family of bipolar fuzzy filters of a hoop algebra $\mathcal{H}$, then*

$$\bigwedge_{\mathfrak{k}\in\Gamma} \Omega_{\mathfrak{k}} = (\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}}, \bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})$$

is a BFF of $\mathcal{H}$.

Proof. Let $\Omega_{\mathfrak{k}} = \{(\Omega^+_{\mathfrak{k}}, \Omega^-_{\mathfrak{k}}) : \mathfrak{k} \in \Gamma\}$ be a family of bipolar fuzzy filters of a hoop $\mathcal{H}$. Let $\hbar_{\mathfrak{a}} \in \mathcal{H}$, and we have

$$(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}})(1) = \inf_{\mathfrak{k}\in\Gamma}\{\Omega^+_{\mathfrak{k}}(1)\} \geq \inf_{\mathfrak{k}\in\Gamma}\{\Omega^+_{\mathfrak{k}}(\hbar_{\mathfrak{a}})\} = (\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}})(\hbar_{\mathfrak{a}}),$$

$$(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})(1) = \sup_{\mathfrak{k}\in\Gamma}\{\Omega^-_{\mathfrak{k}}(1)\} \leq \sup_{\mathfrak{k}\in\Gamma}\{\Omega^-_{\mathfrak{k}}(\hbar_{\mathfrak{a}})\} = (\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})(\hbar_{\mathfrak{a}}).$$

Let $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$. Then, we have

$$\begin{aligned}
(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}})(\hbar_{a_2}) &= \inf_{\mathfrak{k}\in\Gamma}\{\Omega^+_{\mathfrak{k}}(\hbar_{a_2})\} \\
&\geq \inf_{\mathfrak{k}\in\Gamma}\{\min\{\Omega^+_{\mathfrak{k}}(\hbar_{a_1}), \Omega^+_{\mathfrak{k}}(\hbar_{a_1} \to \hbar_{a_2})\}\} \\
&= \min\{\inf_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}}(\hbar_{a_1}), \inf_{\mathfrak{k}\in\Gamma} \Omega^+_{i}(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= \min\{(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}})(\hbar_{a_1}), (\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^+_{\mathfrak{k}})(\hbar_{a_1} \to \hbar_{a_2})\}
\end{aligned}$$

and

$$\begin{aligned}
(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})(\hbar_{a_2}) &= \sup_{\mathfrak{k}\in\Gamma}\{\Omega^-_{\mathfrak{k}}(\hbar_{a_2})\} \\
&\leq \sup_{\mathfrak{k}\in\ \Gamma}\{\max\{\Omega^-_{\mathfrak{k}}(\hbar_{a_1}), \Omega^-_{\mathfrak{k}}(\hbar_{a_1} \to \hbar_{a_2})\}\} \\
&= \max\{\sup_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}}(\hbar_{a_1}), \sup_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}}(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= \max\{(\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})(\hbar_{a_1}), (\bigwedge_{\mathfrak{k}\in\Gamma} \Omega^-_{\mathfrak{k}})(\hbar_{a_1} \to \hbar_{a_2})\}.
\end{aligned}$$

Hence, $\bigwedge_{i\in\Gamma} \Omega_i$ is a BFF of a hoop $\mathcal{H}$. □

Lemma 1. *Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of a hoop algebra $\mathcal{H}$ if and only if Ω^+ and $\overline{\Omega^-}$ are fuzzy filters of $\mathcal{H}$.*

Proof. Assume that $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. Then, by definition, Ω^+ is a fuzzy filter of $\mathcal{H}$. For every $\hbar_a \in \mathcal{H}$, we have

$$\overline{\Omega^-}(1) = -1 - \Omega^-(1) \geq -1 - \Omega^-(\hbar_a) = \overline{\Omega^-}(\hbar_a).$$

Let $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$. Then, we have

$$\begin{aligned}
\overline{\Omega^-}(\hbar_{a_2}) &= -1 - \Omega^-(\hbar_{a_2}) \\
&\geq -1 - \max\{\Omega^-(x), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= \min\{-1 - \Omega^-(\hbar_{a_1}), -1 - \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= \min\{\overline{\Omega^-}(\hbar_{a_1}), \overline{\Omega^-}(\hbar_{a_1} \to \hbar_{a_2})\}.
\end{aligned}$$

Thus, $\overline{\Omega^-}$ is a fuzzy filter of $\mathcal{H}$.

Conversely, assume that Ω^+ and $\overline{\Omega^-}$ are fuzzy filters of $\mathcal{H}$. Then, for every $\hbar_a \in \mathcal{H}$, we have $\Omega^+(1) \geq \Omega^+(\hbar_a)$ and

$$-1 - \Omega^-(1) = \overline{\Omega^-}(1) \geq \overline{\Omega^-}(\hbar_a) = -1 - \Omega^-(\hbar_a),$$

i.e., $\Omega^-(1) \leq \Omega^-(\hbar_a)$. Let $\hbar_{a_1}, \hbar_{a_2} \in \mathcal{H}$. Then, we have

$$\Omega^+(\hbar_{a_2}) \geq \min\{\Omega^+(\hbar_{a_1}), \Omega^+(\hbar_{a_1} \to \hbar_{a_2})\}.$$

Also,

$$\begin{aligned}
-1 - \Omega^-(\hbar_{a_2}) &= \overline{\Omega^-}(\hbar_{a_2}) \\
&\geq \min\{\overline{\Omega^-}(\hbar_{a_1}), \overline{\Omega^-}(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= \min\{-1 - \Omega^-(\hbar_{a_1}), -1 - \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\} \\
&= -1 - \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}.
\end{aligned}$$

Thus, $\Omega^-(\hbar_{a_2}) \leq \max\{\Omega^-(\hbar_{a_1}), \Omega^-(\hbar_{a_1} \to \hbar_{a_2})\}$. Therefore, $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

Theorem 17. *Let $\Omega = (\Omega^+, \Omega^-)$ be a BFF of $\mathcal{H}$ if and only if $(\Omega^+, \overline{\Omega^+})$ and $(\Omega^-, \overline{\Omega^-})$ are fuzzy filters of $\mathcal{H}$.*

Proof. If a BFS $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$, then by Lemma 1, Ω^+ and Ω^- are fuzzy filters of $\mathcal{H}$. Hence, $(\Omega^+, \overline{\Omega^+})$ and $(\Omega^-, \overline{\Omega^-})$ are bipolar fuzzy filters of $\mathcal{H}$.

Conversely, if $(\Omega^+, \overline{\Omega^+})$ and $(\Omega^-, \overline{\Omega^-})$ are fuzzy filters of $\mathcal{H}$, then Ω^+ and $\overline{\Omega^-}$ are fuzzy filters of $\mathcal{H}$. Therefore, the BFS $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{H}$. □

Definition 10. *Let $\Omega = (\Omega^+, \Omega^-)$ be a BFS in $\mathcal{H}$. We define the subset $\Omega^{-1}(1,1)$ of $\mathcal{H}$ by*

$$\Omega^{-1}(1,1) = \{\hbar_{\mathfrak{a}} \in \mathcal{H} \mid \Omega^-(\hbar_{\mathfrak{a}}) = \Omega^-(1) \text{ and } \Omega^+(x) = \Omega^+(1)\}.$$

Theorem 18. *If $\Omega = (\Omega^+, \Omega^-)$ is a bipolar fuzzy sub-hoop of the hoop $\mathcal{H}$, then $\Omega^{-1}(1,1)$ is a sub-hoop of $\mathcal{H}$.*

Proof. Clearly, $1 \in \Omega^{-1}(1,1)$. Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \Omega^{-1}(1,1)$. Then, $\Omega^-(\hbar_{\mathfrak{a}_1}) = \Omega^-(1)$, $\Omega^+(\hbar_{\mathfrak{a}_1}) = \Omega^+(1)$, $\Omega^-(\hbar_{\mathfrak{a}_2}) = \Omega^-(1)$, and $\Omega^+(\hbar_{\mathfrak{a}_2}) = \Omega^+(1)$. Thus, for $\bullet \in \{\odot, \to\}$, we have

$$\Omega^-(1) \leq \Omega^-(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \leq \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_2})\} = \max\{\Omega^-(1), \Omega^-(1)\} = \Omega^-(1)$$

and

$$\Omega^+(1) \geq \Omega^+(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) \geq \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_2})\} = \min\{\Omega^+(1), \Omega^+(1)\} = \Omega^+(1).$$

Thus, $\Omega^-(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) = \Omega^-(1)$ and $\Omega^+(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) = \Omega^+(1)$, which means that $\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2} \in \Omega^{-1}(1,1)$. Therefore, $\Omega^{-1}(1,1)$ is a sub-hoop of $\mathcal{H}$. □

A mapping $\alpha : \mathcal{X} \to \mathcal{Y}$ of hoops is called a homomorphism if

$$\vartheta(\hbar_{\mathfrak{a}_1} \bullet \hbar_{\mathfrak{a}_2}) = \vartheta(\hbar_{\mathfrak{a}_1}) \bullet \vartheta(\hbar_{\mathfrak{a}_2})$$

for all $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{X}$ and $\bullet \in \{\odot, \to\}$. Note that if $\vartheta : \mathcal{X} \to \mathcal{Y}$ is a homomorphism of hoops, then $\vartheta(1) = 1$.

Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be a homomorphism of hoops. For any BFS $\Omega = (\Omega^+, \Omega^-)$ in $\mathcal{X}$, we define a new BFS $\vartheta(\Omega) = (\vartheta_{\sup}(\Omega^+), \vartheta_{\inf}(\Omega^-))$ in $\mathcal{Y}$, where

$$\vartheta_{\sup}(\Omega^+)(\hbar_{\mathfrak{a}_2}) = \begin{cases} \sup\limits_{\hbar_{\mathfrak{a}_1} \in \vartheta^{-1}(\hbar_{\mathfrak{a}_2})} \Omega^+(\hbar_{\mathfrak{a}_1}) & \text{if } \vartheta^{-1}(\hbar_{\mathfrak{a}_2}) \neq \emptyset, \\ 0 & \text{otherwise} \end{cases}$$

and

$$\vartheta_{\inf}(\Omega^-)(\hbar_{\mathfrak{a}_2}) = \begin{cases} \inf\limits_{\hbar_{\mathfrak{a}_1} \in \vartheta^{-1}(\hbar_{\mathfrak{a}_2})} \Omega^-(\hbar_{\mathfrak{a}_1}) & \text{if } \vartheta^{-1}(\hbar_{\mathfrak{a}_2}) \neq \emptyset, \\ 0 & \text{otherwise} \end{cases}$$

for each $\hbar_{\mathfrak{a}_2} \in \mathcal{Y}$.

For any BFS $\Omega = (\Omega^+, \Omega^-)$ in $\mathcal{Y}$, we define a new BFS $\vartheta^{-1}(\Omega) = \{(\hbar_{\mathfrak{a}}, \vartheta^{-1}(\Omega^+)(\hbar_{\mathfrak{a}}), \vartheta^{-1}(\Omega^-)(\hbar_{\mathfrak{a}})) \mid \hbar_{\mathfrak{a}} \in \mathcal{X}\}$.

The following theorem demonstrates that BFFs are preserved under hoop homomorphisms, ensuring their applicability in transformed algebraic systems.

Theorem 19. *Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be a homomorphism of hoops. If a BFS $\Omega = (\mathcal{X}, \Omega^-, \Omega^+)$ is a BFF of $\mathcal{X}$, then $\vartheta(\Omega) = \{(\hbar_\mathfrak{a}, \vartheta_{\sup}(\Omega^+)(\hbar_\mathfrak{a}), \alpha_{\inf}(\Omega^-)(\hbar_\mathfrak{a})) \mid \hbar_\mathfrak{a} \in \mathcal{Y}\}$ is a BFF of $\mathcal{Y}$.*

Proof. For all $\hbar_\mathfrak{a} \in \mathcal{X}$, we have

$$\vartheta(\Omega^+)(\hbar_\mathfrak{a}) = \Omega^+(\vartheta(\hbar_\mathfrak{a})) \leq \Omega^+(1) = \Omega^+(\vartheta(1)) = \vartheta(\Omega^+)(1),$$

$$\vartheta(\Omega^-)(\hbar_\mathfrak{a}) = \Omega^-(\vartheta(\hbar_\mathfrak{a})) \geq \Omega^-(1) = \Omega^-(\vartheta(1)) = \vartheta(\Omega^-)(1).$$

Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{X}$. Then,

$$\begin{aligned} \vartheta(\Omega^+)(\hbar_{\mathfrak{a}_2}) &= \Omega^+(\vartheta(\hbar_{\mathfrak{a}_2})) \\ &\geq \min\{\Omega^+(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^+(\vartheta(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\} \\ &= \min\{\vartheta(\Omega^+)(\hbar_{\mathfrak{a}_1}), \vartheta(\Omega^+)(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}, \end{aligned}$$

$$\begin{aligned} \vartheta(\Omega^-)(\hbar_{\mathfrak{a}_2}) &= \Omega^-(\vartheta(\hbar_{\mathfrak{a}_2})) \\ &\leq \max\{\Omega^-(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^-(\vartheta(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\} \\ &= \max\{\vartheta(\Omega^-)(\hbar_{\mathfrak{a}_1}), \vartheta(\Omega^-)(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}. \end{aligned}$$

Hence, $\vartheta(\Omega) = (\vartheta(\Omega^+), \vartheta(\Omega^-))$ is a BFF of $\mathcal{Y}$. □

The following theorem extends the preservation of BFSH properties under homomorphisms, reinforcing their algebraic stability.

Theorem 20. *Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be an epimorphism of hoops and let $\Omega = (\Omega^-, \Omega^+)$ be a BFS in $\mathcal{X}$. If $\vartheta(\Omega) = (\vartheta(\Omega^+), \vartheta(\Omega^-))$ is a BFF of $\mathcal{Y}$, then $\Omega = (\Omega^-, \Omega^+)$ is a BFF of $\mathcal{X}$.*

Proof. For any $\hbar_\mathfrak{a} \in \mathcal{Y}$, there exist $\mathfrak{p} \in \mathcal{X}$ such that $\vartheta(\mathfrak{p}) = \hbar_\mathfrak{a}$. Then,

$$\Omega^+(\hbar_\mathfrak{a}) = \Omega^+(\vartheta(\mathfrak{p})) = \alpha(\Omega^+)(\mathfrak{p}) \leq \alpha(\Omega^+)(1) = \Omega^+(\vartheta(1)) = \Omega^+(1),$$

$$\Omega^-(\hbar_\mathfrak{a}) = \Omega^-(\vartheta(\mathfrak{p})) = \vartheta(\Omega^-)(\mathfrak{p}) \geq \alpha(\Omega^-)(1) = \Omega^-(\vartheta(1)) = \Omega^-(1).$$

Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{Y}$. Then, there exist $\mathfrak{p}, \mathfrak{q} \in \mathcal{X}$ such that $\vartheta(\mathfrak{p}) = \hbar_{\mathfrak{a}_1}$, $\vartheta(\mathfrak{q}) = \hbar_{\mathfrak{a}_2}$. It follows that

$$\begin{aligned} \Omega^+(\hbar_{\mathfrak{a}_2}) &= \Omega^+(\vartheta(\mathfrak{q})) \\ &\geq \min\{\Omega^+(\vartheta(\mathfrak{p})), \Omega^+(\vartheta(\mathfrak{p}) \to \vartheta(\mathfrak{q}))\} \\ &= \min\{\Omega^+(\hbar_{\mathfrak{a}_1}), \Omega^+(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\} \end{aligned}$$

and

$$\begin{aligned} \Omega^-(\hbar_{\mathfrak{a}_2}) &= \Omega^-(\vartheta(\mathfrak{q})) \\ &\leq \max\{\Omega^-(\vartheta(\mathfrak{p})), \Omega^-(\vartheta(\mathfrak{p}) \to \alpha(\mathfrak{q}))\} \\ &= \max\{\Omega^-(\hbar_{\mathfrak{a}_1}), \Omega^-(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}. \end{aligned}$$

Hence, $\Omega = (\Omega^-, \Omega^+)$ is a BFF of $\mathcal{X}$. □

Theorem 21. *Let $\vartheta : \mathcal{X} \to \mathcal{Y}$ be a homomorphism of hoops and $\Omega = (\Omega^-, \Omega^+)$ be a BFS in $\mathcal{Y}$. If $\Omega = (\Omega^+, \Omega^-)$ is a BFF of $\mathcal{Y}$, then $\vartheta^{-1}(\Omega) = (\Omega^+_{\vartheta^{-1}(\mathcal{Y})}, \Omega^-_{\vartheta^{-1}(\mathcal{Y})})$ is a BFF of $\mathcal{X}$.*

Proof. Since ϑ is a homomorphism of $\mathcal{X}$ into $\mathcal{Y}$, then $\vartheta(1) = 1 \in \mathcal{Y}$ and, by the assumption, $\Omega^+(\vartheta(1)) = \Omega^+(1) \geq \Omega^+(\hbar_{\mathfrak{a}_2})$ for every $\hbar_{\mathfrak{a}_2} \in \mathcal{Y}$. In particular, $\Omega^+_\mathcal{Y}(\vartheta(1)) \geq \Omega^+_\mathcal{Y}(\vartheta(\hbar_{\mathfrak{a}_1}))$ for $\hbar_{\mathfrak{a}_1} \in \mathcal{X}$. Hence, $\Omega^+_{\vartheta^{-1}(\mathcal{Y})}(1) \geq \Omega^+_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1})$. Also, $\Omega^-(\vartheta(1)) = \Omega^-(1) \leq \Omega^-(\hbar_{\mathfrak{a}_2})$ for

every $\hbar_{\mathfrak{a}_2} \in \mathcal{Y}$. In particular, $\Omega^-_{\mathcal{Y}}(\alpha(1)) \leq \Omega^-_{\mathcal{Y}}(\vartheta(\hbar_{\mathfrak{a}_1}))$ for $\hbar_{\mathfrak{a}_1} \in \mathcal{X}$. Hence, $\Omega^-_{\vartheta^{-1}(\mathcal{Y})}(1) \leq \Omega^-_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1})$. Let $\hbar_{\mathfrak{a}_1}, \hbar_{\mathfrak{a}_2} \in \mathcal{X}$. Then, by assumption,

$$\begin{aligned}
\Omega^+_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_2}) &= \Omega^+(\vartheta(\hbar_{\mathfrak{a}_2})) \\
&\geq \min\{\Omega^+(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^+(\vartheta(\hbar_{\mathfrak{a}_1}) \to \vartheta(\hbar_{\mathfrak{a}_2}))\} \\
&= \min\{\Omega^+(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^+(\vartheta(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\} \\
&= \min\{\Omega^+_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1}), \Omega^+_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\},
\end{aligned}$$

$$\begin{aligned}
\Omega^-_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_2}) &= \Omega^-(\vartheta(\hbar_{\mathfrak{a}_2})) \\
&\leq \max\{\Omega^-(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^-(\vartheta(\hbar_{\mathfrak{a}_1}) \to \vartheta(\hbar_{\mathfrak{a}_2}))\} \\
&= \max\{\Omega^-(\vartheta(\hbar_{\mathfrak{a}_1})), \Omega^-(\vartheta(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2}))\} \\
&= \max\{\Omega^-_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1}), \Omega^-_{\vartheta^{-1}(\mathcal{Y})}(\hbar_{\mathfrak{a}_1} \to \hbar_{\mathfrak{a}_2})\}.
\end{aligned}$$

Hence, $\vartheta^{-1}(\Omega) = (\Omega^+_{\vartheta^{-1}(\mathcal{Y})}, \Omega^-_{\vartheta^{-1}(\mathcal{Y})})$ is a BFF of $\mathcal{X}$. □

4. Conclusions

This study advances fuzzy logic by introducing bipolar fuzzy sub-hoops (BFSHs) and bipolar fuzzy filters (BFFs) within hoop algebras, enabling the modeling of both positive and negative information in many-valued logic systems. Below, we summarize the key results and achievements of this study:

- Introduced and defined bipolar fuzzy sub-hoops (BFSHs) and bipolar fuzzy filters (BFFs) in hoop algebras, extending fuzzy logic to handle positive and negative memberships.
- Established the interplay between BFSHs and BFFs, proving that every BFF is a BFSH (Theorem 2).
- Characterized BFFs through level sets (Theorem 3) and alternative conditions involving implication and monotonicity (Theorems 1 and 4).
- Defined and characterized implicative bipolar fuzzy filters (IBFFs) as a specialized subset of BFFs (Theorems 10–15).
- Proved the preservation of BFSH and BFF properties under hoop homomorphisms, ensuring robustness in transformed systems (Theorems 19–21).
- Demonstrated that the intersection of BFFs is a BFF (Proposition 7), supporting their algebraic stability.
- Showed that level sets of BFSHs form sub-hoops, connecting fuzzy and classical structures (Theorem 18).

These results find applications in image processing, spatial reasoning, and decision support systems, as detailed in the subsection below. Future research will explore additional algebraic structures, such as bipolar fuzzy rings, and develop computational algorithms for practical applications in image processing, decision-making, and control systems. This work lays a robust foundation for advanced fuzzy logic systems handling complex, contradictory information.

Future work could explore topological indices for fuzzy graphs, such as the fuzzy misbalance prodeg index, which has shown promise in multi-criteria decision-making [new reference]. Applying bipolar fuzzy sub-hoops and filters to such indices could enhance their ability to handle contradictory data in graph-based fuzzy systems.

In image processing, bipolar fuzzy filters enhance edge detection by modeling pixel intensities with positive and negative membership degrees, capturing both desired features (edges) and undesired features (noise). Using the hoop algebra framework, a bipolar

fuzzy filter (BFF), as defined in Definition 8, assigns a positive degree $\Omega^+(x) \in [0,1]$ to pixels with high gradient magnitudes, indicating likely edge presence, and a negative degree $\Omega^-(x) \in [-1,0]$ to pixels with erratic intensity changes, indicating likely noise. For instance, a pixel at an object boundary may have $\Omega^+(x) = 0.9$ and $\Omega^-(x) = -0.1$, while a noisy pixel in a uniform region may have $\Omega^+(x) = 0.2$ and $\Omega^-(x) = -0.8$. The BFF processes these memberships using hoop operations $\odot$ and $\rightarrow$, retaining pixels with high Ω^+ and low Ω^- while suppressing noise, as supported by Theorems 1 and 4 on BFF properties. This dual-membership approach improves segmentation accuracy over traditional fuzzy filters, enabling precise edge detection in applications like medical imaging, where clear tissue boundaries are critical [12].

Author Contributions: Conceptualization, T.O., R.N., R.K.B. and H.B.; methodology, T.O., R.N., R.K.B. and H.B.; writing T.O., R.N., R.K.B. and H.B.; writing—review and editing, T.O., R.N., R.K.B. and H.B.; visualization, T.O., R.N., R.K.B. and H.B.; supervision, T.O., R.N., R.K.B. and H.B. All authors have read and agreed to the published version of the manuscript.

Funding: The fourth author acknowledges the financial support of the Slovenian Research and Innovation Agency (research core funding no. P2-0103).

Data Availability Statement: Data sharing is not applicable as no datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Bosbach, B. Komplementäre Halbgruppen. Axiomatik und Arithmetik. *Funda. Math.* **1969**, *64*, 257–287. [CrossRef]
2. Bosbach, B. Komplementäre Halbgruppen. Kongruenzen und Quatienten. *Funda. Math.* **1970**, *69*, 1–14. [CrossRef]
3. Aaly Kologani, M.; Borzooei, R.A. On ideal theory of hoops. *Math. Bohem.* **2020**, *145*, 141–162. [CrossRef]
4. Aglianó, P.; Ferreirim, I.M.A.; Montagna, F. Basic hoops: An algebraic study of continuous t-norms. *Stud. Log.* **2007**, *87*, 73–98. [CrossRef]
5. Blok, W.J.; Ferreirim, I.M.A. On the structure of hoops. *Algebra Universalis* **2000**, *43*, 233–257. [CrossRef]
6. Borzooei, R.A. Filter theory of hoop-algebras. *J. Adv. Res. Pure Math.* **2014**, *6*, 1–15. [CrossRef]
7. Borzooei, R.A.; Varasteh, H.R.; Borna, K. Fundamental hoop-algebras. *Ratio Math.* **2015**, *29*, 25–40.
8. Georgescu, G.; Leustean, L.; Preoteasa, V. Pseudo-hoops. *J.-Mult.-Valued Log. Soft Comput.* **2005**, *11*, 153–184.
9. Kondo, M. Some types of filters in hoops. In Proceedings of the 41st IEEE International Symposium on Multiple-Valued Logic, Tuusula, Finland, 23–25 May 2011; pp. 50–53. [CrossRef]
10. Namdar, A.; Borzooei, R.A. Nodal filters in hoop algebras. *Soft Comput.* **2018**, *22*, 7119–7128. [CrossRef]
11. Namdar, A.; Borzooei, R.A.; Borumand Saeid, A.; Aaly Kologani, M. Some results in hoop algebras. *J. Intell. Fuzzy Syst.* **2017**, *32*, 1805–1813. [CrossRef]
12. Zhang, W.R. Bipolar fuzzy sets. In Proceedings of the 1998 IEEE International Conference on Fuzzy Systems Proceedings, Anchorage, AK, USA, 4–9 May 1998; pp. 835–840.
13. Zadeh, L.F. Fuzzy sets. *Inf. Control* **1965**, *8*, 338–353. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

Numbers Whose Powers Are Arbitrarily Close to Integers

Artūras Dubickas

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania; arturas.dubickas@mif.vu.lt

Abstract: In this paper, it is proved that, for any sequence of positive numbers ξ_n, $n = 1, 2, \ldots$, which does not converge to zero faster than the exponential function, and any sequence of positive numbers δ_n, $n = 1, 2, 3, \ldots$, there is an uncountable set of positive numbers S such that, for each $\alpha > 1$ in S, there are infinitely many $n \in \mathbb{N}$ for which the fractional parts $\{\xi_n \alpha^n\}$ are smaller than δ_n, regardless of how fast the sequence δ_n tends to zero. In particular, for any sequence bounded away from zero, namely, $\xi_n \geq \xi > 0$ for $n \geq 1$, it is shown that infinitely many integers n for which the inequality $\{\xi_n \alpha^n\} < \delta_n$ is true can be extracted from an arbitrary subsequence $\mathcal{N}$ of positive integers.

Keywords: fractional parts; powers of transcendental numbers; distribution modulo 1

MSC: 11B07; 11J20; 11J71

1. Introduction

Starting from Weyl's 1916 paper [1], various problems related to the distribution of the sequence of fractional parts

$$\{\xi \alpha^n\}, \quad n = 1, 2, 3, \ldots, \tag{1}$$

where $\xi > 0$ and $\alpha > 1$ are two real numbers, were studied. Weyl's result implies that, for each $\alpha > 1$, the sequence (1) is uniformly distributed for almost all $\xi > 0$. See also [2] for a more precise version of this result. In the opposite direction, Koksma [3] proved that, if $\xi > 0$ is fixed, then the sequence (1) is uniformly distributed for almost all $\alpha > 1$. In this respect, the exceptional α are Pisot and Salem numbers. Recall that an algebraic integer $\alpha > 1$ is called a Pisot number if its conjugates over $\mathbb{Q}$ other than α itself (if any) all lie in the open unit disc $|z| < 1$. An algebraic integer $\alpha > 1$ is called a Salem number if its degree over $\mathbb{Q}$ is an even number $d \geq 4$ and $d - 2$ of its conjugates lie on the unit circle $|z| = 1$. (Since such α is reciprocal its other conjugates are α and α^{-1}.) See, for instance, the paper of Pisot and Salem themselves [4], where they proved that, if $\xi = 1$ and $\alpha > 1$ is a Salem number, then the sequence (1) is everywhere dense in $[0, 1]$, but not uniformly distributed in $[0, 1]$. The monographs [5,6] contain some basic information about Pisot and Salem numbers, while in Smyth's review paper [7] there are more recent references. In some literature, Pisot numbers are also called Pisot–Vijayaraghavan numbers or PV numbers; see, for instance, some early papers of Vijayaraghavan on this subject [8–11].

For algebraic numbers α, at least something can be said about the distribution of (1). Extending an earlier result of Flatto, Lagarias, and Pollington for rational $\alpha > 1$ [12], in [13], it was proved that, for each $\xi > 0$ and each algebraic number $\alpha > 1$, there should be a gap between the largest and the smallest limit points of the sequence (1) which depends only on α except if α is a Pisot number or a Salem number when we need an extra

condition $\xi \notin \mathbb{Q}(\alpha)$. This result is not only of interest itself but also has several applications. In particular, it seems to be useful in a so-called Erdős similarity conjecture [14]. The cases when $\xi \in \mathbb{Q}(\alpha)$ and α is a Pisot number or a Salem number were treated in [15,16], respectively; see also [17]. Nevertheless, for example, Mahler's 3/2-problem [18], where he asks whether, for $\alpha = 3/2$, there is a so-called Z-number, namely, $\xi > 0$, such that all elements of (1) lie in $(0, 1/2)$, is unsolved (see [19–21]). However, the situation with any specific transcendental number α is more complicated and less known. For example, it is not known if (1) with $(\xi, \alpha) = (1, e)$ has one or more than one limit point. Determining whether there is a transcendental number $\alpha > 1$ for which the sequence $\{\alpha^n\}$, $n = 1, 2, 3, \dots$, has only finitely many limit points is still a completely open problem as well.

We remark that the behavior of the sequence (1) for $\xi = 1$ and a transcendental number $\alpha > 1$ can be very different depending on α. In [22], it was shown that, for any sequence of real numbers r_n, $n = 1, 2, 3, \dots$, and any $\varepsilon > 0$, there is a transcendental number $\alpha > 1$ such that

$$\|\alpha^n - r_n\| < \varepsilon \tag{2}$$

for all $n \in \mathbb{N}$. (Here, $\|y\|$ is the distance from $y \in \mathbb{R}$ to the nearest integer.) See also two subsequent papers [23,24]. In fact, if we want (2) to hold not for all $n \in \mathbb{N}$, but only for infinitely many n, then this follows from another paper of Koksma [25] with ε replaced by a sequence of positive numbers ε_n such that the series $\sum_{n=1}^{\infty} \varepsilon_n$ are divergent. In [22], it was also shown that, for any sequence of positive numbers δ_n, $n = 1, 2, 3, \dots$, there is a transcendental number $\alpha > 1$ for which the inequality

$$\{\alpha^n\} < \delta_n$$

holds for infinitely many $n \in \mathbb{N}$. This time, there are no conditions or restrictions whatsoever on the rate of convergence of δ_n to zero.

In this paper, it will be shown that, even if we replace in (1) a fixed number $\xi > 0$ by any sequence of positive numbers ξ_n, $n = 1, 2, 3, \dots$, which is not converging to zero faster than the exponential function, then there are "many" numbers $\alpha > 1$ such that $\{\xi_n \alpha^n\}$ is smaller than an arbitrary positive number δ_n for infinitely many $n \in \mathbb{N}$, regardless of how fast the sequence δ_n, $n = 1, 2, 3, \dots$, converges to zero. (This type of sequence, specifically, with $\xi_n = 1/n$ and an integer $\alpha \geq 2$, was considered before; see [26], where their density in $[0, 1]$ was established, and [27–29].) Of course, the theorem stated below holds in the special case when $\xi_n = \xi > 0$ for each $n \in \mathbb{N}$ and, more generally, when ξ_n is bounded away from zero, namely, $\xi_n \geq \xi > 0$ for $n \in \mathbb{N}$.

Theorem 1. *Let $\boldsymbol{\delta} = \{\delta_1, \delta_2, \delta_3, \dots\}$ and $\boldsymbol{\xi} = \{\xi_1, \xi_2, \xi_3, \dots\}$ be two sequences of positive numbers such that*

$$\limsup_{n \to \infty} \frac{\log \xi_n}{n} \geq 0. \tag{3}$$

Then, for any interval $I = [a, b]$, where $1 \leq a < b$, there is an uncountable set $S(\boldsymbol{\delta}, \boldsymbol{\xi}, I) \subset I$ such that, for each $\alpha \in S(\boldsymbol{\delta}, \boldsymbol{\xi}, I)$, the inequalities

$$0 < \{\xi_n \alpha^n\} < \delta_n \tag{4}$$

hold for infinitely many $n \in \mathbb{N}$.

Note that the condition (3) of Theorem 1 cannot be omitted. For example, if $\tau > 0$, $\xi_n = e^{-\tau n}$ and $\delta_n = 1/n!$, then, for each $\alpha \in [1, e^{\tau})$ and each sufficiently large $n \in \mathbb{N}$, we have

$$\{\xi_n \alpha^n\} = \{e^{(\log \alpha - \tau)n}\} = e^{(\log \alpha - \tau)n} > \frac{1}{n!} = \delta_n,$$

so there is no α in the interval $I = [1, e^\tau)$ for which the inequality (4) is true for infinitely many $n \in \mathbb{N}$. Similarly, if $\xi_n = \delta_n = 1/n!$, then there is no $\alpha > 1$ at all for which (4) is true for infinitely many $n \in \mathbb{N}$.

Of course, since the set $S(\boldsymbol{\delta}, \boldsymbol{\xi}, I)$ is uncountable and $\mathbb{Q}$ is countable, $S(\boldsymbol{\delta}, \boldsymbol{\xi}, I)$ contains an uncountable subset of transcendental numbers α with the property (4). Therefore, Theorem 1 is already more general than Theorem 3 of [22] for $\xi_n = 1$.

Replace each δ_j by

$$\delta_j' := \min(1/j, \delta_1, \dots, \delta_j)$$

and set

$$\Phi_j = \lceil 1/\delta_j' \rceil$$

for every $j \in \mathbb{N}$. (Here and below, $\lceil y \rceil$ is the ceiling function, namely, the smallest integer greater than or equal to $y \in \mathbb{R}$.) It is clear then that $\Phi_1, \Phi_2, \Phi_3, \dots$ is an unbounded nondecreasing sequence of positive integers such that each element of the sequence

$$U = \{1/\Phi_1, 1/\Phi_2, 1/\Phi_3, \dots\}$$

does not exceed the corresponding element of the sequence $\boldsymbol{\delta}$. Therefore, in order to prove Theorem 1, it suffices to show that for each interval $I \subset \mathbb{R}_{>1}$, there is an uncountable set of real numbers $S \subset I$ such that, for every $\alpha \in S$, the inequalities

$$0 < \{\xi_n \alpha^n\} < \frac{1}{\Phi_n} \tag{5}$$

hold for infinitely many $n \in \mathbb{N}$.

We will prove the following more general statement:

Theorem 2. *Let $\boldsymbol{\xi} = \{\xi_1, \xi_2, \xi_3, \dots\}$ be a sequence of positive numbers satisfying* (3)*, and let $\Phi_1 \le \Phi_2 \le \Phi_3 \le \dots$ be an unbounded sequence of positive integers. Then, for any interval $I = [a, b]$, $1 \le a < b$, and any real number $\eta > 1$, there is an uncountable set $S(\boldsymbol{\xi}, \Phi, I, \eta) \subset I$ such that, for each $\alpha \in S(\boldsymbol{\xi}, \Phi, I, \eta)$, the inequalities*

$$\eta^m < \xi_n \alpha^n < \eta^m + \frac{1}{\Phi_n} \tag{6}$$

hold for infinitely many pairs $(n, m) \in \mathbb{N}^2$.

It is clear that (6) implies (5), with, for example, $\eta = 2$, so Theorem 2 immediately implies Theorem 1.

We will derive Theorem 2 from the following proposition of independent interest.

Proposition 1. *Let $\gamma_1, \gamma_2, \gamma_3, \dots$ be a sequence of real numbers, and let $1 = \varepsilon_1 \ge \varepsilon_2 \ge \varepsilon_3 \ge \dots$ be a sequence of positive numbers. Assume that $I = [a, b]$, where $0 \le a < b$, and let $\mathcal{N}$ be an infinite subset of $\mathbb{N}$. Then there is an uncountable set $B \subset I$ such that, for each $\beta \in B$, the inequalities*

$$0 < \{n\beta - \gamma_n\} < \varepsilon_n \tag{7}$$

hold for infinitely many $n \in \mathcal{N}$.

Note that, if $\gamma_1 = \gamma_2 = \gamma_3 = \dots = 0$ and if the sequence ε_n tends to zero faster than any constant power of $1/n$, then the numbers β satisfying (7) are Liouville numbers. Recall that a Liouville number is a real number whose irrationality exponent is infinite,

see p. 248 in [30]. This means that, for any $C > 1$, there is a pair of integers k, n, where $n > 1$, such that

$$0 < \left|\beta - \frac{k}{n}\right| < \frac{1}{n^C}.$$

Therefore, Proposition 1 is the construction of uncountably many Liouville type numbers with good approximation not just by rational fractions k/n, $k, n \in \mathbb{N}$, but by fractions with "moving numerator" $(k + \gamma_n)/n$. The author thanks Prof. Nikolay Moshchevitin for a useful advice towards this construction. Note that the approximation $(k + \gamma_n)/n$ to those special Liouville type numbers is with $k \in \mathbb{Z}$ and with n being not just in $\mathbb{N}$ but in any infinite sequence of positive integers $\mathcal{N}$. For instance, $\mathcal{N}$ can be the set of squares or the set of primes.

Next, we will prove Proposition 1 (Section 2) and then derive Theorem 2 from this proposition (Section 3). In Section 4, we will give a stronger version of Theorem 1 under a condition slightly stronger than that in (3). Then, in Section 5, we provide another application of Proposition 1. Section 6 contains some final remarks.

2. Proof of Proposition 1

We begin with the following simple observation:

Lemma 1. *Let $I = [a, b]$ be a closed real interval with $a < b$, and let $u < v$ be two real numbers. Then, for each sufficiently large positive integer n, there is an integer $k = k(n)$ such that $(k + u)/n, (k + v)/n \in I$.*

Proof. Take any integer n satisfying

$$n \geq \frac{v - u + 1}{b - a}. \tag{8}$$

Note that $n > 0$. Select

$$k = k(n) = \lceil na - u \rceil. \tag{9}$$

Then $k \geq na - u$, and hence $a \leq (k + u)/n$. Next, from (8) and (9), it follows that

$$\frac{k + v}{n} < \frac{na - u + 1 + v}{n} \leq \frac{na + n(b - a)}{n} = \frac{nb}{n} = b.$$

Therefore, the numbers $(k + u)/n$ and $(k + v)/n$ both belong to the interval I, which completes the proof of the lemma. □

Next, for any sequence of real numbers γ_n, $n = 1, 2, 3, \ldots$, and any infinite sequence of positive integers $\mathcal{N}$, we will prove the existence of a real number that is very close to the fraction $(k + \gamma_n)/n$ for infinitely many pairs (n, k), where $n \in \mathcal{N}$ and $k \in \mathbb{Z}$.

Lemma 2. *Let $\gamma_1, \gamma_2, \gamma_3, \ldots$ be a sequence of real numbers, and let $1 = \varepsilon_1 \geq \varepsilon_2 \geq \varepsilon_3 \geq \ldots$ be a sequence of positive numbers. Let $I = [a, b]$, where $0 < a < b$, and let $\mathcal{N} \subseteq \mathbb{N}$ be infinite. Then, for any sequence $\mathbf{u} = \{u_1, u_2, u_3, \ldots\}$, where $u_j \in \{2, 4\}$ for each $j \in \mathbb{N}$, there is a positive real number $\beta(\mathbf{u}) \in I$ and a sequence $n_1 < n_2 < n_3 < \ldots$ in $\mathcal{N}$ such that, for every $j \in \mathbb{N}$, we have*

$$\frac{\varepsilon_{n_j}}{u_j + 1} \leq \{n_j \beta(\mathbf{u}) - \gamma_{n_j}\} \leq \frac{\varepsilon_{n_j}}{u_j}. \tag{10}$$

Proof. We will construct the number $\beta(\mathbf{u})$ using the method of nested intervals. Set $I_0 = I = [a, b]$. Take the least integer n_1 in $\mathcal{N}$ satisfying

$$n_1 \geq \frac{13}{10(b-a)}, \tag{11}$$

and set

$$u = \gamma_{n_1} + \frac{\varepsilon_{n_1}}{5} \quad \text{and} \quad v = \gamma_{n_1} + \frac{\varepsilon_{n_1}}{2}.$$

Note that

$$0 < v - u = \frac{3\varepsilon_{n_1}}{10} \leq \frac{3}{10},$$

so n_1 chosen in (11) satisfies the inequality (8). Choosing k_1 as in (9), namely,

$$k_1 = \lceil n_1 a - \gamma_{n_1} - \varepsilon_{n_1}/5 \rceil$$

and applying Lemma 1, we find that both endpoints of the interval

$$J_1 = [n_1^{-1}(k_1 + \gamma_{n_1} + \varepsilon_{n_1}/5), n_1^{-1}(k_1 + \gamma_{n_1} + \varepsilon_{n_1}/2)]$$

belong to the interval I_0. Consequently, as $u_1 \in \{2, 4\}$,

$$I_1 = [n_1^{-1}(k_1 + \gamma_{n_1} + \varepsilon_{n_1}/(u_1+1)), n_1^{-1}(k_1 + \gamma_{n_1} + \varepsilon_{n_1}/u_1)]$$

is its subinterval, so it satisfies $I_1 \subset I_0$. Furthermore, for any number $\zeta \in I_1$, we have

$$\frac{\varepsilon_{n_1}}{u_1+1} \leq n_1\zeta - \gamma_{n_1} - k_1 \leq \frac{\varepsilon_{n_1}}{u_1}.$$

From $\varepsilon_{n_1} \leq 1$ and $u_1 \in \{2, 4\}$, it follows that $k_1 = \lfloor n_1\zeta - \gamma_{n_1} \rfloor$ (where $\lfloor y \rfloor$ is the integral part of $y \in \mathbb{R}$), so (10) is true for $j = 1$ and any number ζ from the interval I_1.

We now argue by induction on j. Assume that $l \geq 1$ is an integer such that, for $j = 1, 2, \ldots, l$, there is a nested collection of intervals

$$I_j = [n_j^{-1}(k_j + \gamma_{n_j} + \varepsilon_{n_j}/(u_j+1), n_j^{-1}(k_j + \gamma_{n_j} + \varepsilon_{n_j}/u_j)] = [a_j, b_j] \tag{12}$$

with uniquely chosen $n_1 < n_2 < n_3 < \ldots < n_l$ in $\mathcal{N}$ and $k_1, \ldots, k_l \in \mathbb{Z}$ such that

$$I_l \subseteq I_{l-1} \subseteq \cdots \subseteq I_1 \subseteq I_0 = [a, b].$$

For any $\zeta \in I_j$, we clearly have

$$\frac{\varepsilon_{n_j}}{u_j+1} \leq n_j\zeta - \gamma_{n_j} - k_j = \{n_j\zeta - \gamma_{n_j}\} \leq \frac{\varepsilon_{n_j}}{u_j},$$

so (10) is true for $j = 1, 2, \ldots, l$ and any number ζ from the interval I_l.

Next, we will show how to choose the interval I_{l+1} of the form

$$I_{l+1} = [n_{l+1}^{-1}(k_{l+1} + \gamma_{n_{l+1}} + \varepsilon_{n_{l+1}}/(u_{l+1}+1)), n_{l+1}^{-1}(k_{l+1} + \gamma_{n_{l+1}} + \varepsilon_{n_{l+1}}/u_{l+1})] \tag{13}$$

contained in I_l, with $k_{l+1} \in \mathbb{Z}$ and $n_{l+1} > n_l$ in $\mathcal{N}$. To this end, we will apply Lemma 1, with $a = a_l$ being the left endpoint of I_l, $b = b_l$ being the right endpoint of I_l, and the smallest integer $n = n_{l+1} > n_l$ in $\mathcal{N}$ satisfying

$$n_{l+1} \geq \frac{13}{10(b_l - a_l)}. \tag{14}$$

As above, applying Lemma 1 to

$$u = \gamma_{n_{l+1}} + \frac{\varepsilon_{n_{l+1}}}{5} \quad \text{and} \quad v = \gamma_{n_{l+1}} + \frac{\varepsilon_{n_{l+1}}}{2},$$

due to $0 < v - u \leq 3/10$, we can choose an appropriate integer k_{l+1} by (9), namely,

$$k_{l+1} = \lceil n_{l+1}a_l - \gamma_{n_{l+1}} - \varepsilon_{n_{l+1}}/5 \rceil. \tag{15}$$

Then, by Lemma 1, both endpoints of the interval

$$J_{l+1} = [n_{l+1}^{-1}(k_{l+1} + \gamma_{n_{l+1}} + \varepsilon_{n_{l+1}}/5), n_{l+1}^{-1}(k_{l+1} + \gamma_{n_{l+1}} + \varepsilon_{n_{l+1}}/2)]$$

belong to I_l. Consequently, the subinterval I_{l+1} of J_{l+1}, which we defined in (13), satisfies $I_{l+1} \subset J_{l+1} \subseteq I_l$.

By this construction, since the length of I_j, namely, $\varepsilon_{n_j}/(u_j(u_j+1)n_j)$, tends to zero as $j \to \infty$, the unique point of the intersection $\cap_{j=1}^{\infty} I_j$ is the required positive real number $\beta(\mathbf{u})$. (It is clear that $\beta(\mathbf{u}) \in I_1 \subseteq I_0 = [a, b]$.) $\square$

We now show that the numbers $\beta(\mathbf{u})$ and $\beta(\mathbf{u}')$ are distinct for distinct vectors

$$(u_1, u_2, u_3, \dots) \quad \text{and} \quad (u_1', u_2', u_3', \dots).$$

Indeed, let ℓ be the smallest positive integer for which $u_\ell \neq u_\ell'$. Without restriction of generality, we may assume that $u_\ell = 2$ and $u_\ell' = 4$. Since $(u_1, \dots, u_{\ell-1}) = (u_1', \dots, u_{\ell-1}')$, the intervals I_j and I_j' constructed in (12) are the same for $j = 1, 2, \dots, \ell - 1$. Furthermore, the integers n_ℓ and k_ℓ are also the same. (In view of (14) and (15), they do not depend on u_ℓ.) Therefore, by (12) and $(u_\ell, u_\ell') = (2, 4)$, we find that

$$I_\ell = [n_\ell^{-1}(k_\ell + \gamma_{n_\ell} + \varepsilon_{n_\ell}/3), n_\ell^{-1}(k_\ell + \gamma_{n_\ell} + \varepsilon_{n_\ell}/2)]$$

and

$$I_\ell' = [n_\ell^{-1}(k_\ell + \gamma_{n_\ell} + \varepsilon_{n_\ell}/5), n_\ell^{-1}(k_\ell + \gamma_{n_\ell} + \varepsilon_{n_\ell}/4)].$$

Note that the intervals I_ℓ and I_ℓ' are disjoint. Since $\beta(\mathbf{u}) \in I_\ell$ and $\beta(\mathbf{u}') \in I_\ell'$, the numbers $\beta(\mathbf{u})$ and $\beta(\mathbf{u}')$ are distinct. In fact, we always have the inequality $\beta(\mathbf{u}') < \beta(\mathbf{u})$ if the vector $\mathbf{u}$ is lexicographically smaller than the vector $\mathbf{u}'$.

Clearly, there is a continuum of such distinct sequences $\mathbf{u}$ when $\mathbf{u}$ runs over all possible infinite sequences consisting of 2 and 4. As we have shown above, the numbers $\beta(\mathbf{u})$ are all distinct, so there are continuum of numbers $\beta(\mathbf{u})$. This completes the proof of Proposition 1, because in (10) we have $0 < \varepsilon_{n_j}/(u_j + 1)$ and $\varepsilon_{n_j}/u_j < \varepsilon_{n_j}$, so (7) is true for each $n = n_j$.

3. Proof of Theorem 2

Fix any $\eta > 1$ and an interval $I = [a, b]$, where $1 \leq a < b$. Note that, without restriction of generality, we may assume that $a > 1$, because in case $a = 1$, one can consider the subinterval $[(a + b)/2, b]$ of I instead of I itself.

In order to apply Proposition 1, we will consider the sequence of positive numbers $\varepsilon_1 = 1$,

$$\varepsilon_n = \min\left(1, \frac{1}{\Phi_2 2! \xi_2}, \frac{1}{\Phi_3 3! \xi_3}, \dots, \frac{1}{\Phi_n n! \xi_n}\right)$$

for each $n \geq 2$. Then, $1 = \varepsilon_1 \geq \varepsilon_2 \geq \varepsilon_3 \geq \dots$ is a sequence of positive numbers. Let also

$$\gamma_n = -\frac{\log \xi_n}{\log \eta} \tag{16}$$

for each $n \in \mathbb{N}$.

Fix any ϵ in the interval $(0, \log a)$. Then, by (3), there is an infinite sequence $\mathcal{N} \subset \mathbb{N}$ such that, for each $n \in \mathcal{N}$, we have

$$\xi_n \geq e^{-\epsilon n}. \tag{17}$$

Furthermore, by (17), for $\alpha \geq a$, we have

$$\xi_n \alpha^n \to \infty \quad \text{as} \quad n \in \mathcal{N} \quad \text{tends to infinity.} \tag{18}$$

Now, by Proposition 1 applied to the interval

$$J = [\log a / \log \eta, \log b / \log \eta] \tag{19}$$

and (16), there is an uncountable in J set of positive numbers B such that, for each $\beta \in B$, the inequalities

$$0 < n\beta + \frac{\log \xi_n}{\log \eta} - m < \varepsilon_n \leq \frac{1}{\Phi_n n! \xi_n}$$

hold for infinitely many pairs (n, m), where $n \in \mathcal{N}$ and $m \in \mathbb{Z}$. Multiplying all this by $\log \eta > 0$, we derive that the inequalities

$$0 < n\beta \log \eta + \log \xi_n - m \log \eta < \frac{1}{\Phi_n (n-1)! \xi_n} \tag{20}$$

hold for infinitely many pairs (n, m), where $n \in \mathcal{N}$ and $m \in \mathbb{Z}$. Note that, by (17), we have

$$\Phi_n (n-1)! \xi_n \to \infty \quad \text{as} \quad n \in \mathcal{N} \quad \text{tends to infinity.} \tag{21}$$

Let S be the set of numbers of the form $\alpha = \eta^\beta$, where β runs over every element of B. Note that the map $x \mapsto \eta^x$ maps the interval J defined in (19) into the interval $[a, b]$. Therefore, the set S is a subset of $[a, b]$. Moreover, the set S is uncountable because so is the set B.

Consider the difference

$$\xi_n \alpha^n - \eta^m = e^{n\beta \log \eta + \log \xi_n} - e^{m \log \eta} = \eta^m (e^{n\beta \log \eta + \log \xi_n - m \log \eta} - 1).$$

By (20), the exponent here is in the interval $(0, 1/(\Phi_n (n-1)! \xi_n))$. Additionally, $\eta^m < \xi_n \alpha^n$ by (20) as well. Consequently, from (21), it follows that

$$0 < \xi_n \alpha^n - \eta^m = \eta^m (e^{n\beta \log \eta + \log \xi_n - m \log \eta} - 1) < \xi_n \alpha^n \cdot \frac{2}{\Phi_n (n-1)! \xi_n} = \frac{2\alpha^n}{\Phi_n (n-1)!} < \frac{1}{\Phi_n}$$

for a sufficient large $n \in \mathcal{N}$. Here, in view of (18), for each sufficiently large $n \in \mathcal{N}$, the corresponding integer m must be positive. This completes the proof of (6).

4. A Different Version of the Main Result

Note that, in the proof of Theorem 2, we did not use (3) but rather the condition (18), with a subsequence $\mathcal{N}$. Therefore, we can change the initial condition (3) for the sequence ξ_n, $n = 1, 2, 3, \ldots$, by the condition

$$\xi_n a^n \to \infty \quad \text{as} \quad n \in \mathcal{N} \quad \text{tends to infinity,} \tag{22}$$

where $\mathcal{N}$ is an arbitrary infinite sequence of positive integers and $a > 1$ is a fixed number. Observe that (22) is true for any infinite sequence $\mathcal{N} \subseteq \mathbb{N}$ and any $a > 1$ if, say, $\xi_n \geq \xi > 0$ for every $n \in \mathbb{N}$.

Then, by the argument given in Section 3, we obtain the following version of Theorem 1:

Theorem 3. *Let $I = [a, b]$ be an interval with $1 < a < b$. Assume that $\mathcal{N}$ is an infinite sequence of positive integers, and $\boldsymbol{\xi} = \{\xi_1, \xi_2, \xi_3, \dots\}$ is a sequence of positive numbers satisfying* (22) *with this $\mathcal{N}$. Then, for any sequence of positive numbers $\boldsymbol{\delta} = \{\delta_1, \delta_2, \delta_3, \dots\}$, there is an uncountable set $S(I, \mathcal{N}, \boldsymbol{\xi}, \boldsymbol{\delta}) \subset I$ such that, for each $\alpha \in S(I, \mathcal{N}, \boldsymbol{\xi}, \boldsymbol{\delta})$, the inequalities*

$$0 < \{\xi_n \alpha^n\} < \delta_n \tag{23}$$

hold for infinitely many $n \in \mathcal{N}$.

We omit the proof, since it is exactly the same as that above.

5. An Application of Proposition 1

Recently, in [31], we studied the following problem. Given $\theta \in \mathbb{R}_{>0} \setminus \mathbb{N}$, let $R_\theta(N)$ be the least nonzero value of $\|a^\theta\|$ as $a = 1, 2, \dots, N$. Define

$$E_\theta = \limsup_{N \to \infty} \frac{\log(1/R_\theta(N))}{\log N}.$$

In Theorem 5 of [31], we provided several estimates for the quantity E_θ for some θ. For example, it was shown that $E_{2/3} \geq 1$, with the equality holding under assumption of the *abc*-conjecture.

Then Iyer [32] showed that $E(\theta)$ can be infinite for some $\theta \in \mathbb{R}_{>0} \setminus \mathbb{N}$. This follows from Theorem 1.9 of [32], where it was shown that, for any sequence of positive numbers δ_n, $n = 1, 2, 3, \dots$, there are many $\tau \in \mathbb{R}_{>0} \setminus \mathbb{N}$ for which the inequalities

$$0 < \|n^\tau\| < \delta_n$$

hold for infinitely many $n \in \mathbb{N}$. Indeed, selecting $\delta_n = 1/n!$ and all the corresponding numbers τ, we see that $E_\tau = \infty$ for each of those τ, because $\log(n!)/\log(n) \to \infty$ as $n \to \infty$.

We will derive the following more general result:

Theorem 4. *Let $I = [a, b]$ be an interval with $0 < a < b$. Assume that $\boldsymbol{\xi} = \{\xi_1, \xi_2, \xi_3, \dots\}$ is a sequence of positive numbers satisfying*

$$\xi_n n^a \to \infty \quad as \quad n \to \infty. \tag{24}$$

Then, for any sequence of positive numbers $\boldsymbol{\delta} = \{\delta_1, \delta_2, \delta_3, \dots\}$, there is an uncountable set $W(I, \boldsymbol{\xi}, \boldsymbol{\delta}) \subset I$ such that, for each $\tau \in W(I, \boldsymbol{\xi}, \boldsymbol{\delta})$, the inequalities

$$0 < \{\xi_n n^\tau\} < \delta_n \tag{25}$$

hold for infinitely many $n \in \mathbb{N}$.

Proof. Without restriction of generality, we may assume that $\delta_n < 1$ for each $n \in \mathbb{N}$. In all that follows, it will be shown that (25) holds for infinitely many powers of 2, namely, the inequalities

$$0 < \{\xi_{2^n} 2^{n\tau}\} < \delta_{2^n} \tag{26}$$

are true for infinitely many $n \in \mathbb{N}$.

To this end, we will apply Proposition 1 to $I = [a, b]$,

$$\gamma_n = -\frac{\log \zeta_{2^n}}{\log 2},$$

and the sequence of positive numbers ε_n, $n = 1, 2, 3, \ldots$, where $\varepsilon_1 = 1$ and

$$\varepsilon_n = \min\left(\varepsilon_1, \ldots, \varepsilon_{n-1}, \frac{\delta_{2^n}}{\xi_{2^n} 2^{nb}}\right) \tag{27}$$

for $n = 2, 3, 4, \ldots$. It is clear that $1 = \varepsilon_1 \geq \varepsilon_2 \geq \varepsilon_3 \geq \ldots$.

By Proposition 1, it follows that there is an uncountable in I set of positive numbers W such that, for each $\tau \in W$, the inequalities

$$0 < n\tau + \frac{\log \xi_{2^n}}{\log 2} - m < \varepsilon_n$$

hold for infinitely many pairs (n, m), where $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Multiplying by $\log 2$, we obtain that the inequalities

$$0 < n\tau \log 2 + \log \xi_{2^n} - m \log 2 < \varepsilon_n \log 2 \tag{28}$$

hold for infinitely many pairs (n, m), where $n \in \mathbb{N}$ and $m \in \mathbb{Z}$.

Now, we consider the difference

$$\xi_{2^n} 2^{n\tau} - 2^m = e^{n\tau \log 2 + \log \xi_{2^n}} - e^{m \log 2} = 2^m (e^{n\tau \log 2 + \log \xi_{2^n} - m \log 2} - 1).$$

By (28), the exponent here is in the interval $(0, \varepsilon_n \log 2)$. Additionally, $2^m < \xi_{2^n} 2^{n\tau}$ by (28), and $\xi^{2^n} 2^{nb} \varepsilon_n \leq \delta_{2^n}$ by (27). Therefore,

$$0 < \xi_{2^n} 2^{n\tau} - 2^m = 2^m (e^{n\tau \log 2 + \log \xi_{2^n} - m \log 2} - 1) < \xi_{2^n} 2^{n\tau} \cdot (2\varepsilon_n \log 2) < \xi_{2^n} 2^{nb} \varepsilon_n \leq \delta_{2^n}$$

for each of those $n \in \mathbb{N}$.

Here, we have

$$\zeta_{2^n} 2^{n\tau} \to \infty \quad \text{as} \quad n \to \infty,$$

because

$$\zeta_{2^n} 2^{na} \to \infty \quad \text{as} \quad n \to \infty.$$

Consequently, as

$$2^m > \xi_{2^n} 2^{n\tau} - \delta_{2^n} > \xi_{2^n} 2^{n\tau} - 1,$$

the corresponding integer m must be positive for each sufficiently large $n \in \mathbb{N}$, and hence $2^m \in \mathbb{Z}$.

Combined with $0 < \delta_{2^n} < 1$, this implies that 2^m is the integer part of the number $\xi_{2^n} 2^{n\tau}$. Thus, for infinitely many $n \in \mathbb{N}$, we have

$$0 < \{\xi_{2^n} 2^{n\tau}\} = \xi_{2^n} 2^{n\tau} - 2^m < \delta_{2^n}$$

which is (26). This completes the proof of the theorem. □

Note that we cannot omit the condition (24). Indeed, select, for instance, $\xi_n = \delta_n = 1/n!$. Then, for each $\tau > 0$, we have $0 < \xi_n n^\tau < 1$ for each sufficiently large $n \in \mathbb{N}$. Therefore, for each $\tau > 0$ and all sufficiently large $n \in \mathbb{N}$, we have

$$\{\xi_n n^\tau\} = \xi_n n^\tau > \xi_n = \frac{1}{n!} = \delta_n,$$

so (25) does not hold for $\tau > 0$.

6. Concluding Remarks

In particular, Theorem 3 implies that, for any $\xi > 0$ and any sequence of positive numbers δ_n, $n = 1, 2, 3, \ldots$, there are uncountably many $\alpha > 1$ for which the inequalities

$$0 < \{\xi \alpha^p\} < \delta_p$$

hold for infinitely many primes p, and uncountably many $\gamma > 1$ for which the inequalities

$$0 < \{\xi \gamma^{n^2}\} < \delta_{n^2}$$

hold for infinitely many $n \in \mathbb{N}$.

On the other hand, we do not know whether our method can be extended to conclude the same as stated in Theorem 3 with inequality (23) replaced by

$$0 < \{\xi_n \alpha^n - \eta_n\} < \delta_n,$$

where η_n, $n = 1, 2, 3, \ldots$, is an arbitrary sequence of real numbers. This problem is open even if $\xi_n = 1$ for $n \in \mathbb{N}$. More precisely, we do not know whether for any sequence of real numbers η_n, $n = 1, 2, 3, \ldots$, and any sequence of positive numbers δ_n, $n = 1, 2, 3, \ldots$, there is a real number $\alpha > 1$ for which we have

$$0 < \{\alpha^n - \eta_n\} < \delta_n$$

for infinitely many $n \in \mathbb{N}$.

Similarly, with respect to Theorem 4, we may ask whether for any sequence of real numbers η_n, $n = 1, 2, 3, \ldots$, and any sequence of positive numbers δ_n, $n = 1, 2, 3, \ldots$, there is a real number $\tau > 0$ for which the inequalities

$$0 < \{n^\tau - \eta_n\} < \delta_n$$

hold for infinitely many $n \in \mathbb{N}$.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Weyl, H. Über die Gleichverteilung von Zahlen modulo Eins. *Math. Ann.* **1916**, *77*, 313–352. [CrossRef]
2. Aistleitner, C. Quantitative uniform distribution results for geometric progressions. *Israel J. Math.* **2014**, *204*, 155–197. [CrossRef]
3. Koksma, J.F. Ein mengentheoretischer Satz über Gleichverteilung modulo eins. *Compos. Math.* **1935**, *2*, 250–258.
4. Pisot, C.; Salem, R. Distribution modulo 1 of the powers of real numbers larger than 1. *Compos. Math.* **1964**, *16*, 164–168.
5. Salem, R. *Algebraic Numbers and Fourier Analysis*; D. C. Heath and Co.: Boston, MA, USA, 1963.
6. Bertin, M.-J.; Decomps-Guilloux, A.; Grandet-Hugot, M.; Pathiaux-Delefosse, M.; Schreiber, J.-P. *Pisot and Salem Numbers*; Birkhäuser Verlag: Basel, Switzerland, 1992.
7. Smyth, C. Seventy years of Salem numbers. *Bull. Lond. Math. Soc.* **2015**, *47*, 379–395. [CrossRef]
8. Vijayaraghavan, T. On the fractional parts of the powers of a number. I. *J. Lond. Math. Soc.* **1940**, *15*, 159–160. [CrossRef]
9. Vijayaraghavan, T. On the fractional parts of the powers of a number. II. *Proc. Camb. Philos. Soc.* **1941**, *37*, 349–357. [CrossRef]
10. Vijayaraghavan, T. On the fractional parts of the powers of a number. III. *J. Lond. Math. Soc.* **1942**, *17*, 137–138. [CrossRef]
11. Vijayaraghavan, T. On the fractional parts of the powers of a number. IV. *J. Indian Math. Soc.* **1948**, *12*, 33–39.
12. Flatto, L.; Lagarias, J.C.; Pollington, A.D. On the range of fractional parts $\{\xi(p/q)^n\}$. *Acta Arith.* **1995**, *70*, 125–147. [CrossRef]

13. Dubickas, A. Arithmetical properties of powers of algebraic numbers. *Bull. Lond. Math. Soc.* **2006**, *38*, 70–80. [CrossRef]
14. Jung, Y.; Lai, C.-K.; Mooroogen, Y. Fifty years of the Erdős similarity conjecture. *Res. Math. Sci.* **2025**, *12*, 9. [CrossRef]
15. Dubickas, A. On the limit points of the fractional parts of powers of Pisot numbers. *Arch. Math.* **2006**, *42*, 151–158.
16. Zaïmi, T. An arithmetical property of powers of Salem numbers. *J. Number Theory* **2006**, *120*, 179–191. [CrossRef]
17. Zaïmi, T. Comments on the distribution modulo one of powers of Pisot and Salem numbers. *J. Publ. Math. Debr.* **2012**, *80*, 417–426. [CrossRef]
18. Mahler, K. An unsolved problem on the powers of 3/2. *J. Austral. Math. Soc.* **1968**, *8*, 313–321. [CrossRef]
19. Akiyama, S. Mahler's *Z*-number and 3/2 number systems. *Unif. Distrib. Theory* **2008**, *3*, 91–99.
20. Akiyama, S.; Frougny, C.; Sakarovitch, J. Powers of rationals modulo 1 and rational base number systems. *Israel J. Math.* **2008**, *168*, 53–91. [CrossRef]
21. Dubickas, A. On the powers of 3/2 and other rational numbers. *Math. Nachr.* **2008**, *281*, 951–958. [CrossRef]
22. Dubickas, A. On the powers of some transcendental numbers. *Bull. Austral. Math. Soc.* **2007**, *76*, 433–440. [CrossRef]
23. Baker, S. On the distribution of powers of real numbers modulo 1. *Unif. Distrib. Theory* **2015**, *10*, 67–75.
24. Schleischitz, J. Integral powers of numbers in small intervals modulo 1: The cardinality gap phenomenon. *Unif. Distrib. Theory* **2017**, *12*, 69–98. [CrossRef]
25. Koksma, J.F. Sur la théorie métrique des approximations diophantiques. *Indag. Math.* **1945**, *7*, 54–70.
26. Cilleruelo, J.; Kumchev, A.; Luca, F.; Rué, J.; Shparlinski, I.E. On the fractional parts of a^n/n. *Bull. Lond. Math. Soc.* **2013**, *45*, 249–256. [CrossRef]
27. Dubickas, A. Density of some sequences modulo 1. *Colloq. Math.* **2012**, *128*, 237–244. [CrossRef]
28. Dubickas, A. Density of some special sequences modulo 1. *Mathematics* **2023**, *11*, 1727. [CrossRef]
29. Lind, M. Limit points and discrepancy of the fractional parts of b^n/n. *Acta Arith.* **2024**, *216*, 19–34. [CrossRef]
30. Bugeaud, Y. *Distribution Modulo One and Diophantine Approximation*; Cambridge Tracts in Mathematics; Cambridge University Press: Cambridge, UK, 2012; Volume 193.
31. Dubickas, A. Approximate equality for two sums of roots. *J. Complex.* **2024**, *84*, 101866. [CrossRef]
32. Iyer, S. Distribution of θ-powers and their sums. *J. Math. Anal. Appl.* **2025**, *551*, 129672. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

Polyadic Encryption

Steven Duplij [1,2,*] and Qiang Guo [3]

[1] Yantai Research Institute, Harbin Engineering University, Yantai 265615, China
[2] Center for Information Technology (CIT), Universität Münster, Röntgenstrasse 7-13, D-48149 Münster, Germany
[3] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China; guoqiang292004@163.com or guoqiang@hrbeu.edu.cn
* Correspondence: douplii@uni-muenster.de or duplij@gmx.de

Abstract: A novel original procedure of encryption/decryption based on the polyadic algebraic structures and on signal processing methods is proposed. First, we use signals with integer amplitudes to send information. Then, we use polyadic techniques to transfer the plaintext into series of special integers. The receiver restores the plaintext using special rules and systems of equations.

Keywords: polyadic ring; signal processing; encryption; decryption; polyadic integer; plaintext; arity shape; polyadic structure; congruence class; representative

MSC: 11H71; 11R04; 17A42; 20N15; 68P25; 94A12

1. Introduction

We propose a new approach to transfer hidden information in (continuous-time discrete-valued) signal processing (see, e.g., [1,2]) by considering the parameters of signals not as the ordinary integers [3,4], but as a special kind of integer numbers, polyadic integers, introduced in [5]. The polyadic integers form polyadic (m,n)-rings having (or closed with respect to) m additions and n multiplications [6]. In this way, preservation of the property to be in the same polyadic ring after signal processing will give various restrictions on the signal parameters. The main idea is to use these restrictions (as equations) to encrypt and decrypt a series of ordinary numbers using sets of signals prepared in special ways.

2. Polyadic Rings

We first remind that the polyadic ring or (m,n)-ring is a set with m-ary addition (being a m-ary group) and n-ary multiplication (being a n-ary semigroup), which are connected by the polyadic distributive law [6]. A polyadic ring is nonderived, if its full operations cannot be obtained as repetition of binary operations. As the simplest example of the binary ring or $(2,2)$-ring is the set ordinary integers $\mathbb{Z}$, the example of (m,n)-ring is the set of polyadic integers $\mathbb{Z}_{(m,n)}$ [5]. The concrete realization of polyadic integers is the set of representatives of the conguence class (residue class) of an integer a modulo b (with both a and b fixed)

$$\mathbb{Z}^{[a,b]}_{(m,n)} = [[a]]_b = \{\{a + b \cdot k\} \mid k \in \mathbb{Z},\ \ a \in \mathbb{Z}_+,\ b \in \mathbb{N},\ 0 \leq a \leq b-1\}. \tag{1}$$

We denote a representative element by $x_k = x^{[a,b]}_k = a + b \cdot k$, which are polyadic intergers $\left\{x^{[a,b]}_k\right\} \in \mathbb{Z}^{[a,b]}_{(m,n)}$, because only m additions and n multiplications are possible in the nonderived case

$$\overbrace{x_{k_1}+x_{k_2}+\ldots+x_{k_m}}^{m}\in\mathbb{G}_{add(m)}^{[a,b]}\subset\mathbb{Z}_{(m,n)}^{[a,b]}, \tag{2}$$

$$\overbrace{x_{k_1}x_{k_2}\ldots x_{k_n}}^{n}\in\mathbb{S}_{mult(n)}^{[a,b]}\subset\mathbb{Z}_{(m,n)}^{[a,b]},\ \ k_i\in\mathbb{Z}, \tag{3}$$

where $\mathbb{G}_{add(m)}^{[a,b]}$ and $\mathbb{S}_{mult(n)}^{[a,b]}$ are the m-ary additive group and n-ary multiplicative semigroup of the polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$.

It follows from (2) and (3) that more generally, the m-admissible sum consists of $\ell_m(m-1)+1$ summands and the n-admissible product contains $\ell_n(n-1)+1$ elements, where ℓ_m is a number of m-ary additions (m-polyadic power) and ℓ_n is a number of n-ary multiplications (n-polyadic power). Therefore, in general

$$\overbrace{x_{k_1}+x_{k_2}+\ldots+x_{k_m}}^{\ell_m(m-1)+1}\in\mathbb{G}_{add(m)}^{[a,b]}\subset\mathbb{Z}_{(m,n)}^{[a,b]}, \tag{4}$$

$$\overbrace{x_{k_1}x_{k_2}\ldots x_{k_n}}^{\ell_n(n-1)+1}\in\mathbb{S}_{mult(n)}^{[a,b]}\subset\mathbb{Z}_{(m,n)}^{[a,b]},\ \ k_i\in\mathbb{Z}. \tag{5}$$

$\ell_m(m-1)+1$

For instance, in the residue (congruence) class

$$[[3]]_4=\{\ldots-25,-21,-17,-13,-9,-5,-1,3,7,11,15,19,23,27,31,35,39\ldots\} \tag{6}$$

we can add $4\ell_m+1$ representatives and multiply $2\ell_n+1$ representatives (ℓ_m, ℓ_n are polyadic powers) to retain in the same class $[[3]]_4$. If, for example, we take $\ell_m=2$, $\ell_n=3$, then we obtain closeness of polyadic operations

$$(7+11+15+19+23)-5-9-13-1=47=3+4\cdot11\in[[3]]_4, \tag{7}$$

$$((7\cdot3\cdot11)\cdot19\cdot15)\cdot31\cdot27=55\,103\,895=3+4\cdot13\,775\,973\in[[3]]_4. \tag{8}$$

Thus, we cannot add and multiply arbitrary quantities of representatives in $[[3]]_4$, only the admissible ones. This means that $[[3]]_4$ is really the polyadic $(5,3)$-ring $\mathbb{Z}_{(5,3)}^{[3,4]}$.

In general, a congruence class $[[a]]_b$ is a polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$, if the following relations hold valid [5]

$$(m-1)\frac{a}{b}=I^{(m)}(a,b)=I=\text{integer}, \tag{9}$$

$$\frac{a^n-a}{b}=J^{(n)}(a,b)=J=\text{integer}, \tag{10}$$

where I, J are called a (polyadic) shape invariants of the congruence class $[[a]]_b$, e.g., for the congruence class $[[3]]_4$, the shape invariants (9) and (10) are $I=3$ and $J=6$, correspondingly.

In Table 1, the mapping

$$\Phi_{(m,n)}^{[a,b]}:(a,b)\longrightarrow(m,n) \tag{11}$$

of the congruence class parameters to the polyadic ring arities (we call it the arity shape) and shape invariants is presented for their lowest values. The arity shape mapping (11) is injective and non-surjective (empty cells), and it cannot be expressed in closed form. Moreover, e.g., the congruence classes $[[2]]_4$, $[[2]]_8$, $[[3]]_9$, $[[4]]_8$, $[[6]]_8$ and $[[6]]_9$ do not correspond to any ring, while the same $(6,5)$-ring can be described by different congruence classes $[[2]]_5$, $[[3]]_5$, $[[2]]_{10}$, and $[[8]]_{10}$.

The polyadic arity shape $\Phi_{(m,n)}^{[a,b]}$ (11) is the main tool in the encryption/decryption procedure, described below.

Table 1. The polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$ of the fixed residue class $[[a]]_b$: the arity shape $\Phi_{(m,n)}^{[a,b]}$.

$a \setminus b$	2	3	4	5	6	7	8	9	10
1	$m = \mathbf{3}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{4}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{5}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{6}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{7}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{8}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{9}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{10}$ $n = \mathbf{2}$ $I = 1$ $J = 0$	$m = \mathbf{11}$ $n = \mathbf{2}$ $I = 1$ $J = 0$
2		$m = \mathbf{4}$ $n = \mathbf{3}$ $I = 2$ $J = 2$		$m = \mathbf{6}$ $n = \mathbf{5}$ $I = 2$ $J = 6$	$m = \mathbf{4}$ $n = \mathbf{3}$ $I = 1$ $J = 1$	$m = \mathbf{8}$ $n = \mathbf{4}$ $I = 2$ $J = 2$		$m = \mathbf{10}$ $n = \mathbf{7}$ $I = 2$ $J = 14$	$m = \mathbf{6}$ $n = \mathbf{5}$ $I = 1$ $J = 3$
3			$m = \mathbf{5}$ $n = \mathbf{3}$ $I = 3$ $J = 6$	$m = \mathbf{6}$ $n = \mathbf{5}$ $I = 3$ $J = 48$	$m = \mathbf{3}$ $n = \mathbf{2}$ $I = 1$ $J = 1$	$m = \mathbf{8}$ $n = \mathbf{7}$ $I = 3$ $J = 312$	$m = \mathbf{9}$ $n = \mathbf{3}$ $I = 3$ $J = 3$		$m = \mathbf{11}$ $n = \mathbf{5}$ $I = 3$ $J = 24$
4				$m = \mathbf{6}$ $n = \mathbf{3}$ $I = 4$ $J = 12$	$m = \mathbf{4}$ $n = \mathbf{2}$ $I = 2$ $J = 2$	$m = \mathbf{8}$ $n = \mathbf{4}$ $I = 4$ $J = 36$		$m = \mathbf{10}$ $n = \mathbf{4}$ $I = 4$ $J = 28$	$m = \mathbf{6}$ $n = \mathbf{3}$ $I = 2$ $J = 6$
5					$m = \mathbf{7}$ $n = \mathbf{3}$ $I = 5$ $J = 20$	$m = \mathbf{8}$ $n = \mathbf{7}$ $I = 5$ $J = 11160$	$m = \mathbf{9}$ $n = \mathbf{3}$ $I = 5$ $J = 15$	$m = \mathbf{10}$ $n = \mathbf{7}$ $I = 5$ $J = 8680$	$m = \mathbf{3}$ $n = \mathbf{2}$ $I = 1$ $J = 2$
6						$m = \mathbf{8}$ $n = \mathbf{3}$ $I = 6$ $J = 30$			$m = \mathbf{6}$ $n = \mathbf{2}$ $I = 3$ $J = 3$
7							$m = \mathbf{9}$ $n = \mathbf{3}$ $I = 7$ $J = 42$	$m = \mathbf{10}$ $n = \mathbf{4}$ $I = 7$ $J = 266$	$m = \mathbf{11}$ $n = \mathbf{5}$ $I = 7$ $J = 1680$
8								$m = \mathbf{10}$ $n = \mathbf{3}$ $I = 8$ $J = 56$	$m = \mathbf{6}$ $n = \mathbf{5}$ $I = 4$ $J = 3276$
9									$m = \mathbf{11}$ $n = \mathbf{3}$ $I = 9$ $J = 72$

3. Polyadic Encryption/Decryption Procedure

Let us consider the initial plaintext as a series of ordinary integer numbers (any plaintext can be transformed to that by the corresponding encoding procedure)

$$\mathbf{T} = y_1, y_2, \dots y_r, \qquad y_j \in \mathbb{Z}. \tag{12}$$

We propose a general encryption/decryption procedure, when each of $y = y_j$ is connected with the various parameters of signal series, and the latter are transfered to the receiver, who then restores y using special rules and systems of equations known to him only.

The main idea is to examine such signals which have parameters as polyadics integers, that is, they are in the polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$ (1). This can be treated as a polyadic gener-

alization of the (binary) discretization technique (in which the parameters are ordinary integers $\mathbb{Z}$), and so we call it the polyadic discretization. Its crucial new feature is the possibility to transfer information (e.g., arities, minimal allowed number of additions and multiplications) using signal parameters, as it will be shown below.

Here, we apply this idea to signal amplitudes (such signals are called the continuous-time discrete-valued or quantized analog signal [7,8]) and their addition only. This means that we look on the additive part of the polyadic ring $\mathbb{Z}^{[a,b]}_{(m,n)}$ which is a nonderived (allowed to add exactly m terms, no fewer) m-ary group $\mathbb{G}^{[a,b]}_{add(m)}$ (2). In this way, we denote the single ith signal shape as

$$\Psi_i^{(\ell_f)} = A_i^{(\ell_f)} \cdot f^{(\ell_f)}(t), \tag{13}$$

where $A_i^{(\ell_f)}$ is the amplitude of the normalized (in some manner) ith signal $f^{(\ell_f)}(t)$, t is time, and the natural $\ell_f \in \mathbb{N}$ corresponds to the special kind of signal (by consequent numerating sine/cosine, triangular, rectangular, etc.).

First, we assume that the amplitude $A_i^{(\ell_f)}$ is in polyadic ring, i.e., it is a representative of the congruence class $[[a]]_b$, $b \in \mathbb{N}$, $0 \leq a \leq b-1$, and therefore, it has the form (1)

$$A_i^{(\ell_f)} = a + b \cdot k_i^{(\ell_f)} \in \mathbb{G}^{[a,b]}_{add(m)} \subset \mathbb{Z}^{[a,b]}_{(m,n)}, \qquad k_i^{(\ell_f)} \in \mathbb{Z}. \tag{14}$$

Second, we identify the number of signal species ℓ_f with the m-polyadic power ℓ_m from (4)

$$\ell_f = \ell_m. \tag{15}$$

In this picture, for the signal species ℓ_f, we prepare the sum of $\ell_f(m-1)+1$ signals as

$$\Psi_{tot}^{(\ell_f)} = \sum_{i=1}^{\ell_f(m-1)+1} \Psi_i^{(\ell_f)} = A_{tot}^{(\ell_f)} \cdot f^{(\ell_f)}(t) \tag{16}$$

where the total amplitude $A_{tot}^{(\ell_f)}$ becomes different for distinct species ℓ_f and after usage of (14) has the general form

$$A_{tot}^{(\ell_f)} = \sum_{i=1}^{\ell_f(m-1)+1} A_i^{(\ell_f)} = a \cdot \Big(\ell_f(m-1)+1\Big) + b \cdot K\Big(m, \ell_f\Big) \in \mathbb{G}^{[a,b]}_{add(m)} \subset \mathbb{Z}^{[a,b]}_{(m,n)}, \tag{17}$$

$$K\Big(m, \ell_f\Big) = \sum_{i=1}^{\ell_f(m-1)+1} k_i^{(\ell_f)}. \tag{18}$$

Thus, we observe that the total amplitude (17) of the signal (13) contains all parameters of the m-ary group $\mathbb{G}^{[a,b]}_{add(m)}$ (the additive part of the polyadic ring $\mathbb{Z}^{[a,b]}_{(m,n)}$ (1)). This allows us to use the combination of signals (in the above particular case sums) to transfer securely the plaintext variables y_j (12) from sender to recepient, if we encode each of them $y = y_j$ by the polyadic ring parameters $y \longrightarrow (a,b,m)$. The recepient obtains the set of the total amplitudes $A_{tot}^{(\ell_f)}$ and treats (17) as the system of equations for parameters (a,b,m), and then after the decoding $(a,b,m) \longrightarrow y \longrightarrow y = y_j$ for each j obtains the initial plaintext **T** (12). Schematically, we can present the proposed encryption/decryption procedure as

$$\text{snd: } y \overset{\text{encoding by snd}}{\longrightarrow} (a,b,m) \overset{\text{summing}}{\longrightarrow} A_{tot}^{(\ell_f)} \overset{\text{preparing signals}}{\longrightarrow} \Psi_{tot}^{(\ell_f)} \overset{\text{transferring to rcp}}{\longrightarrow} \tag{19}$$

$$\text{rcp: system of equations } A_{tot}^{(\ell_f)} \ (17) \overset{\text{solving by rcp}}{\longrightarrow} (a,b,m) \overset{\text{decoding by rcp}}{\longrightarrow} y \tag{20}$$

The security of this procedure is goverened not by one key, as in the standard cases, but by the system (17) and Table 1, and by connection between a kind of signal ℓ_f and m-polyadic power (15), which are all unknown to the third party.

4. Example

Let us consider a concrete example of the proposed encryption/decryption procedure for the congruence class $[[a]]_b$ and one kind of signal $\ell_f = \ell_m \equiv \ell$, where ℓ is m-polyadic power. Each of such class gives (by Table 1) the arity m as the plaintext entry to transfer $y = m$. Next, we should choose the shape of the function $K(m, \ell)$ (18), which is, in general, arbitrary. In the simplest case, we take the same linear function

$$k_i^{(\ell)} = i - 1, \tag{21}$$

for all m-polyadic powers ℓ, but any functional dependence in (21) can be chosen, and it is different for different ℓ, which increases security of the procedure. The choice (21) gives

$$K(m, \ell) = \frac{1}{2}\ell(m-1)(\ell(m-1)+1). \tag{22}$$

So, the total amplitudes for different polyadic powers become

$$A_{tot}^{(\ell)} \equiv B_\ell = a \cdot (\ell(m-1)+1) + \frac{b}{2}\ell(m-1)(\ell(m-1)+1)\cdot \tag{23}$$

The recepient obtains the set of signals with amplitudes (23) as polyadic integers

$$\Psi_{tot}^{(\ell)} = B_\ell \cdot f^{(\ell)}(t). \tag{24}$$

To obtain the values of three variables (a, b, m), one needs three equations, i.e., three total amplitudes with different arbitrary polyadic powers $\ell = \ell_1, \ell_2, \ell_3 \in \mathbb{N}$. Because the general solution is too cumbersome, we choose the first three consequent polyadic powers $\ell = 1, 2, 3$, while any three natural numbers are possible to increase the security. This gives the following system of quadratic equations

$$a \cdot m + b \cdot \frac{(m-1)m}{2} = B_1, \tag{25}$$

$$a \cdot (2m-1) + b \cdot (m-1)(2m-1) = B_2, \tag{26}$$

$$a \cdot (3m-2) + b \cdot \frac{3(m-1)(3m-2)}{2} = B_3. \tag{27}$$

The general solution of the system is

$$m = \frac{7B_1 - 4B_2 + B_3 \mp \sqrt{B_1^2 - 8B_2B_1 - 2B_3B_1 + 16B_2^2 + B_3^2 - 8B_2B_3}}{4(3B_1 - 3B_2 + B_3)}, \tag{28}$$

$$a = 3B_1 - 3B_2 + B_3, \tag{29}$$

$$b = \frac{1}{(3B_1 - 3B_2 + B_3)(2B_2 - B_1 - B_3)} \times$$
$$\Big[\Big(11B_1^2 - 16B_2B_1 + 6B_3B_1 - 4B_2^2 + 4B_2B_3 - B_3^2\Big)(3B_1 - 3B_2 + B_3)$$
$$- \frac{105}{2}B_1^3 + \frac{333}{2}B_1^2B_2 - 162B_1B_2^2 + 48B_2^3 - \frac{113}{2}B_1^2B_3$$
$$+ 107B_1B_2B_3 - 46B_2^2B_3 - \frac{35}{2}B_1B_3^2 + \frac{29}{2}B_2B_3^2 - \frac{3}{2}B_3^3$$
$$\pm \left(\frac{15}{2}B_1^2 - \frac{39}{2}B_1B_2 + 12B_2^2 + 7B_1B_3 - \frac{17}{2}B_2B_3 + \frac{3}{2}B_3^2\right) \times$$
$$\sqrt{B_1^2 - 8B_2B_1 - 2B_3B_1 + 16B_2^2 + B_3^2 - 8B_2B_3} \Big]. \tag{30}$$

The sign in (28) and (30) should be chosen so that the solutions are ordinary integers.

In this particular case, for instance, the congruence class $[[3]]_4$ (6) has 5-ary addition, as follows from Table 1. So, if the sender wants to securely submit one element $y = m = 5$ from his plainintext (12), he applies the proposed encryption procedure and prepares three sums of (quantized analog) signals (having integer amplitudes) corresponding to the polyadic powers $\ell = 1, 2, 3$, as follows (using (16) and (23)):

$$\Psi_{tot}^{(1)} = 55 \cdot f^{(1)}(t), \tag{31}$$
$$\Psi_{tot}^{(2)} = 171 \cdot f^{(2)}(t), \tag{32}$$
$$\Psi_{tot}^{(3)} = 351 \cdot f^{(3)}(t), \tag{33}$$

where $f^{(1,2,3)}(t)$ are different (or the same) normalized signals. The recepient receives three (quantized analog) signals (31)–(33), and because he knows the normalized signals, he immediately obtains the integer values $B_1 = 55$, $B_2 = 171$, $B_3 = 351$. Inserting them into the system of quadratic equations (known to him ahead) (25)–(27), he (directly or using (28)–(30)) derives the values $m = 5$, $a = 3$, $b = 4$ and the desired element $y = m = 5$ from the initial plaintext (12). The same procedure should be provided for each element $y_j = y$ of the plaintext (12), which completes its decryption.

5. Conclusions

Thus, we proposed a principally new encryption/decryption procedure based on exploiting the signal processing. The main idea is to consider the signal parameters as polyadic integers being representative of the fixed polyadic ring, which is treated as some kind of polyadic discretization depending on the ring integer characteristics. They allow us to transfer numerical information from sender to recepient by submitting special sets of signals with genuine properties agreed before. The recepient knows the rules and equations to solve, to decrypt the initial plaintext. Security is achieved by using a mathematical process where public information is exchanged openly, but this information is useless without a corresponding piece of private, secret information that is never transmitted.

Author Contributions: Writing—original draft, S.D.; Writing—review and editing, Q.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Oppenheim, A.V. *Applications of Digital Signal Processing*; Prentice-Hall: Englewood Cliffs, NJ, USA, 1978.
2. Wang, B. *Digital Signal Processing Techniques and Applications in Radar Image Processing*; Wiley: Hoboken, NJ, USA, 2008. [CrossRef]
3. Berber, S. *Discrete Communication Systems*; Oxford University Press: Oxford, UK, 2021. [CrossRef]
4. Pedrouzo-Ulloa, A.; Troncoso-Pastoriza, J.R.; Pérez-González, F. Number theoretic transforms for secure signal processing. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1125–1140. [CrossRef]
5. Duplij, S. *Polyadic Algebraic Structures*; IOP Publishing: Bristol, UK, 2022; p. 461. [CrossRef]
6. Leeson, J.J.; Butson, A.T. On the general theory of (m, n) rings. *Algebra Universalis* **1980**, *11*, 42–76. [CrossRef]
7. Musayev, J.; Liscidini, A. Quantised inverter amplifier. *Electron. Lett.* **2018**, *54*, 416–418. [CrossRef]
8. Karthik, A.; V, A.; Nijhawan, G.; Rana, A.; Khan, I.; Naser, Z.L. Quantum signal processing: A new frontier in information processing. In Proceedings of the 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 1–3 December 2023; IEEE: New York, NY, USA, 2023; Volume 10, pp. 1527–1532. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

An Algorithm for Determining Whether the Quotient Ring Modulo an Ideal Has a Cyclic Basis

Hengjia Cao and Chang Tan *

Department of Mathematics, Northeast Forestry University, Harbin 150040, China; chj13044059685@163.com
* Correspondence: tanchang@nefu.edu.cn

Abstract: This paper focuses on the research of the existence of cyclic bases for the quotient ring modulo, a zero-dimensional ideal. Based on the necessary and sufficient condition for the existence of cyclic bases, it further deduces an equivalent condition for the existence of cyclic bases. In accordance with this condition, a new algorithm is proposed. The existence of a cyclic is determined by constructing a matrix and calculating its determinant in the algorithm. Compared with the original algorithm, it narrows the scope of the candidate element set and improves the computational efficiency of the algorithm.

Keywords: zero-dimensional ideal; width of an ideal; cyclic basis; multiplication matrix

MSC: 14Q20

1. Introduction

As a class of basis vector sets with cyclic structures, cyclic bases play a key role in the fields of mathematics and computer science. On the one hand, they can significantly simplify the representation form and analysis process of objects with cyclic characteristics [1]. On the other hand, they can effectively optimize the computational process and reduce the computational complexity in the research of coding theory. Cyclic bases also play an important role in the research of zero-dimensional ideals, especially in the field of solving rational univariate representations [2,3], and they also have significant applications in aspects such as the primary decomposition of ideals [3]. Therefore, the problem of solving the cyclic basis of the quotient ring of a zero-dimensional ideal is of great research significance.

Solving polynomial systems is a core problem in computational algebraic geometry, among which the classical symbolic methods include the Gröbner basis method [4], the resultant method [5], Wu's method [6], and so on. In subsequent research, many scholars have made improvements to these algorithms. For example, in the Gröbner basis method, the FGLM [7] algorithm proposed by Faugère in 1990 converts the symbolic computation of Gröbner bases into linear algebra computations, and this research pioneered a new problem-solving approach. Additionally, the F4 [8] and F5 [9] algorithms proposed by Faugère have improved the efficiency of computing lexicographic Gröbner bases. In Wu's method, Wang Dongming proposed the theory of regular systems [6], which is applied to triangular decomposition. In 2016, Wang Dongming established the connection between characteristic sets and lexicographic Gröbner bases [10]. Furthermore, based on this theory, many studies have focused on characteristic decomposition [11–13].

In recent years, a commonly used solution method has been the Rational Univariate Representation (RUR). Furthermore, in recent years, many scholars have devoted themselves to research in this field [14,15]. The Rational Univariate Representation (RUR) was

developed from the Shape Lemma. In 1999, Rouillier [16] proposed a method for computing the Rational Univariate Representation (RUR) of a general zero-dimensional ideal I. Some of the methods proposed by Rouillier have laid an important foundation for subsequent research on related theories. In 2003, Noro and Yokoyama proposed an algorithm for computing RUR using the modular method [17]. In 2010, Tan Chang, Zhang Shugong [18] and others extended Rouillier's algorithm to positive-dimensional ideals, making it possible to represent all zeros of the ideal$I$. In 2010, Zeng Guangxing and Xiao Shuijing [19] proposed computing RUR using Wu's method, which results in a more concise univariate representation but loses the multiplicity information of solutions. When the quotient ring of the corresponding ideal has a cyclic basis, both the corresponding ideal and the quotient ring possess favorable properties. In 2017, Shang Baoxin proposed that the existence of a cyclic basis in the quotient ring of a zero-dimensional ideal is equivalent to the ideal having a Shape basis. Furthermore, by virtue of the idea of basis transformation, he provided the RUR for zero-dimensional ideals with a Shape basis [3]. In 2021, Pan Jian combined the Gröbner basis with the zero-width theory, and proposed the necessary and sufficient conditions for the existence of a cyclic basis in the quotient ring of a zero-dimensional ideal. Based on these conditions, he further presented an existence judgment algorithm for the cyclic basis of the quotient ring by traversing the candidate elements in the set and computing the minimal polynomial of its multiplication matrix using fast linear algebra methods [2].

The cyclic basis judgment algorithm in Reference [2] requires traversing the candidate elements in the set and calculating their minimal polynomials one by one to verify the existence of cyclic bases in the quotient ring. Moreover, the calculation steps for the minimal polynomial of each candidate element are independent of each other and need to be performed repeatedly. By investigating the relationship between the coefficients of candidate elements and the width of the ideal, this paper derives the equivalent condition for the existence of cyclic bases in the quotient ring and designs an algorithm that constructs a matrix using the coefficients of candidate elements to determine whether cyclic bases exist. Compared with the original method, the proposed method has a smaller scope of the candidate element set and higher computational efficiency. This paper reveals the relationship between the coefficients of candidate elements and the width of the ideal, providing new ideas and methods for the research of subsequent related issues.

2. Preliminaries

Most of the concepts used in this paper will be introduced firstly.

Let K be a field of characteristic zero and $K[X]$ be the polynomial ring in n variables, where $K[X] = K[x_1, x_2, \ldots, x_n]$. Let $\bar{K}$ be the algebraic closure of K. Let $\mathbb{V}_{\overline{K}}(I) = \{z \in \overline{K}^n \mid h(z) = 0 \text{ for all } h \in I\}$ be the affine variety of the ideal I. Let T denotes the set of all monomials over $K[X]$, defined as $T = \{X^{\boldsymbol{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} | \boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n\}$. Let $\mathrm{lt}(h)$ denote the leading term of h.

Definition 1 ([5]). *If a finite subset $G = \{g_1, g_2, \ldots, g_n\}$ of an ideal I satisfies*

$$\langle \mathrm{lt}(G) \rangle \triangleq \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_n) \rangle,$$

then G is called a Gröbner basis of the ideal I with respect to the monomial order $\prec$.

Theorem 1 ([5]). *Let $I \subset K[x_1, \ldots, x_n]$ be a zero-dimensional ideal, then the following are equivalent:*

1. *$\mathbb{V}_K(I)$ is a finite set;*
2. *$K[x_1, \ldots, x_n]/I$ is a finite-dimensional space over K;*

3. *The K-vector space Span*$\{u = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \in T[X] | u \notin \langle lt(I) \rangle\}$ *is finite-dimensional.*

Definition 2 ([16]). *A polynomial* $t \in K[X]$ *is called a separating element of* $\mathbb{V}_{\overline{K}}(I)$ *if for all* $z_1, z_2 \in \mathbb{V}_{\overline{K}}(I)$ *with* $z_1 \neq z_2$*, it holds that* $t(z_1) \neq t(z_2)$*.*

Definition 3 ([20]). *Let* $I \subseteq K[X]$ *be a zero-dimensional ideal, and let* $N_1 = (\omega_1, \omega_2, \ldots, \omega_r)^T$ *be a basis vector of the monomial quotient ring with respect to the ordering* $\prec$*, where* $\dim(K[X]/I) = r$*. For a given* $h \in K[X]$*, suppose*

$$hN_1 \equiv (h\omega_1, h\omega_2, \ldots, h\omega_r)^T \equiv M_h N_1 \mod I,$$

Then $M_h \in K^{r \times r}$ *is called the multiplication matrix of h in the quotient ring* $K[X]/I$ *with respect to* N_1*.*

Proposition 1 ([16]). *Let* M_h *be the multiplication matrix of h in the quotient ring* $K[X]/I$ *with respect to* N_1*. For* $\alpha \in \mathbb{V}_{\overline{K}}(I)$*, let* $\mu(\alpha)$ *denote the multiplicity of* α*. Then the following hold:*

1. $Det(M_h) = \prod_{\alpha \in \mathbb{V}_{\overline{K}}(I)} h(\alpha)^{\mu(\alpha)}$.
2. $Tr(M_h) = \sum_{\alpha \in \mathbb{V}_{\overline{K}}(I)} h(\alpha)\mu(\alpha)$.
3. *The characteristic polynomial of the matrix* M_h *is* $\prod_{\alpha \in \mathbb{V}_{\overline{K}}(I)} (T - h(\alpha))^{\mu(\alpha)}$.

Let t be a separating element. By constructing the multiplication matrix M_t of t, it follows that each $t(z_i)$,where $z_i \in \mathbb{V}_{\overline{K}}(I)$, is an eigenvalue of the multiplication matrix.

This paper mainly studies problems in zero-dimensional ideals. Let $I = \langle f_1, f_2, \ldots, f_s \rangle$ be a zero-dimensional ideal in $K[X]$. By Theorem 1, it follows that $\mathbb{V}_{\overline{K}}(I) = \{z_1, z_2, \ldots, z_m\}$ is a finite set of points

3. Width of an Ideal

Let K be a field, $T(X) = T(x_1, x_2, \ldots, x_n)$ be the set of all monomials in the polynomial ring $K[X]$, where each monomial is of the form $u = x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$ with exponents $(\gamma_1, \gamma_2, \ldots, \gamma_n) \in \mathbb{N}^n$($\mathbb{N}$ denotes the set of non-negative integers). $\mathbb{V}_{\overline{K}}(I) = \{\xi_1, \xi_2, \cdots, \xi_m\}$. Define the operator:

$$\partial u = \frac{1}{\gamma_1! \gamma_2! \cdots \gamma_n!} \cdot \frac{\partial^{\gamma_1 + \gamma_2 + \cdots + \gamma_n}}{\partial x_1^{\gamma_1} \partial x_2^{\gamma_2} \cdots \partial x_n^{\gamma_n}}.$$

This operator ∂u is called a differential operator, and its degree is defined as $\sum_{i=1}^{n} \gamma_i$. In particular, $\partial 1$ denotes the identity operator, where the monomial $1 = x_1^0 x_2^0 \cdots x_n^0$.

Let $\mathcal{U} = \{\partial u \mid u \in T(X)\}$. Then the shift operator $\sigma_{x_j} : \mathcal{U} \to \mathcal{U} \cup \{0\}$ is defined as follows:

$$\sigma_{x_j}(\partial u) = \begin{cases} \dfrac{1}{\gamma_1! \gamma_2! \cdots (\gamma_j - 1)! \cdots \gamma_n!} \cdot \dfrac{\partial^{\gamma_1 + \gamma_2 + \cdots + (\gamma_j - 1) + \cdots + \gamma_n}}{\partial x_1^{\gamma_1} \partial x_2^{\gamma_2} \cdots \partial x_j^{\gamma_j - 1} \cdots \partial x_n^{\gamma_n}}, & \text{if } \gamma_j \geq 1; \\ 0, & \text{if } \gamma_j = 0. \end{cases}$$

Let $(\eta_1, \eta_2, \ldots, \eta_n) \in \mathbb{N}^n$ and $v = x_1^{\eta_1} x_2^{\eta_2} \cdots x_n^{\eta_n} \in T(X)$. By the relation $\sigma_{vx_i} = \sigma_v \sigma_{x_i}$, the operator $\sigma_v : \mathcal{U} \to \mathcal{U} \cup \{0\}$ is defined. Denote

$$\overrightarrow{\mathrm{Span}}_{\underline{K}}(\mathcal{U}) := \{\sum c_u \partial u \mid c_u \in \underline{K},\ u \in \mathcal{U}\}.$$

where $\underline{K}$ is the smallest algebraic extension field containing ξ_i for $1 \leq i \leq m$.

The degree of an element in $\overrightarrow{\mathrm{Span}}_{\underline{K}}(\mathcal{U})$ is the degree of the highest-degree differential operator ∂u within that element.

Definition 4 ([21]). *Let $\Delta \subset \overrightarrow{Span}_{\underline{K}}(\mathcal{U})$ be a linear space. If Δ is finite-dimensional and is closed under the action of all shift operators σ_v, then Δ is called a closed subspace.*

Definition 5 ([21]). *Let $I \subset K[X]$ be a zero-dimensional ideal, and let z be a zero of I. Consider a family of differential operators $\mathcal{L} = \{L_0 = \partial 1, L_1, \ldots, L_D\}$. Suppose these operators are linearly independent over the field K, and the subspace they span, $\Delta_z(I) := \overrightarrow{Span}_{\underline{K}}(L_0, L_1, \ldots, L_D)$, is a closed subspace. Furthermore, if for all $L \in \Delta_z(I)$ and all $f \in I$, it holds that $L(f)|_{X=z} = 0$, then $\Delta_z(I)$ is called the closed subspace of differential operators at the zero z.*

Let q be a non-negative integer, then $\Delta_z^{(q)}(I)$ is called the closed space of differential operators with degree not exceeding q in $\Delta_z(I)$.

Based on the above conditions, the definition of the width of a zero pint is as follows.

Definition 6 ([22]). *Let $z \in \mathbb{V}_{\overline{K}}(I)$. The width κ of z is defined as:*

$$\kappa = \dim\left(\Delta_z^{(1)}(I)\right) - \dim\left(\Delta_z^{(0)}(I)\right), \quad 0 \leqslant \kappa \leqslant n.$$

Furthermore,we can define the width of an ideal.

Definition 7 ([2]). *The width of an ideal I is defined as the maximum width of the maximum width of the zero points of ideal I.*

4. The Equivalent Condition for the Existence of a Cyclic Basis in the Quotient Ring Modulo a Zero-Dimensional Ideal

Focusing on a zero-dimensional ideal I, this section first puts forward the following conclusion: if the width of a zero-dimensional ideal Idoes not exceed 1, its quotient ring necessarily has a cyclic basis. Based on this, the main work of this section is to obtain the equivalence condition for the width of I being at most 1 by integrating the definition of width. This condition is also the equivalent condition for the existence of a cyclic basis in its quotient ring. This section will also prove the feasibility of this condition, which provides essential theoretical support for verifying the rationality of the algorithm in the following sections.

Lemma 1 ([23]). *If $z \in \mathbb{V}_{\overline{K}}(I)$ satisfies $\dim\left(\Delta_z^{(1)}(I)\right) - \dim\left(\Delta_z^{(0)}(I)\right) = \kappa$, $1 \leq \kappa \leq n$, then for any $t \in \mathbb{N} \setminus \{0\}$, the following holds:*

$$\dim\left(\Delta_z^{(t)}(I)\right) - \dim\left(\Delta_z^{(t-1)}(I)\right) \leq \binom{\kappa + t - 1}{\kappa - 1}.$$

Based on the lemma, without loss of generality, we take the first variable z_1 for any $z \in \mathbb{V}_{\overline{K}}(I)$. If $\dim\left(\Delta_z^{(1)}(I)\right) - \dim\left(\Delta_z^{(0)}(I)\right) = 1$, then for any $t \in \mathbb{N} \setminus \{0\}$, the following holds:

$$\dim\left(\Delta_z^{(t)}(I)\right) - \dim\left(\Delta_z^{(t-1)}(I)\right) \leq 1.$$

Definition 8 ([2]). *If the maximum width among the zeros of the ideal I is 1, then the ideal I is said to have width 1.*

The following proposition is easily obtained.

Proposition 2. *If the width of an ideal I is at most 1, then there exists $k \in K$ such that the multiplication matrix M_t corresponding to $t = x_1 + kx_2 + \cdots + k^{n-1}x_n$ is a non-defective matrix.*

Corollary 1. *If the multiplication matrix M_t corresponding to any $t = x_1 + kx_2 + \cdots + k^{n-1}x_n$, is a defective matrix, then the width of the ideal is at least 2.*

Theorem 2 ([2])**.** *Let $I \subseteq K[X]$ be a zero-dimensional ideal. The necessary and sufficient condition for the width of I to be at most* 1 *is that $K[X]/I$ has a cyclic basis.*

From the above theorem, we can conclude that whether an quotient ring has a cyclic basis can be determined by verifying its width.

Let $N = (\omega_1, \omega_2, \ldots, \omega_r)^T$ be the monomial basis of the quotient ring $K[X]/I$. Then, for every $f \in K[X]$, its residue class $[f]$ modulo the ideal I can be expressed in terms of the monomial basis N. That is, there exist $a_i \in K$ for $i = 1, \ldots, r$ such that $[f] = a_1\omega_1 + \cdots + a_r\omega_r$. It is easily seen that the vector of $[f]$ with respect to the monomial basis is

$$\overrightarrow{[f]} = (a_1, a_2, \ldots, a_r).$$

For any $f^i \in K[X]$, we have $[f^i] \in K[X]/I$. Define $\overrightarrow{[f^i]} = (a_{i1}, a_{i2}, \ldots, a_{ir})$, where $[1] = (1, 0, \ldots, 0)$. For the convenience of subsequent notation in the paper, denote $[1] = (a_{01}, a_{02}, \ldots, a_{0r})$.

We now proceed to present the equivalent theorems for determining the width of an ideal.

Theorem 3. *Let I be a zero-dimensional ideal. Let $t = x_1 + kx_2 + \cdots + k^{n-1}x_n \in K[X]$ where $k \in \mathbb{Z}$. Denote the vector of $[t^i]$ with respect to the monomial basis as $\overrightarrow{[t^i]} = (a_{i1}, a_{i2}, \ldots, a_{ir})$. Then we have that the width of I is at least* 2 *, if and only if, for all $k \in \mathbb{Z}$, $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ are linearly dependent.*

Proof. It is easily seen that, for all $k \in \mathbb{N}$, the linear dependence of $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ is equivalent to the system of equations

$$\begin{cases} a_{01}x_1 + a_{11}x_2 + \cdots + a_{r-1,1}x_r = 0, \\ a_{02}x_1 + a_{12}x_2 + \cdots + a_{r-1,2}x_r = 0, \\ \vdots \\ a_{0r}x_1 + a_{1r}x_2 + \cdots + a_{r-1,r}x_r = 0, \end{cases} \tag{1}$$

having a non-trivial solution for any $k \in \mathbb{Z}$.

"$\Leftarrow$" Let $N = (\omega_1, \omega_2, \ldots, \omega_r)^T$ be the monomial basis of the quotient ring $K[X]/I$. Since for $\forall k \in \mathbb{Z}$, the system of (1) has a non-trivial solution, denoted as $(b_0, \ldots, b_{r-1})$. Then for all $k \in \mathbb{Z}$, we have:

$$b_0 \cdot \overrightarrow{[1]} + b_1 \cdot \overrightarrow{[t]} + \cdots + b_{r-1} \cdot \overrightarrow{[t^{r-1}]} = \overrightarrow{0}.$$

It follows that

$$\left(b_0 \cdot \overrightarrow{[1]} + b_1 \cdot \overrightarrow{[t]} + \cdots + b_{r-1} \cdot \overrightarrow{[t^{r-1}]} \right) \cdot (\omega_1, \omega_2, \ldots, \omega_r)^T = 0.$$

That is,

$$b_0 + b_1 \cdot [t] + \cdots + b_{r-1} \cdot [t^{r-1}] = 0.$$

Since $\sum_{i=0}^{r-1} b_i[t^i] = 0$, we have $\sum_{i=0}^{r-1} b_i t^i \in I$. Thus, for any monomial $x^\alpha \in K[X]$, it holds that

$$x^\alpha \cdot \sum_{i=0}^{r-1} b_i t^i \in I.$$

In other words, $x^\alpha \cdot \sum_{i=0}^{r-1} b_i t^i = \sum_{i=0}^{r-1} b_i x^\alpha t^i \in I$, which implies $\sum_{i=0}^{r-1} b_i[x^\alpha t^i] = 0$.

Taking $x^\alpha = 1$, we obtain the following:

$$\sum_{i=0}^{r-1} b_i \cdot 1 \cdot t^i = \sum_{i=0}^{r-1} b_i[t^i] = 0.$$

That is,

$$\sum_{i=0}^{r-1} b_i(1, 0, 0, \cdots, 0) M_{t^i}(\omega_1, \ldots, \omega_r)^T = 0,$$

which shows that the first row of $\sum_{i=0}^{r-1} b_i M_{t^i}$ is entirely zero.

Taking $x^\alpha = \omega_2$, we obtain:

$$\sum_{i=0}^{r-1} b_i \cdot \omega_2 \cdot t^i = \sum_{i=0}^{r-1} b_i[\omega_2 t^i] = 0.$$

That is,

$$\sum_{i=0}^{r-1} b_i(0, 1, 0, \cdots, 0) M_{t^i}(\omega_1, \ldots, \omega_r)^T = 0,$$

which shows that the second row of $\sum_{i=0}^{r-1} b_i M_{t^i}$ is entirely zero.

$\vdots$

Taking $x^\alpha = \omega_r$, we obtain:

$$\sum_{i=0}^{r-1} b_i \cdot \omega_r \cdot t^i = \sum_{i=0}^{r-1} b_i[\omega_r t^i] = 0.$$

That is,

$$\sum_{i=0}^{r-1} b_i(0, 0, \cdots, 1) M_{t^i}(\omega_1, \ldots, \omega_r)^T = 0,$$

which shows that the r-th row of $\sum_{i=0}^{r-1} b_i M_{t^i}$ is entirely zero.

In summary, $\sum_{i=0}^{r-1} b_i M_{t^i}$ is the zero matrix. Let $h(x) = b_0 + b_1 \cdot x + \cdots + b_{r-1} \cdot x^{r-1}$, then $h(M_t) = 0$.

Let the minimal polynomial of the multiplication matrix M_t be $h_\alpha(x)$. Then $h_\alpha(x) \mid h(x)$. It is easily seen that $\deg(h_\alpha(x)) \leq \deg(h(x)) \leq r - 1$. Hence, the characteristic polynomial cannot be equal to the minimal polynomial, meaning the multiplication matrix M_t is a defective matrix. By Corollary 1, the width of the ideal I is at least 2.

"⇒" Since the width of I is at least 2, $K[X]/I$ has no cyclic basis. This implies there does not exist any generator $t \in K[X]$ such that $\{1, t, t^2, \ldots, t^{r-1}\}$ forms a cyclic basis. In other words, there exist scalars $b_0, b_1, \ldots, b_{r-1}$, not all zero, that satisfy

$$b_0 + b_1[t] + \cdots + b_{r-1}[t^{r-1}] = 0.$$

That is,

$$(b_0 + b_1 t + \cdots + b_{r-1} t^{r-1}) \mod I = 0,$$

which implies:

$$b_0 + b_1 \cdot [t] + \cdots + b_{r-1} \cdot [t^{r-1}] = 0.$$

Thus, we have $b_0 \cdot \overrightarrow{[1]} + b_1 \cdot \overrightarrow{[t]} + \cdots + b_{r-1} \cdot \overrightarrow{[t^{r-1}]} = \overrightarrow{0}$.
This means the system of equations

$$\begin{cases} a_{01}x_1 + a_{11}x_2 + \cdots + a_{r-1,1}x_r = 0, \\ a_{02}x_1 + a_{12}x_2 + \cdots + a_{r-1,2}x_r = 0, \\ \vdots \\ a_{0r}x_1 + a_{1r}x_2 + \cdots + a_{r-1,r}x_r = 0, \end{cases}$$

has a non-trivial solution for all $k \in \mathbb{Z}$. □

By Theorem 3, we can derive the following corollary:

Corollary 2. *The width of the ideal I is at most 1 ,if and only if, there exists $k \in \mathbb{Z}$ such that $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ are linearly independent, where $t = x_1 + kx_2 + \cdots + k^{n-1}x_n \in K[X]$.*

Herein, we present equivalent conditions for the ideal I to have a width of at most 1. Since a width of at most 1 implies that the corresponding quotient ring has a cyclic basis, determining the width of the ideal is important for solving the problem. Subsequently, we provide a method for judging the width of the ideal based on the equivalent conditions.

Theorem 4. *The width of the ideal I is at least 2 if, for all integers $k \in \mathbb{Z}$ where $0 \leq k \leq r(r-1)\frac{(n-1)}{2}$, the vectors $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ are linearly dependent.*

Proof. Denote the coefficient matrix of the system of (1) as:

$$A = \begin{pmatrix} a_{01} & a_{11} & \cdots & a_{r-1,1} \\ a_{02} & a_{12} & \cdots & a_{r-1,2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0r} & a_{1r} & \cdots & a_{r-1,r} \end{pmatrix}.$$

By Theorem 3, the width of the ideal I being at least 2 is equivalent to the system (1) having a non-trivial solution for all $k \in \mathbb{N}$. From the existence theorem for solutions of homogeneous linear systems, $Ax = 0$ has a non-trivial solution if and only if the rank of the coefficient matrix A is less than the number of unknowns, i.e., $\text{rank}(A) < n$. This is equivalent to $|A| = 0$. Since $|A|$ is an r-th order determinant, and by the earlier definition, $a_{01} = 1$ and $a_{02} = \cdots = a_{0r} = 0$, the first column of matrix A is $(1, 0, \ldots, 0)^T$. By properties of determinants, computing $|A|$ is equivalent to computing the determinant of the matrix:

$$B = \begin{pmatrix} a_{12} & \cdots & a_{r-1,2} \\ \vdots & \ddots & \vdots \\ a_{1r} & \cdots & a_{r-1,r} \end{pmatrix}.$$

For an $l \times l$ matrix $M = [m_{ij}]$, its determinant can be expressed as the algebraic sum over all permutations, by properties of determinants:

$$\text{Det}(M) = \sum_{\sigma \in S_l} \text{sgn}(\sigma) \cdot m_{1\sigma(1)} m_{2\sigma(2)} \cdots m_{l\sigma(l)}.$$

where S_l is the set of all permutations of $\{1, 2, \ldots, l\}$, σ denotes a permutation, $\sigma(i)$ indicates the column index of the element in row i, and $\text{sgn}(\sigma)$ is the sign of the permutation ($+1$ for even permutations, -1 for odd permutations). Since the determinant of a transpose equals

the determinant of the original matrix, we may without loss of generality consider products of elements selected column-wise.

By the earlier definition, the degree of the function t with respect to k is $n-1$, so the degree of $[t]$ with respect to k is at most $n-1$. The degree of t^2 with respect to k is $2(n-1)$, so the degree of $[t^2]$ with respect to k is at most $2(n-1)$. Similarly, the degree of t^i with respect to k is $i(n-1)$, so the degree of $[t^i]$ with respect to k is at most $i(n-1)$ for $0 \leq i \leq r-1$. It follows that each term $a_{0\sigma(1)}a_{1\sigma(2)}\cdots a_{r-1\sigma(r)}$ in the determinant sum has a maximum degree with respect to k of $r(r-1)\frac{(n-1)}{2}$. Thus, the determinant itself has a maximum degree with respect to k of $r(r-1)\frac{(n-1)}{2}$, so we can express $\mathrm{Det}(A)$ as a polynomial in k:

$$\mathrm{Det}(A) = b_{r(r-1)\frac{(n-1)}{2}}k^{r(r-1)\frac{(n-1)}{2}} + \cdots + b_1k + b_0.$$

where $b_0, b_1, \ldots, b_{r(r-1)\frac{(n-1)}{2}} \in \mathbb{Z}$.

We conclude that $\det(A)$ is a polynomial in k of degree $r(r-1)\frac{(n-1)}{2}$, so $\det(A) = 0$ has at most $r(r-1)\frac{(n-1)}{2}$ solutions. Therefore, if $g(k) = 0$ holds for all k from 0 to $r(r-1)\frac{(n-1)}{2}$,then the polynomial of the $\mathrm{Det}(A)$ with respect to the variable k is the zero polynomial, i.e., $\mathrm{Det}(A) = 0$ identically. Hence, the width of the ideal I is at least 2. □

By Corollary 2 and Theorem 4, we obtain the following theorem.

Theorem 5. *The width of the ideal I is at most 1 if there exists $k \in \mathbb{Z}$ with $0 \leq k \leq r(r-1)\frac{(n-1)}{2}$ such that $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ are linearly independent.*

The theorem implies that if the determinant is non-zero when $k = j$ (where $0 \leq j \leq r(r-1)\frac{(n-1)}{2}$), then the width of the ideal I is at most 1. Conversely, if the determinant is zero for all k with $0 \leq k \leq r(r-1)\frac{(n-1)}{2}$, then the width of the ideal I is at least 2. Thus, it suffices to check all integers k from 0 to $r(r-1)\frac{(n-1)}{2}$ to determine the width of the ideal I.

5. Algorithm for Determining the Width of an Ideal

By Theorem 5 from the previous section, if the width of the ideal is at most 1, then in the set

$$T = \left\{ t = x_1 + kx_2 + \cdots + k^{n-1}x_n \mid 0 \leq k \leq r(r-1)\frac{(n-1)}{2} \right\},$$

there exists at least one candidate element t such that the determinant of the matrix formed by its corresponding vectors is non-zero. Therefore, by determining whether there exists an element in the set T such that the determinant of the matrix formed by the vector corresponding to this element is non-zero, we can further judge whether the width of the ideal I is at most 1.

In the algorithm, since computing $\overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ individually involves extensive calculations, the computation of these vectors can be simplified as follows.

Since $t \cdot \omega_1 \mod I = [t]$, we have $\overrightarrow{[t]} = (1, 0, \ldots, 0) \cdot M_t$. Similarly, $\overrightarrow{[t^2]} = (1, 0, \ldots, 0) \cdot M_{t^2} = (1, 0, \ldots, 0) \cdot M_t \cdot M_t$, which implies $\overrightarrow{[t^2]} = \overrightarrow{[t]} \cdot M_t$. This leads to the recursive formula for the vectors:

$$\overrightarrow{[t^i]} = \overrightarrow{[t^{i-1}]} \cdot M_t$$

It follows from Theorem 3 that if there exists $[t^i]$ which is a zero vector, then it can be directly concluded that the width of the ideal is at least 2. The following presents a method for determining the width of an ideal.

Algorithm 1 Algorithm for Determining the Width of an Ideal

Input: Ideal I, the monomial basis $N = (\omega_1, \omega_2, \ldots, \omega_r)^T$ of the quotient ring $K[X]/I$ with respect to the order $\prec_{\text{grevlex}}$ and the multiplication matrix M_{x_i} of x_i with respect to N.
Output: The width of the ideal I.
Step 1: From the set $T = \{t = x_1 + kx_2 + \cdots + k^{n-1}x_n \mid 0 \leqslant k \leqslant (n-1)^{\frac{r(r-1)}{2}}\}$, compute $\overrightarrow{[1]}, \overrightarrow{[t]}, \ldots, \overrightarrow{[t^{r-1}]}$ one by one in the order of increasing k. If any vector is $\overrightarrow{0}$, select the next k and repeat Step 1; otherwise, proceed to Step 2.
Step 2: Form these vectors into an r-th order matrix $A = (\overrightarrow{[1]}^T, \overrightarrow{[t]}^T, \cdots, \overrightarrow{[t^{r-1}]}^T)^T$. Remove the first row and the first column of A, and denote the matrix formed by the remaining elements as B.
Step 3: Compute $\text{Det}(B)$. If $\text{Det}(B) \neq 0$, terminate the computation and return that the width of the ideal I is at most 1.
Step 4: If for all $k \in \mathbb{N}$ where $0 \leqslant k \leqslant (n-1)^{\frac{r(r-1)}{2}}$, $\det(B) = 0$ holds, then return that the width of the ideal I is at least 2.

Proposition 3. *Let $I \subseteq K[X]$ be a zero-dimensional ideal, $\dim(K[X]/I) = r$, and $T = \left\{t = x_1 + kx_2 + \cdots + k^{n-1}x_n \mid 0 \leqslant k \leqslant (n-1)^{\frac{r(r-1)}{2}}\right\}$. Then the complexity of Algorithm 1 determines the Width of an Ideal is at most*

$$O\left(\frac{5}{6}nr^5\right)$$

basic arithmetic operations in K.

Proof. In complexity analysis, addition operations can be omitted since their order is lower than that of multiplication operations. Moreover, the most general case is considered in the analysis. From the formula $\overrightarrow{[t^i]} = \overrightarrow{[t^{i-1}]} \cdot M_t, i = 1, 2, \cdots, r-1$, the complexity of computing a single vector $\overrightarrow{[t^i]}$ requires $O(r^2)$ arithmetic operations in K. It follows that the complexity of Step 1 in Algorithm 1 needs $O(r^2(r-2)) = O(r^3)$arithmetic operations in K.

For computing the determinant of an $(r-1)$-th order matrix, we first transform the matrix into an upper triangular matrix via row operations and then multiply the diagonal elements. The arithmetic operations of this process is at most $O\left(\frac{2r^3}{3}\right)$.

That is, the arithmetic operations of determining whether the coefficients of a candidate element satisfy the existence condition of a cyclic basis is at most $O\left(\frac{5r^3}{3}\right)$.Let H_i denote the complexity of judging one candidate element in Algorithm 1. From the above analysis, it is known that computing H_i needs at most $O\left(\frac{5r^3}{3}\right)$arithmetic operations in K. According to the most general case, the maximum number of steps requires iterating over $0 \leq k \leq \frac{(n-1)r(r-1)}{2}$, and calculating the determinant value of the candidate element corresponding to each k to determine the width of the ideal. The total complexity of Algorithm 1 is $O\left(\sum_{i=0}^{\frac{(n-1)r(r-1)}{2}} H_i\right)$.

When each H_i, $(i = 1, 2, \ldots, r)$ takes its maximum value, the expression simplifies to:

$$O\left(\frac{(n-1)r(r-1)}{2} \cdot \frac{5r^3}{3}\right) = O\left(\frac{5}{6}nr^5\right).$$

That is, the complexity of Algorithm 1 is at most $O\left(\frac{5}{6}nr^5\right)$. □

It follows from [2] that the complexity of the original algorithm is at most

$$O(\frac{3}{2}n(r^5 + r^4\log(r)\log(\log(r)))).$$

From the complexities of the new algorithm and the original algorithm, it can be seen that the efficiency of the new algorithm is superior to that of the original algorithm.

Example 1. *Consider the ideal* $J = \langle x^2 - yz, -xz + y^2, -xy + z^2, xyz - x, y^3 - y \rangle$.

Using Maple 2024, we compute the Gröbner basis of the ideal J *in the quotient ring* $K[x, y, z]/J$ *as* $G = [x - y, -y^2 + yz, -y^2 + z^2, y^3 - y]$, *and its monomial basis as* $(1, y, z, y^2)$. *Thus, the set of candidate elements is* $T = \{t = x + ky + k^2 z \mid 0 \leqslant k \leqslant 12\}$.

We implement Algorithm 1 using Maple. When substituting $k = 1$, *we obtain* $t = x + y + z$, *and the corresponding multiplication matrix is*

$$M_t = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 9 \\ 0 & 27 & 0 & 0 \end{bmatrix}.$$

The corresponding matrix B *is computed as*

$$B = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 0 & 9 \\ 27 & 0 & 0 \end{bmatrix},$$

i.e., $\mathrm{Det}(B) \neq 0$.

The algorithm terminates at $k = 1$, *and we conclude that the width of the ideal* J *is at most 1, meaning there exists a cyclic basis in the quotient ring* $K[x, y, z]/J$.

Example 2. *Consider the ideal* $I = \langle x^3 - yz, y^3 - xz, -x^2 y + z^2, x^2 y^2 - z \rangle \subseteq K[x, y, z]$.

Using Maple, we compute the Gröbner basis of the ideal I *in the quotient ring* $K[x, y, z]/I$ *as*

$$G = [xz - z, yz - z, z^2 - z, x^3 - z, x^2 y - z, y^3 - z],$$

its monomial basis as $[1, x, y, z, x^2, yx, y^2, y^2 x]$. *Thus, the set of candidate elements is* $T = \{t = x + ky + k^2 z \mid 0 \leqslant k \leqslant 56\}$.

Implementing Algorithm 1 with Maple, the algorithm terminates at $k = 56$, *we find that for all candidate elements, the determinant of the matrix corresponding to their coefficients is zero. We conclude that the width of the ideal* I *is at least 2, meaning that* I *does not admit a cyclic basis.*

6. Conclusions

This paper takes zero-dimensional ideals as the main research object, focusing on the problem of determining the existence of cyclic bases for their quotient rings. By combining the structural properties of quotient ring bases of zero-dimensional ideals when the ideal width is at most 1 with Gröbner basis theory, the study derives equivalent characterization conditions for the ideal width being at most 1. Further, using matrix theories, it designs an algorithm for determining the ideal width. Relying on the connection between ideal width being at most 1 and the existence of cyclic bases in quotient rings, the determination of the existence of cyclic bases in quotient rings is realized.

Compared with traditional methods, the method proposed in this paper designs an algorithm to judge the existence of a cyclic basis based on the relationship between the coefficients of the candidate elements and the width of the ideal. It reduces the scope of the candidate element set compared with the original method, provides a new approach for the cyclic basis judgment of the quotient ring of zero-dimensional ideals, and also offers new ideas for algorithm optimization in subsequent related fields.

Author Contributions: Conceptualization, H.C. and C.T.; software, H.C.; validation, H.C.; writing—original draft preparation, H.C.; writing—review and editing, C.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Scientific Research Project of Northeast Forestry University (Grant No. HKF250900005).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions of this study are contained in this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Steel A. A new algorithm for the computation of canonical forms of matrices over fields. *J. Symb. Comput.* **1997**, *24*, 409–432. [CrossRef]
2. Pan, J.; Shang, B.; Li, Z.; Zhang, S. Computing PUR of Zero-Dimensional Ideals of Breadth at Most One. *J. Syst. Sci. Complex* **2021**, *34*, 2396–2409. [CrossRef]
3. Shang, B.; Zhang, S.; Tan, C.; Xia, P. A simplified rational representation for positive-dimensional polynomial systems and SHEPWM equations solving. *J. Syst. Sci. Complex.* **2017**, *30*, 1470–1482. [CrossRef]
4. Buchberger B. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringses Nach Einem Nulldimensionalen Polynomideal. Ph.D. Thesis, Universität Innsbruck, Innsbruck, Austria, 1965.
5. Cox, D.A.; Little, J.; O'Shea, D. *Ideals, Varieties, and Algorithms*, 2nd ed.; Springer Science+Business Media: New York, NY, USA, 1992.
6. Wang, D. *Elimination Methods*; Springer Science and Business Media: Vienna, Austria, 2001.
7. Faugere, J.C.; Gianni, P.; Lazard, D.; Mora, T. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.* **1993**, *16*, 329–344. [CrossRef]
8. Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra* **1999**, *139*, 61–88. [CrossRef]
9. Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Lille, France, 7–10 July 2002; pp. 75–83.
10. Wang, D.; Dong, R.; Mou, C. Decomposition of polynomial sets into characteristic pairs. *Math. Comput.* **2020**, *89*, 1993–2015. [CrossRef]
11. Dong, R.; Wang, D. Computing strong regular characteristic pairs with Gröbner bases. *J. Symb. Comput.* **2021**, *104* 312–327. [CrossRef]
12. Wang, L.; Mou, C. Simple Characteristic Decomposition of Polynomial Sets. *J. Syst. Sci. Complex* **2025**, *38*, 1226–1242. [CrossRef]
13. Wang, D.; Wang, L. Decomposition of Polynomial Ideals into Triangular Regular Sequences. In Proceedings of the International Symposium on Symbolic and Algebraic Computation, Raleigh, NC, USA, 16–19 July 2024; pp. 244–253.
14. Xiao, S.; Zeng, G. Decomposing the Radicals of Polynomial Ideals by Rational Univariate Representations. *J. Syst. Sci. Complex* **2023**, *36*, 2703–2724. [CrossRef]
15. Xiao, S.; Zeng, G. Irredundant Decomposition of the Radicals of Polynomial Ideals Based on Rational Univariate Representations. *J. Syst. Sci. Complex* **2025**, 1–22. [CrossRef]
16. Rouillier, F. Solving zero-dimensional systems through the Rational Univariate Representation. *Appl. Algebra Eng. Commun. Comput.* **1999**, *9*, 433–461. [CrossRef]
17. Noro, M.; Yokoyama, K. A modular method to compute the Rational Univariate Representation of zero-dimensional ideals. *J. Symb. Comput.* **1999**, *28*, 243–263. [CrossRef]
18. Tan, C.; Zhang, S. Computation of the Rational Representation for Solutions of High-dimensional Systems. *Comm. Math. Res.* **2010**, *26*, 119–130.
19. Zeng, G.X.; Xiao, S.J. Computing the rational univariate representations for zero-dimensional systems by Wu's method. *Sci. Sin. Math.* **2010**, *40*, 999–1016.
20. Cox, D.; Little, J.; O'shea, D. *Using Algebraic Geometry*, 2nd ed.; Springer: New York, NY, USA, 2005.
21. Marinari, M.G.; Möller, H.M.; Mora T. Gröbner basis of ideals defined by functionals with an application to ideals of projective points. *Appl. Algebra Eng. Commun. Comput.* **1993**, *4*, 103–145. [CrossRef]

22. Dayton, B.H.; Zeng, Z.G. Computing the multiplicity structure in solving polynomial systems. In Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, Beijing, China, 24–27 July 2005; pp. 116–123.
23. Zeng, Z. The closedness subspace method for computing the multiplicity structure of a polynomial system. *Contemp. Math.* **2009**, *496*, 347. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

axioms

MDPI

Article

On the Existence of Optimal $(v, 5, 1)$ and $(v, 6, 1)$ Binary Cyclically Permutable Constant-Weight Codes

Tsonka Baicheva [1,2,*] and Svetlana Topalova [1,2]

[1] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; svetlana@math.bas.bg
[2] Centre of Excellence in Informatics and Information and Communication Technologies, 1113 Sofia, Bulgaria
* Correspondence: tsonka@math.bas.bg

Abstract

The problem of the existence of optimal $(v, k, 1)$ binary cyclically permutable constant-weight (CPCW) codes has been completely solved for codeword weights $k < 5$. We consider the smallest open cases, namely $k = 5$ and $k = 6$. We present such codes for small values of the code length v and derive necessary conditions for the existence of optimal $(k(k-1)t + 2, k, 1)$ CPCW codes. These necessary conditions can be used to construct such codes, as well as to show that optimal codes with some parameters do not exist. In particular, we use them to prove that an optimal $(92, 6, 1)$ CPCW code does not exist.

Keywords: coding theory; binary cyclically permutable constant-weight code; optical orthogonal code; cyclic design

MSC: 94B60; 94B65

1. Introduction

1.1. Definitions

Denote by $\mathbb{Z}_v$ the additive group of integers modulo v. Let $C = \{c_0, c_1, \ldots, c_{k-1}\}$ be a k-element subset of $\mathbb{Z}_v$. Then, $\triangle C = \{c_i - c_j |\ i, j = 0, 1, \ldots, k-1; i \neq j\}$ is the multiset of differences of C, and $C + t$ denotes a t-translate of C, where $C + t = \{c_0 + t, c_1 + t, \ldots, c_{k-1} + t\}$ for $t \in \mathbb{Z}_v$.

Definition 1. *A $(v, k, 1)$ binary cyclically permutable constant-weight (CPCW) code of size s can be defined as a collection $\mathcal{C} = \{C_1, \ldots, C_s\}$ of k-subsets of $\mathbb{Z}_v$ (codewords) such that any two distinct translates of a codeword share at most one element, and any two translates of two distinct codewords also share at most one element:*

$$|C_i \cap (C_i + t)| \leq 1,\ \ 1 \leq i \leq s,\ \ 1 \leq t \leq v-1 \tag{1}$$

$$|C_i \cap (C_j + t)| \leq 1,\ \ 1 \leq i < j \leq s,\ \ 0 \leq t \leq v-1 \tag{2}$$

Everywhere in the text that follows, the abbreviation *CPCW* means "binary cyclically permutable constant weight". Originally, a CPCW code was defined as a collection of $\{0, 1\}$ sequences, but, for some purposes, it is easier to present the codewords as subsets of $\mathbb{Z}_v$, and that is why the above definition is widely used too. Condition (1) is called the auto-correlation property and (2) the cross-correlation property. We denote by s the *size* of $\mathcal{C}$, namely the number of its codewords.

Consider a codeword $C = \{c_0, c_1, \ldots, c_{k-1}\}$. The auto-correlation property means that all the differences of a codeword of a $(v, k, 1)$ CPCW code are different, and the cross-correlation property means that $\triangle C_1 \bigcap \triangle C_2 = \emptyset$ for two codewords C_1 and C_2. Since $|\triangle C| = k(k-1)$, the size of a $(v, k, 1)$ CPCW code cannot exceed

$$\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor.$$

CPCW codes that reach this bound are called *optimal* [1,2].

If the code size is exactly $(v-1)/k(k-1)$, the optimal $(v, k, 1)$ CPCW code is *perfect*; that is, all nonzero differences are covered.

CPCW codes are related to many other combinatorial structures. Definition 1, for instance, holds for a $(v, k, 1)$ optical orthogonal code (OOC) too [1]. In this paper, we will use the relation to partial designs.

Definition 2. *Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of points and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ be a finite collection of k-element subsets of V, called blocks. $D = (V, \mathcal{B})$ is a design (partial design) with parameters 2-(v,k,1) if any 2-subset of V is contained in exactly (at most) one block of $\mathcal{B}$. A 2-(v,k,1) design is also called a Steiner system and denoted by $S(2, k, v)$.*

Partial designs are also known as *packings* [3] or *packing designs* [4]. We call them partial designs following [5]. An *automorphism* of a 2-$(v, k, 1)$ partial design D is a permutation of its points that maps each block of D to a block of D.

Definition 3. *A 2-(v,k,1) design (partial design) is cyclic if it has an automorphism α permuting its points in one cycle, and it is strictly cyclic if each block orbit under this automorphism is of length v (no short orbits).*

A cyclic partial design with the maximum possible number of blocks is optimal.

Definition 4. *A circulant matrix (circulant) of order v is a (0,1) square matrix $M = (m_{i,j})_{v \times v}$ with v rows and columns such that $m_{i+1,j+1} = m_{i,j}$, $i, j \in \mathbb{Z}_v$.*

Perfect $(v, k, 1)$ CPCW codes are equivalent to strictly cyclic 2-$(v, k, 1)$ designs. An optimal $(v, k, 1)$ CPCW code is equivalent to an optimal 2-$(v, k, 1)$ strictly cyclic partial design. The incidence matrix of a 2-$(v, k, 1)$ strictly cyclic partial design contains submatrices, which are circulant matrices of order v. Each such circulant matrix corresponds to the translates of one of the codewords of the corresponding optimal $(v, k, 1)$ CPCW code. An example illustrating this equivalence is presented in Figure 1.

We are not going to define more related structures here. We shall only mention that optimal $(v, k, 1)$ CPCW codes correspond to $(v, k; \lfloor (v-1)/k(k-1) \rfloor)$ difference packings, and that perfect $(v, k, 1)$ CPCW codes are equivalent to $(v, k, 1)$ cyclic difference families. An interested reader can find more information, for instance, in [6,7].

1.2. Known Results and the Contribution of the Present Paper

Optimal $(v, k, 1)$ CPCW codes are studied in [2,8–10]. There are also many results on CPCW codes that were obtained for related combinatorial objects, like optical orthogonal codes [11–21], difference families [6,22–26], and combinatorial designs [27–30].

It was proved in [12] that an optimal $(v, 3, 1)$ CPCW code exists for all v except for $v = 6t + 2$ and $t \equiv 2$ or $3 \pmod 4$. Direct constructions with explicit codewords are presented in [21] to show the existence of an optimal (v,4,1) CPCW (OOC) code for any

https://doi.org/10.3390/axioms15010035

positive integer $v \neq 25$. The existence of an optimal $(v, k, 1)$ CPCW code for $k \geq 5$ is still an open problem.

In this paper, we consider $k = 5$ and 6.

(**a**) Optimal (43,5,1) CPCW code

$\mathcal{C}$	$\triangle C$
{0, 1, 3, 7, 19}	{1, 2, 3, 4, 6, 7, 12, 16, 18, 19, 24, 25, 27, 31, 36, 37, 39, 40, 41, 42}
{0, 5, 13, 22, 33}	{5, 8, 9, 10, 11, 13, 15, 17, 20, 21, 22, 23, 26, 28, 30, 32, 33, 34, 35, 38}

Uncovered differences: 0, 14, 29

(**b**) Related optimal partial cyclic 2-(43,5,1) design

```
1000000000000000000000001000000000001000101  1000000000100000000001000000001000000010000
1100000000000000000000000100000000000100010  0100000000010000000000100000000100000001000
0110000000000000000000000010000000000010001  0010000000001000000000010000000010000000100
1011000000000000000000000001000000000001000  0001000000000100000000001000000001000000010
0101100000000000000000000000100000000000100  0000100000000010000000000100000000100000001
0010110000000000000000000000010000000000010  1000010000000001000000000010000000010000000
0001011000000000000000000000001000000000001  0100001000000000100000000001000000001000000
1000101100000000000000000000000100000000000  0010000100000000010000000000100000000100000
0100010110000000000000000000000010000000000  0001000010000000001000000000010000000010000
0010001011000000000000000000000001000000000  0000100001000000000100000000001000000001000
0001000101100000000000000000000000100000000  0000010000100000000010000000000100000000100
0000100010110000000000000000000000010000000  0000001000010000000001000000000010000000010
0000010001011000000000000000000000001000000  0000000100001000000000100000000001000000001
0000001000101100000000000000000000000100000  1000000010000100000000010000000000100000000
0000000100010110000000000000000000000010000  0100000001000010000000001000000000010000000
0000000010001011000000000000000000000001000  0010000000100001000000000100000000001000000
0000000001000101100000000000000000000000100  0001000000010000100000000010000000000100000
0000000000100010110000000000000000000000010  0000100000001000010000000001000000000010000
0000000000010001011000000000000000000000001  0000010000000100001000000000100000000001000
1000000000001000101100000000000000000000000  0000001000000010000100000000010000000000100
0100000000000100010110000000000000000000000  0000000100000001000010000000001000000000010
0010000000000010001011000000000000000000000  0000000010000000100001000000000100000000001
0001000000000001000101100000000000000000000  1000000001000000010000100000000010000000000
0000100000000000100010110000000000000000000  0100000000100000001000010000000001000000000
0000010000000000010001011000000000000000000  0010000000010000000100001000000000100000000
0000001000000000001000101100000000000000000  0001000000001000000010000100000000010000000
0000000100000000000100010110000000000000000  0000100000000100000001000010000000001000000
0000000010000000000010001011000000000000000  0000010000000010000000100001000000000100000
0000000001000000000001000101100000000000000  0000001000000001000000010000100000000010000
0000000000100000000000100010110000000000000  0000000100000000100000001000010000000001000
0000000000010000000000010001011000000000000  0000000010000000010000000100001000000000100
0000000000001000000000001000101100000000000  0000000001000000001000000010000100000000010
0000000000000100000000000100010110000000000  0000000000100000000100000001000010000000001
0000000000000010000000000010001011000000000  1000000000010000000010000000100001000000000
0000000000000001000000000001000101100000000  0100000000001000000001000000010000100000000
0000000000000000100000000000100010110000000  0010000000000100000000100000001000010000000
0000000000000000010000000000010001011000000  0001000000000010000000010000000100001000000
0000000000000000001000000000001000101100000  0000100000000001000000001000000010000100000
0000000000000000000100000000000100010110000  0000010000000000100000000100000001000010000
0000000000000000000010000000000010001011000  0000001000000000010000000010000000100001000
0000000000000000000001000000000001000101100  0000000100000000001000000001000000010000100
0000000000000000000000100000000000100010110  0000000010000000000100000000100000001000010
0000000000000000000000010000000000010001011  0000000001000000000010000000010000000100001
```

Figure 1. The corresponding partial design.

First, we will summarize the known results for optimal CPCW codes or related combinatorial objects for $k = 5$ and 6.

- An optimal $(15p, 5, 1)$ OOC with p a product of primes congruent to 1 modulo 4 and greater than 5 exists according to [18].
- It is shown in [14] that an optimal $(4p, 5, 1)$ OOC exists for prime $p \equiv 1 \pmod{10}$, and that there is an optimal $(4up, 5, 1)$ OOC for $u = 2, 3$ and prime $p \equiv 11 \pmod{20}$.
- A proof of the existence of a $(3^s 5v, 5, 1)$ OOC if v is a product of primes congruent to 1 modulo 4 and s is a non-negative integer is given in [16,17].
- There are also several direct constructions for optimal $(gv, 5, 1)$ OOCs where $60 \leq g \leq 180$, $g \equiv 0 \pmod{20}$, and v is a product of primes greater than 5.

https://doi.org/10.3390/axioms15010035

- A class of optimal $(gv, 6, 1)$ optical orthogonal codes with v a product of primes congruent to 7 modulo 12 and greater than 7 and $g = 15, 20, 105, 140$ is obtained in [19].
- Some combinatorial constructions for optimal $(v, k, 1)$ OOCs using g-regular cyclic packings are derived in [4,20].

Some existence results about CPCW codes with $k = 5$ and 6 follow from results about cyclic difference families and combinatorial designs.

- It is shown in [23] that a $(p, 5, 1)$ difference family exists for $p \equiv 1 \pmod{20}$ for prime p.
- According to [26], a $(20t + 1, 5, 1)$ difference family exists for $1 \leq t \leq 50$ except possibly for $t = 16, 25, 31, 34, 40, 45$.
- The existence of a cyclic $(pq, 5, 1)$ difference family whenever p and q are primes congruent to $11 \pmod{20}$ is proved in [6].
- Existence of a $(q, 6, 1)$ cyclic difference family for any prime power $q \equiv 1 \pmod{30}$ with the exception of $q = 61$ is shown in [22].
- It was proved in [29] that a cyclic $(5p, 5, 1)$ combinatorial design exists for all $p \equiv 1 \pmod{4}$ and $p \neq 5$.

Nonexistence results for optimal $(v, 5, 1)$ OOCs with $v \equiv 22 \pmod{40}$ and for an optimal $(62, 6, 1)$ OOC are presented in [7].

Classification results about $(v, k, 1)$ CPCW codes for $k = 5$ and 6 or about related combinatorial objects can be found in [25,27,28,30,31]. The results obtained in these works show that, when v grows, the number of nonequivalent codes becomes extremely large. This makes the classifications for the next larger lengths practically unusable.

In this work, we consider $k = 5$ and 6 and the first values of v for which existence or nonexistence results are not known and try to find an example of an optimal $(v, k, 1)$ CPCW code for these parameters. We conduct this for $k = 5$ and $v \leq 181$ and $k = 6$ and $v \leq 151$. We cannot find an optimal code for 9 of the considered parameter sets. We notice that two of these gaps are for $v = k(k-1)t + 2$. This motivates us to consider the properties of such codes, and we derive necessary conditions for their existence and prove that an optimal $(92, 6, 1)$ CPCW code does not exist.

The paper is organized as follows: Section 2 demonstrates the basis of our approach. Section 3 presents both the computer-aided and analytical results that we obtain. Section 4 contains final remarks and open problems.

2. Methods

The explicit examples of new optimal $(v, 5, 1)$ and $(v, 6, 1)$ CPCW codes are obtained by the algorithm for classification of such codes, which we have used and described in [31]. It implies the construction of an array L with all possible codewords, namely with k-subsets of $\mathbb{Z}_v$ for which the auto-correlation property holds. We then construct codes by choosing their codewords from L in all possible ways. For that purpose, backtrack search on the elements of L is applied, and some partial solutions are filtered away if there exists an automorphism of $\mathbb{Z}_v$ that maps the partial solution to a partial solution that has already been constructed.

Our aim in the present work is not to obtain all the codes with these parameters but to find one such code. That is why we let the computation stop after having constructed one code, or after having worked for several days on a personal computer. The fact that we have not succeeded to construct a code with definite parameters does not mean that such a code does not exist.

The necessary conditions for the existence of optimal $(k(k-1)t + 2, k, 1)$ CPCW codes are derived using a method that is very popular in Design Theory, namely the counting of points and pairs of points in two different ways. The nonexistence of an optimal $(92, 6, 1)$

https://doi.org/10.3390/axioms15010035

CPCW code is proved by using these necessary conditions and applying counting of the pairs of points in one more way.

3. Results

3.1. Examples of Optimal $(v, 5, 1)$ *and* $(v, 6, 1)$ *CPCW Codes*

We present in Tables 1 and 2 all the previously known existence and nonexistence results regarding optimal $(v, 5, 1)$ and $(v, 6, 1)$ CPCW codes with $v \leq 181$ and 151, respectively. Normal font is used for the v with theoretical results from [6–24,26,29] and italics for the results from the computer classifications in [25,27,28,30,31]. A normal or an italic v is struck through if the corresponding result (theoretic or computer-aided) shows nonexistence of optimal $(v, 5, 1)$ or $(v, 6, 1)$ CPCW codes. A question mark means that nothing is known about the existence of optimal codes with this length.

Table 1. Optimal $(v, 5, 1)$ CPCW codes before the present study.

41	~~*42*~~	*43*	~~44~~	~~45~~	*46–60*	61	~~62~~	*63–64*	65	*66–80*
81	*82–87*	88	89	?	101	~~102~~	?	105	?	121
?	124	125	?	132	?	135	?	141	~~142~~	?
145	?	161	?	164	165	?	181	~~182~~	?	185

Normal font for theoretical results, italic for computer-aided, strikethrough for nonexistence and symbol ? when nothing is known.

Table 2. Optimal $(v, 6, 1)$ CPCW codes before the present study.

~~*61*~~	~~62~~	*63*	~~*64*~~	~~*65*~~	*66–91*	~~*92*~~	*93–105*	?	121	?	151

Normal font for theoretical results, italic for computer-aided, strikethrough for nonexistence and symbol ? when nothing is known.

Tables 3 and 4 are organized in a similar way to Tables 1 and 2, but in them the existence results from the present paper are implemented too, and bold font is used for them. The question marks mean that we could not find optimal codes for these values of v and the question of the existence of such codes remains open. In particular, we have not found examples of optimal $(v, 5, 1)$ CPCW codes for $v = 143, 144, 146, 162$, and 167, and of optimal $(v, 6, 1)$ CPCW codes for $v = 122, 123, 124$, and 126. These are $(k(k-1)t + c, k, 1)$ CPCW codes with relatively small c. The latter is also small for the optimal codes for which there are no theoretical nonexistence results, but they have been proved not to exist with the help of a computer [31], namely an optimal $(42, 5, 1)$ CPCW code and optimal $(v, 6, 1)$ CPCW codes for $v = 61, 64, 65$, and 92. This motivated our study of the properties of optimal $(k(k-1)t + 2, k, 1)$ CPCW codes.

Table 3. New optimal $(v, 5, 1)$ CPCW codes.

41	~~*42*~~	*42–43*	~~44~~	~~45~~	*46–60*	61	~~62~~	*63–64*	65	*66–80*
81	*82–87*	88	89	**90–100**	101	~~102~~	**103–104**	105	**106–120**	121
122–123	124	125	**126–131**	132	**133–134**	135	**136–140**	141	~~142~~	?
145	?	**147–160**	161	?	164	165	**166**	?	**168–180**	181

Bold font for results in the present paper, normal font for theoretical results, italic for computer-aided, strikethrough for nonexistence and symbol ? when nothing is known.

https://doi.org/10.3390/axioms15010035

Table 4. New optimal $(v, 6, 1)$ CPCW codes.

~~61~~	~~62~~	*63*	~~64~~	~~65~~	*66–91*	~~92~~	*93–105*	**106–120**	121	?	**125**	?	**127–150**	151

Bold font for results in the present paper, normal font for theoretical results, italic for computer-aided, strikethrough for nonexistence and symbol ? when nothing is known.

Tables A1 and A2 in Appendix A contain all the examples of new optimal $(v, 5, 1)$ and $(v, 6, 1)$ CPCW codes. Each codeword contains the element $0 \in \mathbb{Z}_v$, and therefore this element is not presented.

3.2. Properties of Optimal $(k(k-1)t+2, k, 1)$ CPCW Codes

The optimal $(v, k, 1)$ CPCW codes of length $k(k-1)t+1$ correspond to 2-$(k(k-1)t+1, k, 1)$ designs. They are perfect because their codewords cover all $v-1$ differences. Optimal CPCW codes of length $k(k-1)t+2$, however, have remarkable combinatorial properties too because they do not cover only one difference. We derive here some necessary conditions for the existence of such codes.

Lemma 1. *The element $\frac{v}{2} \in \mathbb{Z}_v$ cannot be covered by the differences of the codewords of a $(v, k, 1)$ CPCW code of even length. For even v, the element $\frac{v}{2} \in \mathbb{Z}_v$ can be obtained as the difference $a-b$ of $\frac{v}{2}$ different pairs $\{a, b\}$.*

Proof. Let C be a codeword of a $(v, k, 1)$ CPCW code $\mathcal{C}$ of even length. Let $a, b \in C$. Then, $a-b$ and $b-a$ must be two different differences from $\triangle C$. Suppose $a-b=\frac{v}{2}$, and then $b-a=v-\frac{v}{2}=\frac{v}{2}$, and $\frac{v}{2}$ appears twice in $\triangle C$, but this is impossible for a $(v, k, 1)$ CPCW code. Since $a-b=b-a=\frac{v}{2}$, the element $\frac{v}{2} \in \mathbb{Z}_v$ can be obtained as the difference $a-b$ of the $\frac{v}{2}$ different pairs $\{a, a+\frac{v}{2}\}$, $a \leq \frac{v}{2}$. □

Lemma 2. *The codewords of an optimal $(k(k-1)t+2, k, 1)$ CPCW code leave uncovered only the difference $\frac{v}{2}$.*

Proof. Since $k(k-1)t+2$ is even, by Lemma 1, the possible differences are $v-2 = k(k-1)t$. The size of such a code is

$$\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor = \left\lfloor \frac{k(k-1)t+1}{k(k-1)} \right\rfloor = t,$$

and each codeword covers $k(k-1)$ differences. Then, all the codewords cover $k(k-1)t = v-2$ differences; that is, only one difference remains uncovered. □

An optimal $(k(k-1)t+2, k, 1)$ CPCW code corresponds to an optimal partial cyclic 2-$(k(k-1)t+2, k, 1)$ design. The translates of each codeword correspond to v blocks of this partial design and to a circulant submatrix of the incidence matrix of the partial design. We next consider some properties of this partial design.

Lemma 3. *The $\frac{v}{2}$ pairs of points $\{a, a+\frac{v}{2}\}$ are not contained in the blocks of an optimal partial cyclic 2-$(k(k-1)t+2, k, 1)$ design corresponding to an optimal $(k(k-1)t+2, k, 1)$ CPCW code. Each of the remaining $\frac{v(v-2)}{2}$ pairs of points is in exactly one block of this partial design.*

Proof. The $\frac{v}{2}$ pairs of points that are not contained in the blocks of the design correspond to the $\frac{v}{2}$ different pairs $\{a, a+\frac{v}{2}\}$ from Lemma 1. □

Lemma 4. *Denote the rows/columns of a circulant M of an even order v by the numbers $0, 1, 2, \ldots v-1$. Let φ be a permutation that rearranges the rows and the columns of M in*

https://doi.org/10.3390/axioms15010035

such a way that they follow each other as $0, 2, 4 \ldots v-2, 1, 3, 5, \ldots v-1$. *Then, the resulting matrix* φM *is composed of* 4 *circulants* A, B, C, *and* D *of order* $\frac{v}{2}$.

$$\varphi M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Denote by u_A, u_B, u_C, *and* u_D *the number of ones in a row/column of the matrices* A, B, C, *and* D, *respectively. Then,* $u_A = u_D$ *and* $u_B = u_C$.

Proof. Cutting off the even rows and even columns of M leads to a matrix A of dimension $\frac{v}{2} \times \frac{v}{2}$. Let $m_{i,j}$ be the element in row i and column j of M and $a_{i,j}$ be the element in row i and column j of A. Then, $a_{i,j} = m_{2i,2j}$.

We want to show that A is a circulant matrix. Addition of the indices of A is modulo $\frac{v}{2}$, and of M modulo v. Since $2i \pmod{v} = 2(i \pmod{\frac{v}{2}})$, the addition of the even indices of M can be considered modulo $\frac{v}{2}$ too. Then, $a_{i+1,j+1} = m_{2i+2,2j+2}$. M is a circulant, and therefore $m_{2i+2,2j+2} = m_{2i,2j} = a_{i,j}$. It follows that $a_{i+1,j+1} = a_{i,j}$; that is, A is a circulant matrix.

Similarly, the circulants B, C, and D are obtained by cutting off the even rows and odd columns, the odd rows and even columns, and the odd rows and odd columns, respectively.

The number of ones in each row and column of φM is the same, and therefore $u_A = u_D$ and $u_B = u_C$. □

Example 1. *We illustrate the action of* φ *on two arbitrary circulants of even orders* 10 *and* 8.

	0 1 2 3 4 5 6 7 8 9
0	0 1 0 0 0 1 0 1 0 0
1	0 0 1 0 0 0 1 0 1 0
2	0 0 0 1 0 0 0 1 0 1
3	1 0 0 0 1 0 0 0 1 0
4	0 1 0 0 0 1 0 0 0 1
5	1 0 1 0 0 0 1 0 0 0
6	0 1 0 1 0 0 0 1 0 0
7	0 0 1 0 1 0 0 0 1 0
8	0 0 0 1 0 1 0 0 0 1
9	1 0 0 0 1 0 1 0 0 0

	0 1 2 3 4 5 6 7 8 9
0	0 1 0 0 0 1 0 1 0 0
2	0 0 0 1 0 0 0 1 0 1
4	0 1 0 0 0 1 0 0 0 1
6	0 1 0 1 0 0 0 1 0 0
8	0 0 0 1 0 1 0 0 0 1
1	0 0 1 0 0 0 1 0 1 0
3	1 0 0 0 1 0 0 0 1 0
5	1 0 1 0 0 0 1 0 0 0
7	0 0 1 0 1 0 0 0 1 0
9	1 0 0 0 1 0 1 0 0 0

	0 2 4 6 8	1 3 5 7 9
0	0 0 0 0 0	1 0 1 1 0
2	0 0 0 0 0	0 1 0 1 1
4	0 0 0 0 0	1 0 1 0 1
6	0 0 0 0 0	1 1 0 1 0
8	0 0 0 0 0	0 1 1 0 1
1	0 1 0 1 1	0 0 0 0 0
3	1 0 1 0 1	0 0 0 0 0
5	1 1 0 1 0	0 0 0 0 0
7	0 1 1 0 1	0 0 0 0 0
9	1 0 1 1 0	0 0 0 0 0

	0 1 2 3 4 5 6 7
0	0 1 0 1 0 0 1 0
1	0 0 1 0 1 0 0 1
2	1 0 0 1 0 1 0 0
3	0 1 0 0 1 0 1 0
4	0 0 1 0 0 1 0 1
5	1 0 0 1 0 0 1 0
6	0 1 0 0 1 0 0 1
7	1 0 1 0 0 1 0 0

	0 1 2 3 4 5 6 7
0	0 1 0 1 0 0 1 0
2	1 0 0 1 0 1 0 0
4	0 0 1 0 0 1 0 1
6	0 1 0 0 1 0 0 1
1	0 0 1 0 1 0 0 1
3	0 1 0 0 1 0 1 0
5	1 0 0 1 0 0 1 0
7	1 0 1 0 0 1 0 0

	0 2 4 6	1 3 5 7
0	0 0 0 1	1 1 0 0
2	1 0 0 0	0 1 1 0
4	0 1 0 0	0 0 1 1
6	0 0 1 0	1 0 0 1
1	0 1 1 0	0 0 0 1
3	0 0 1 1	1 0 0 0
5	1 0 0 1	0 1 0 0
7	1 1 0 0	0 0 1 0

Lemma 5. *Let* M *be the incidence matrix of an optimal partial cyclic* 2-$(k(k-1)t+2, k, 1)$ *design* D *corresponding to an optimal* $(k(k-1)t+2, k, 1)$ *CPCW code. If the permutation* φ *from Lemma 4 is applied to the rows of* M *and to the columns of each of its* t *circulant submatrices, a matrix with* $4t$ *circulant submatrices of order* $\frac{v}{2}$ *is obtained. If* $v \equiv 2 \pmod{4}$, *the columns of each of the two rows of submatrices cover all possible* $\frac{v(v-2)}{8}$ *pairs of points, and the missing* $\frac{v}{2}$ *pairs of points in the partial design have one point from the first and one from the second row of*

https://doi.org/10.3390/axioms15010035

submatrices. If $v \equiv 0 \pmod 4$, *there are* $\frac{v}{4}$ *pairs of points that are not covered by the columns of each row of submatrices, and all possible* $\frac{v^2}{4}$ *pairs of points having one point from the first and one from the second row of submatrices are covered.*

Proof. By Lemma 4, the permutation φ transforms each of the t circulants of order v to 4 circulants of order $\frac{v}{2}$. That is why the incidence matrix φM of the partial design has $4t$ circulant submatrices of order $\frac{v}{2}$. If $v \equiv 2 \pmod 4$, then $\frac{v}{2}$ is odd. That is why, if a is odd, $a + \frac{v}{2}$ is even and vice versa. Since the first row of submatrices of φM contains the even rows of M and the second the odd rows, the missing pairs of points $\{a, a + \frac{v}{2}\}$ (Lemma 3) have one point from the first row of submatrices and one from the second. If $v \equiv 0 \pmod 4$, then $\frac{v}{2}$ is even, a and $a + \frac{v}{2}$ are both even or both odd, and the missing pairs of points consist of two points from one and the same row of submatrices. □

With respect to the number of ones in the four submatrices, φ can transform a circulant of order v to $\left\lfloor \frac{k}{2} \right\rfloor + 1$ types of matrices $A_0, A_1, \ldots A_{\left\lfloor \frac{k}{2} \right\rfloor}$ such that A_i has two circulant submatrices with i ones in each row/column and two with $k - i$ ones in each row/column.

Example 2. *Types of matrices for* $k = 5$ *and* 6

For $k = 5$, *the types of matrices are*

A_0	A_1	A_2
0 5 *5 0*	*1 4* *4 1*	*2 3* *3 2*

For $k = 6$, *the types of matrices are*

A_0	A_1	A_2	A_3
0 6 *6 0*	*1 5* *5 1*	*2 4* *4 2*	*3 3* *3 3*

Theorem 1. *For an optimal* $(v, k, 1)$ *CPCW code with* $v = k(k-1)t + 2$ *and* $v \equiv 2 \pmod 4$, *the following equations hold:*

$$\sum_{i=0}^{\frac{v}{2}} a_i = \frac{v-2}{k(k-1)} \tag{3}$$

$$\sum_{i=0}^{\frac{v}{2}} \left(\frac{i(i-1)}{2} + \frac{(k-i)(k-i-1)}{2} \right) a_i = \frac{v-2}{4} \tag{4}$$

$$\sum_{i=1}^{\frac{v}{2}} i(k-i) a_i = \frac{v-2}{4} \tag{5}$$

Proof. We obtain the equations by counting in different ways the pairs of points in φM. Denote by a_i the number of $v \times v$ matrices of type A_i that are contained in φM. Their number is $t = \frac{v-2}{k(k-1)}$, and this is Equation (3). Equation (4) counts the pairs of points from one and the same row of submatrices. By Lemma 5, their number is $\frac{v(v-2)}{8}$. On the other hand, each $\frac{v}{2} \times \frac{v}{2}$ submatrix of a matrix of type A_i covers $\frac{v}{2}\left(\frac{i(i-1)}{2} + \frac{(k-i)(k-i-1)}{2} \right)$ pairs of points. Equation (5) counts the pairs in which the two points are from different rows of submatrices. By Lemma 5, all but the missing $\frac{v}{2}$ pairs are covered; that is, all such pairs are $\frac{v^2}{4} - \frac{v}{2} = \frac{v(v-2)}{4}$. On the other hand, each $v \times v$ submatrix of type A_i covers $i(k-i)v$ such pairs of points. □

https://doi.org/10.3390/axioms15010035

Theorem 2. *For an optimal* $(v, k, 1)$ *CPCW code with* $v = k(k-1)t + 2$ *and* $v \equiv 0 \pmod 4$, *the following equations hold:*

$$\sum_{i=0}^{\frac{v}{2}} a_i = \frac{v-2}{k(k-1)} \tag{6}$$

$$\sum_{i=0}^{\frac{v}{2}} \left(\frac{i(i-1)}{2} + \frac{(k-i)(k-i-1)}{2} \right) a_i = \frac{v-4}{4} \tag{7}$$

$$\sum_{i=1}^{\frac{v}{2}} i(k-i)a_i = \frac{v}{4} \tag{8}$$

Proof. The proof is similar to that of Theorem 1, but, by Lemma 5, the pairs of points from one and the same row of submatrices are $\frac{v(v-2)}{8} - \frac{v}{4} = \frac{v(v-4)}{8}$. All the pairs in which the two points are from different rows of submatrices are covered. That is why their number is $\frac{v^2}{4}$. □

Corollary 1. *An optimal* $(20t + 2, 5, 1)$ *CPCW code can only exist if* t *is even.*

Proof. In this case, $v \equiv 2 \pmod 4$, and Equation (5) gives

$$4a_1 + 6a_2 = \frac{v-2}{4}.$$

That is why $v - 2$ should be divisible by 8. □

Corollary 1 is not a new result. It is part of the nonexistence results presented in [7], Theorem 4.6. The next example shows the application of Theorem 1 on an optimal $(20t + 2, 5, 1)$ CPCW code with even t.

Example 3. *For an optimal* $(82, 5, 1)$ *CPCW code by Theorem 1:*

$$a_0 + a_1 + a_2 + a_3 = 4 \tag{9}$$

$$5a_0 + 3a_1 + 2a_2 = 10 \tag{10}$$

$$2a_1 + 3a_2 = 10 \tag{11}$$

There exists a unique integer solution: $a_0 = 0, a_1 = 2, a_2 = 2$, *and the optimal* $(82, 5, 1)$ *CPCW codes comply with it.*

3.3. Nonexistence of an Optimal $(92, 6, 1)$ *CPCW Code*

Multiple nonexistence results on optimal $(v, k, 1)$ CPCW codes are obtained in [7]. They include the nonexistence of an optimal $(62, 6, 1)$ code. We do not know other theoretical nonexistence results for optimal $(30t + 2, 6, 1)$ CPCW codes. Our computer-aided classification in [31] shows that an optimal $(92, 6, 1)$ CPCW code does not exist. Using Theorem 2, we shall now prove this without a computer.

Proposition 1. *An optimal* $(92, 6, 1)$ *CPCW code does not exist.*

Proof. By Theorem 2:

$$a_0 + a_1 + a_2 + a_3 = 3 \tag{12}$$

$$15a_0 + 10a_1 + 7a_2 + 6a_3 = 22 \tag{13}$$

$$5a_1 + 8a_2 + 9a_3 = 23 \tag{14}$$

https://doi.org/10.3390/axioms15010035

There exists a unique integer solution:

$$a_0 = 0, a_1 = 1, a_2 = 0, a_3 = 2 \tag{15}$$

It follows that the number of ones in φM is distributed as

$$\begin{array}{ccc} 5\,1 & 3\,3 & 3\,3 \\ 1\,5 & 3\,3 & 3\,3 \end{array}$$

We can see from (15) that the submatrices of dimension 46×46 have $1, 3$, or 5 ones in each row/column. Since 46 is even and $v/4 = 23$ is odd, we can use the same ideology as in Lemma 5 and Theorem 1 on the variable-length code corresponding to the first 46 rows of φM; that is, we apply to the first 46 rows of φM a permutation φ' such that after its application these rows follow each other as $0, 2, 4 \ldots 44, 1, 3, 5, \ldots 45$, and we apply the same permutation to the columns of the submatrices of dimension 46.

A 46×46 circulant with 1, 3, or 5 ones in each row/column can be transformed by φ' to one, two, or three types of matrices, respectively. We denote them $A_{1,0}$,$A_{3,0}$, $A_{3,1}$, $A_{5,0}$, $A_{5,1}$, and $A_{5,2}$. The matrix $A_{i,j}$ is of dimension 46×46 and has four submatrices of dimension 23×23, two of them with j and two with $i - j$ ones in each row/column.

$$\begin{array}{cccccc} A_{1,0} & A_{3,0} & A_{3,1} & A_{5,0} & A_{5,1} & A_{5,2} \\ 0\,1 & 0\,3 & 1\,2 & 0\,5 & 1\,4 & 2\,3 \\ 1\,0 & 3\,0 & 2\,1 & 5\,0 & 4\,1 & 3\,2 \end{array}$$

Denote by $a_{i,j}$ the number of 23×23 matrices of type $A_{i,j}$ that are contained in the first 23 rows of $\varphi' \varphi M$. Since 23 is odd, we can apply Theorem 1 and write an analogue of Equation (5) for $a_{i,j}$; thus, we obtain

$$\sum_{(i,j) \in S} j(i-j) a_{i,j} = \frac{46-2}{4} = 11 \tag{16}$$

where $S = \{(1,0), (3,0), (3,1), (5,0), (5,1), (5,2)\}$. It follows that

$$2a_{3,1} + 4a_{5,1} + 6a_{5,2} = 11. \tag{17}$$

The same result can be obtained by counting the pairs of points such that one is from the first 23 rows of $\varphi' \varphi M$ and the other from the second 23 rows. The missing 23 pairs of points are among them, and therefore

$$46(2a_{3,1} + 4a_{5,1} + 6a_{5,2}) = 23 \cdot 23 - 23 = 23 \cdot 22 = 46 \cdot 11.$$

This results in Equation (17) again. Equation (17), however, has no integer solutions because its left side is even and the right one is odd. That is why an optimal $(92, 6, 1)$ CPCW code cannot exist. □

4. Discussion

The presented examples of optimal $(v, 5, 1)$ and $(v, 6, 1)$ CPCW codes might be useful in relevant applications, as well as in future research on the topic. The results for small parameters show that nonexistence of some optimal $(k(k-1)t + c, k, 1)$ CPCW codes with small c can be expected. The solutions of the equations from Theorems 1 and 2 might be useful in further theoretical or computer-aided research on optimal $(k(k-1)t + 2, k, 1)$ CPCW codes whose existence remains undecided.

https://doi.org/10.3390/axioms15010035

Author Contributions: Conceptualization, S.T. and T.B.; methodology, S.T. and T.B.; software, S.T.; validation, S.T. and T.B.; investigation, S.T. and T.B.; data curation, T.B.; writing—original draft preparation, S.T. and T.B.; writing—review and editing, S.T. and T.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research of both authors was partially supported by the Centre of Excellence in Informatics and ICT under Grant No. BG16RFPR002-1.014-0018-C01, financed by the Research, Innovation and Digitalization for Smart Transformation Programme 2021–2027 and co-financed by the European Union.

Data Availability Statement: All the new results are included in the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CPCW Code	Binary Cyclically Permutable Constant-Weight Code
OOC	Optical Orthogonal Code
CDF	Cyclic Difference Family

Appendix A

Table A1. Optimal (v,5,1) CPCW codes.

Length	Codewords				
90	1 3 7 18	5 25 33 52	13 39 53 69	9 31 55 67	
91	1 3 7 12	8 33 49 73	14 35 52 71	10 23 54 69	
92	1 3 7 12	15 35 54 76	13 30 55 78	8 26 36 60	
93	1 3 7 12	8 27 40 73	10 26 48 78	14 31 49 70	
94	1 3 7 12	8 34 50 77	14 33 53 71	10 31 46 59	
95	1 3 7 15	9 32 53 84	13 41 59 78	5 29 39 55	
96	1 3 7 12	10 36 63 76	8 25 57 75	14 37 52 68	
97	1 3 7 12	10 30 53 70	13 32 47 68	8 24 46 72	
98	1 3 7 12	16 38 59 78	8 26 61 74	10 27 41 56	
99	1 3 7 12	10 34 51 72	14 29 57 83	8 33 55 68	
100	1 3 7 12	14 38 66 81	13 36 54 71	8 30 40 61	
103	1 3 15 96	9 49 65 92	4 37 50 79	6 41 58 77	5 30 64 85
104	1 3 7 90	9 27 63 82	10 35 47 81	5 45 65 93	8 38 51 80
106	1 3 8 43	11 48 60 79	13 34 67 89	9 45 59 74	4 20 82 100
107	1 3 7 34	9 23 51 71	10 32 50 96	8 24 37 63	5 35 54 95
108	1 3 7 39	9 26 56 93	10 31 53 95	8 19 33 68	5 34 50 62
109	1 3 7 31	8 22 33 65	9 35 48 58	5 50 68 97	15 53 69 90
110	1 3 7 27	8 42 72 101	12 25 40 73	5 36 52 96	10 21 53 75
111	1 3 7 21	12 41 65 84	9 44 78 89	10 47 62 98	8 25 63 79
112	1 3 7 16	10 45 62 88	8 19 49 74	12 44 73 91	5 28 42 64

https://doi.org/10.3390/axioms15010035

Table A1. *Cont.*

Length	Codewords					
113	1 3 7 12	13 34 58 84	10 30 47 70	15 31 59 77	8 27 49 88	
114	1 3 7 15	9 41 59 86	10 21 52 81	17 51 75 95	5 40 66 89	
115	1 3 7 25	8 34 45 102	5 28 84 101	9 41 61 71	12 51 67 100	
116	1 3 7 17	8 30 90 101	5 36 54 75	12 59 78 91	9 29 64 92	
117	1 3 7 18	5 38 66 74	10 30 70 83	16 42 71 92	9 31 68 103	
118	1 3 7 24	9 27 63 98	11 33 61 77	12 31 79 93	5 15 45 58	
119	1 3 7 16	10 30 41 70	5 43 71 105	8 26 72 95	12 33 77 94	
120	1 3 7 24	13 39 72 91	9 46 66 102	10 41 53 85	8 58 73 98	
122	1 3 21 33	10 34 93 106	8 36 76 111	6 51 58 113	4 42 85 99	5 49 74 105
123	1 3 22 53	8 67 93 103	4 17 33 65	9 55 98 109	5 12 49 88	6 24 51 66
126	1 3 25 122	6 23 85 100	8 38 75 91	11 44 72 92	12 68 86 99	9 66 80 116
127	1 3 21 54	4 12 84 89	9 25 57 91	11 41 63 112	6 29 68 87	7 17 31 44
128	1 3 82 119	4 99 105 110	7 21 69 97	13 39 55 96	8 51 75 111	15 35 65 109
129	1 3 15 105	13 36 82 100	8 99 109 120	6 32 63 85	4 37 71 78	5 54 73 89
130	1 3 8 75	6 17 51 105	12 35 64 83	9 27 37 117	4 30 73 114	15 39 77 109
131	1 3 9 55	4 64 105 115	11 33 81 99	5 12 36 108	15 49 68 106	13 58 75 102
133	1 3 8 113	9 27 72 86	12 36 62 96	10 51 68 103	6 39 85 117	4 29 42 118
134	1 3 7 37	12 55 68 94	9 47 92 111	22 57 81 106	5 15 46 63	8 29 62 73
136	1 3 7 23	8 73 82 100	14 57 89 108	11 60 91 106	12 38 78 115	5 34 69 86
137	1 3 7 16	12 36 55 84	11 33 50 77	5 42 63 117	10 40 86 109	8 49 67 81
138	1 3 7 27	10 22 66 127	9 48 62 107	16 84 103 120	8 49 81 123	5 30 43 80
139	1 3 7 28	8 24 56 85	10 33 53 102	12 31 46 76	13 55 73 113	14 65 82 117
140	1 3 7 34	9 26 78 127	8 29 43 66	10 55 83 102	5 64 89 129	12 36 80 122
147	1 3 9 88 12 40 76 126	5 48 72 113	4 19 100 122	17 37 91 129	7 23 49 101	13 27 58 90
148	1 3 44 58 9 19 37 79	6 108 119 141	4 27 81 86	15 45 83 132	8 34 84 131	12 32 85 124
149	1 3 18 127 13 27 56 80	4 12 61 72	10 26 58 105	7 52 94 115	5 33 64 83	9 39 74 112
150	1 3 36 110 4 48 64 132	5 39 58 138	9 81 104 130	6 56 63 71	11 32 123 137	10 52 83 113
151	1 3 10 56 11 25 92 124	4 12 40 73	15 39 87 104	16 76 110 130	5 88 107 138	22 45 80 122
152	1 3 10 95 14 29 84 134	11 33 110 133	8 54 91 125	6 31 72 93	5 101 114 140	4 28 44 107
153	1 3 11 32 4 17 40 67	14 44 70 118	7 19 62 84	5 33 94 133	9 24 66 82	6 47 81 99

https://doi.org/10.3390/axioms15010035

Table A1. *Cont.*

Length	Codewords					
154	1 3 10 100 4 16 30 82	11 50 71 129	8 49 89 135	6 35 67 126	5 20 53 137	18 56 80 103
155	1 3 7 62 22 47 82 127	12 36 84 124	13 39 57 91	8 27 38 114	17 46 102 135	5 21 63 86
156	1 3 7 87 17 41 94 130	5 15 35 123	9 55 73 105	8 29 57 71	16 39 61 98	19 66 100 131
157	1 3 7 15 19 42 75 99	9 27 63 135	16 48 83 112	17 51 98 119	11 52 118 131	10 30 70 114
158	1 3 7 33 11 67 80 129	9 27 63 139	8 43 58 141	10 41 57 94	21 45 87 135	12 77 97 136
159	1 3 7 33 10 53 72 92	14 42 98 144	5 27 71 95	11 59 96 119	16 54 89 134	13 49 107 125
160	1 3 7 23 5 51 101 141	13 39 91 139	8 41 79 107	9 27 63 74	12 29 43 87	10 25 93 128
166	1 5 39 140 17 79 109 142	3 15 88 117 6 42 112 152	7 35 107 150	11 32 116 129	9 19 77 95	2 46 113 121
168	1 3 16 125 6 18 42 72	4 38 117 149 7 21 77 140	11 37 104 129	10 41 81 110	5 52 85 146	8 53 73 159
169	1 3 17 126 11 24 122 143	6 18 80 102 4 69 79 118	7 32 41 70	5 92 115 134	8 76 91 121	20 53 81 117
170	1 3 16 116 18 44 68 151	7 21 112 132 4 32 131 140	5 27 80 164	12 47 72 141	10 61 92 128	8 74 97 114
171	1 3 9 60 20 44 99 130	5 15 45 134 18 53 124 143	16 48 121 144	12 80 113 149	13 39 117 146	7 21 84 95
172	1 3 10 130 22 56 82 119	11 31 114 137 4 96 108 144	6 57 151 159	15 33 62 100	5 59 84 133	14 30 91 131
173	1 3 10 77 18 65 100 122	4 12 40 135 25 79 110 143	5 32 144 157	19 60 105 149	6 23 62 121	11 37 83 103
174	1 3 7 127 8 27 70 99	5 15 35 113 14 53 71 93	13 36 82 150	11 56 84 133	12 44 86 153	9 34 119 157
175	1 3 7 94 11 33 75 140	9 27 63 146 5 85 128 152	8 61 77 134	10 96 113 127	15 34 55 131	12 25 51 155
176	1 3 8 34 12 28 137 156	9 27 72 130 10 54 75 161	14 94 129 153	11 49 71 147	6 56 97 140	4 93 106 123
177	1 3 9 83 7 21 54 65	5 15 45 61 23 85 110 134	4 26 104 164	12 50 126 157	18 37 106 142	27 68 120 149
178	1 3 7 133 10 72 107 157	9 27 63 129 5 16 103 150	14 70 92 153	12 38 148 161	8 90 113 154	15 34 74 94
179	1 3 7 22 24 67 104 129	10 30 41 70 12 57 108 143	13 39 91 107	17 49 76 141	14 42 98 132	5 23 69 102
180	1 3 7 146 9 68 106 162	11 33 77 166 8 32 107 128	19 42 88 137	13 39 67 117	12 70 127 163	15 55 116 164

https://doi.org/10.3390/axioms15010035

Table A2. Optimal (v,6,1) CPCW codes.

Length	Codewords			
106	1 3 7 15 36	5 45 56 65 84	10 26 44 57 74	
107	1 3 7 12 89	8 34 47 63 83	10 27 41 69 84	
108	1 3 7 12 37	8 29 51 69 93	10 45 58 77 91	
109	1 3 7 12 39	8 28 41 58 83	10 24 53 72 88	
110	1 3 7 12 33	8 36 54 76 95	10 27 47 71 85	
111	1 3 7 12 29	8 24 56 66 96	13 33 47 74 93	
112	1 3 7 12 28	8 31 57 77 90	10 47 64 83 98	
113	1 3 7 12 25	8 27 43 60 81	10 36 51 65 93	
114	1 3 7 12 25	10 30 44 71 86	8 31 48 67 93	
115	1 3 7 12 25	8 37 54 81 95	10 26 45 77 92	
116	1 3 7 12 26	8 43 60 70 100	13 28 49 78 96	
117	1 3 7 12 22	13 33 50 74 92	8 31 47 77 91	
118	1 3 7 12 22	13 39 57 77 91	8 24 53 70 95	
119	1 3 7 12 25	8 28 43 62 89	10 42 59 82 98	
120	1 3 7 12 22	8 24 51 74 92	13 33 47 78 95	
125	1 3 19 31 54	5 47 64 93 104	7 41 50 77 110	4 67 80 105 119
127	1 3 8 51 113	6 38 61 96 108	4 20 33 60 101	10 34 52 88 116
128	1 3 10 30 53	6 21 45 87 100	4 18 35 40 72	8 33 59 71 117
129	1 3 9 25 97	5 15 60 80 98	12 52 73 102 115	4 23 71 82 99
130	1 3 7 15 107	9 41 57 75 119	5 33 50 72 93	10 35 71 84 111
131	1 3 23 36 105	6 65 73 97 116	9 37 54 79 93	4 11 16 57 87
132	1 3 10 26 87	5 57 74 95 108	11 33 73 100 112	6 14 50 78 97
133	1 3 7 25 95	5 48 78 105 125	9 26 49 68 80	11 46 61 75 112
134	1 3 7 92 107	8 48 66 101 113	9 46 63 82 120	5 25 84 95 108
135	1 3 7 38 61	8 24 34 56 107	5 17 30 50 93	9 27 66 80 95
136	1 3 7 31 47	8 49 74 88 124	10 52 65 103 125	5 64 83 109 118
137	1 3 7 20 56	8 46 58 83 122	9 44 72 104 115	10 26 78 96 123
138	1 3 7 15 48	9 43 64 96 116	5 24 62 80 108	10 23 49 60 121
139	1 3 7 16 57	11 42 60 74 111	10 48 68 103 115	5 22 66 99 118
140	1 3 7 15 59	11 35 48 86 112	5 30 46 79 113	9 62 80 109 130
141	1 3 7 15 102	9 19 35 53 128	5 33 60 89 110	11 41 58 78 103
142	1 3 7 15 46	9 29 61 87 114	10 35 75 86 108	5 23 93 106 123
143	1 3 7 15 47	5 27 43 62 112	9 29 77 101 118	10 55 83 94 120
144	1 3 7 15 93	5 39 81 118 128	17 46 73 91 121	9 22 50 109 133
145	1 3 7 12 33	8 57 74 111 125	13 44 73 97 120	16 59 81 99 126
146	1 3 7 15 105	16 34 54 86 119	5 40 62 87 115	10 29 55 68 79
147	1 3 7 15 44	11 39 56 69 90	5 24 40 72 105	9 31 83 93 129
148	1 3 7 12 42	10 56 88 115 135	15 34 51 72 96	18 44 73 98 126
149	1 3 7 12 102	8 34 71 122 139	13 32 55 75 96	14 30 45 103 127
150	1 3 7 12 45	8 39 87 124 134	13 54 69 86 136	19 49 72 107 129

https://doi.org/10.3390/axioms15010035

References

1. Chung, F.R.K.; Salehi, J.A.; Wei, V.K. Optical orthogonal codes: Design, analysis and applications. *IEEE Trans. Inf. Theory* **1989**, *35*, 595–604. [CrossRef]
2. Bitan, S.; Etzion, J. Constructions for optimal constant weight cyclically permutable codes and difference families. *IEEE Trans. Inf. Theory* **1992**, *41*, 77–87. [CrossRef]
3. Stinson, D.R.; Wei, R.; Yin, J. Packings. In *The CRC Handbook of Combinatorial Designs*, 2nd ed.; Colbourn, C.J., Dinitz, J.H., Eds.; Chapman and Hall/CRC Press: Boca Raton, FL, USA, 2006; pp. 550–556
4. Fuji-Hara, R.; Miao, Y. Optical orthogonal codes: Their bounds and new optimal constructions. *IEEE Trans. Inf. Theory* **2000**, *46*, 2396–2406. [CrossRef]
5. Chu, W.; Colbourn, C.J. Optimal (n, 4, 2)-OOC of small order. *Discret. Math.* **2004**, *279*, 163–172. [CrossRef]
6. Buratti, M.; Pasotti, A. Further progress on difference families with block size 4 or 5. *Des. Codes Cryptogr.* **2010**, *56*, 1–20. [CrossRef]
7. Buratti, M.; Stinson, D.R. New results on modular Golomb rulers, optical orthogonal codes and related structures. *Ars Math. Contemp.* **2020**, *1*, 1–27. [CrossRef]
8. Baicheva, T.; Topalova, S. Classification of optimal (v,4,1) binary cyclically permutable constant weight codes and cyclic S(2,4,v) designs with $v \leq 76$. *Probl. Inf. Transm.* **2011**, *47*, 224–231. [CrossRef]
9. Moreno, O.; Zhan, Z.; Kumar, P.V.; Zinoviev, V.A. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Inf. Theory* **1995**, *41*, 448–455. [CrossRef]
10. Nguyen, Q.A.; Gyöfri, L.; Massey, J.L. Constructions of binary constant weight cyclic codes and cyclically permutable codes. *IEEE Trans. Inf. Theory* **1992**, *38*, 940–949. [CrossRef]
11. Baicheva, T.; Topalova, S. Classification of maximal optical orthogonal codes of weight 3 and small lengths. *Serdica J. Comput.* **2015**, *9*, 83–92. [CrossRef]
12. Brickell, E.F.; Wei, V.K. Optical orthogonal codes and cyclic block designs. *Congr. Numer.* **1987**, *58*, 175–192.
13. Buratti, M.; Momihara, K.; Pasotti, A. New results on optimal (v, 4, 2, 1) optical orthogonal codes. *Des. Codes Cryptogr.* **2011**, *58*, 89–109. [CrossRef]
14. Chang, Y.; Ji, L. Optimal $(4up, 5, 1)$ optical orthogonal codes. *J. Comb. Des.* **2004**, *12*, 346–361. [CrossRef]
15. Chu, W.; Golomb, S.W. A new recursive construction for optical orthogonal codes. *IEEE Trans. Inf. Theory* **2003**, *49*, 3072–3076.
16. Ma, S.; Chang, Y. A new class of optimal optical orthogonal codes with weight five. *IEEE Trans. Inf. Theory* **2004**, *50*, 1848–1850. [CrossRef]
17. Ma, S.; Chang, Y. Constructions of optimal optical orthogonal codes with weight five. *J. Comb. Des.* **2005**, *13*, 54–69. [CrossRef]
18. Tang, Y.; Yin, J. Combinatorial constructions for a class of optimal OOCs. *Sci. China A* **2002**, em 45, 1268–1275.
19. Wang, S.; Wang, L.; Wang, J. A new class of optimal optical orthogonal codes with weight six. In Proceedings of the Seventh International Workshop of Signal Design and its Applications in Communications, Bengaluru, India, 14–18 September 2015.
20. Yin, J. Some combinatorial constructions for optical orthogonal codes. *Discrere Math.* **1998**, *185*, 201–219. [CrossRef]
21. Zhao, C.; Chang, Y.; Feng, F. The existence of optimal (v, 4, 1) optical orthogonal codes achieving the Johnson bound. *IEEE Trans. Inf. Theory* **2024**, *70*, 8746–8757. [CrossRef]
22. Chen, K.; Zhu, L. Existence of (q, 6, 1) difference families with q a prime power. *Des. Codes Cryptogr.* **1998**, *15*, 167–173. [CrossRef]
23. Chen, K.; Zhu, L. Existence of (q, k, 1) difference families with q a prime power and k = 4,5. *J. Comb. Des.* **1999**, *7*, 21–30. [CrossRef]
24. Chen, K.; Wei, R.; Zhu, L. Existence of (q, 7, 1) difference families with q a prime power. *J. Comb. Des.* **2002**, *10*, 126–138. [CrossRef]
25. Hetman, I.; Baicheva, T.; Topalova, S. Construction of (v,k,1) cyclic difference families with small parameters. *J. Algebra Comb. Discret. Struct. Appl.* **2026**, *13*, 111–119.
26. Julian, R.; Abel, R.; Costa, S.; Finizio, N. Directed-ordered whist tournaments and (v,5,1) difference families: Existence results and some new classes of Z-cyclic solutions. *Discret. Appl. Math.* **2004**, *143*, 43–53. [CrossRef]
27. Colbourn, M.J.; Mathon, R.A. On cyclic Steiner 2-designs. *Ann. Discret. Math.* **1980**, *7*, 215–253.
28. Colbourn, C.J.; Colbourn, M.J. On cyclic Steiner systems S(2,6,91). *Abstr. Pap. Present. Am. Math. Soc.* **1982**, *5*, 463.
29. Hanani, H. Balanced incomplete block designs and related designs. *Discret. Math.* **1975**, *11*, 255–369. [CrossRef]
30. Janko, Z.; Tonchev, V.D. Cyclic 2-(91, 6, 1) designs with multiplier automorphisms. *Discret. Math.* **1991**, *97*, 265–268. [CrossRef]
31. Baicheva, T.; Topalova, S. Classification of optimal (v, k, 1) binary cyclically permutable constant weight codes with k = 5, 6 and 7 and small lengths. *Des. Codes Cryptogr.* **2019**, *87*, 365–374. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

https://doi.org/10.3390/axioms15010035

axioms

MDPI

Article

Radical Numerical Semigroups

María Ángeles Moreno-Frías [1,*,†] and José C. Rosales [2,†]

[1] Department of Mathematics, Faculty of Sciences, University of Cádiz, E-11510 Cádiz, Spain
[2] Department of Algebra, Faculty of Sciences, University of Granada, E-18071 Granada, Spain
* Correspondence: mariangeles.moreno@uca.es
† These authors contributed equally to this work.

Abstract

This work contributes to the study of radical numerical semigroups. If $n \in \mathbb{Z}$ where $n \geq 2$, then the product of all its prime positive divisors is called the radical of n. It is denoted by $\mathrm{r}(n)$. A radical numerical semigroup is a numerical semigroup S such that $s + \mathrm{r}(s) \in S$ for every $s \in S \backslash \{0\}$. We present three algorithms that will help us understand the structure of radical semigroups. These algorithms allow us to calculate all radical numerical semigroups with a fixed genus, with a fixed Frobenius number, as well as with a fixed multiplicity. Furthermore, given X, a set of positive integers such that $\gcd(X) = 1$, we will prove the existence of the smallest radical semigroup containing X. We will also present an algorithm to obtain it.

Keywords: radical numerical semigroup; frobenius variety; frobenius pseudo-variety; frobenius number; genus; multiplicity

MSC: 20M14; 11D07

1. Introduction

Let $\mathbb{Z} = \{0, 1, -1, 2, -2, \cdots\}$ be the set of integers and $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$. A subset M of $\mathbb{N}$ is a submonoid of $(\mathbb{N}, +)$ if $a + b \in M$ for all $a, b \in M$ and $0 \in M$. We will say that a submonoid S of $(\mathbb{N}, +)$ is a numerical semigroup if $\mathbb{N} \backslash S = \{x \in \mathbb{N} \mid x \notin S\}$ is a finite set.

Given S, a numerical semigroup, let us consider the following notable elements of S: $\mathrm{m}(S) = \min(S \backslash \{0\})$, $\mathrm{F}(S) = \max\{z \in \mathbb{Z} \mid z \notin S\}$ and $\mathrm{g}(S) = \sharp(\mathbb{N} \backslash S)$ (where $\sharp X$ denotes the cardinality of a set X). These are three important invariants, which we will call multiplicity, the Frobenius number and the genus of S, respectively.

Let A be a non-empty subset of $\mathbb{N}$. Denote by $\langle A \rangle$ the submonoid of $(\mathbb{N}, +)$ generated by A. That is

$$\langle A \rangle = \{\lambda_1 a_1 + \cdots + \lambda_r a_r \mid r \in \mathbb{N} \backslash \{0\},\ \{a_1, \ldots, a_r\} \subseteq A \text{ and } \{\lambda_1, \ldots, \lambda_r\} \subseteq \mathbb{N}\}.$$

By virtue of ([1], Lema 2.1), the necessary and sufficient condition for $\langle A \rangle$ to be a numerical semigroup is $\gcd(A) = 1$.

We will say that a non-empty subset A of $\mathbb{N}$ constitutes a system of generators of a submonoid M of $\mathbb{N}$ if $M = \langle A \rangle$. When this set is minimal with respect to inclusion order, then A is a minimal system of generators of M. In ([1], Corollary 2.8), it is proven that every submonoid of $(\mathbb{N}, +)$ has a unique minimal system of generators, which is finite. The minimal system of generators of M will be denoted by $\mathrm{msg}(M)$. The cardinality of this system defines the embedding dimension of M and will be denoted by $\mathrm{e}(M)$.

There is a close relationship between numerical semigroups and Diophantine equations, since historically numerical semigroups arose from the study of the solutions of Diophantine equations.

The study of numerical semigroups is equivalent to the study of non-negative integer solutions of a linear equation with coefficients in $\mathbb{N}$. For this reason, it is a classic problem, and there is a large list of works dedicated to its study (see, for instance, [2–9]).

The reader unfamiliar with the study of numerical semigroups may find the notation multiplicity, embedding dimension, genus, ... somewhat surprising.

We will say in this regard that in the literature there is a long list of publications dedicated to the study of analytically irreducible one-dimensional local domains via their semigroup of values, which turns out to be a numerical semigroup (see [10–17]). All these invariants introduced above have their interpretation in this context, hence their names. In this sense [10], it is a good dictionary for translating the results of numerical semigroup theory into ring theory.

The Frobenius problem for numerical semigroups consists of calculating invariants such as genus and Frobenius number based solely on the minimal generators of the semigroup (see [18]). Historically, the two-embedding dimension case was solved by Sylvester [19]; however, finding a general solution for embedding dimension greater than or equal to three remains one of the outstanding challenges in the theory today. Despite this, current research has led to solutions for a wide variety of special families of numerical semigroups (see, for instance, [2,4–7,17]).

The relationship between the Frobenius number, the genus and the embedding dimension of a numerical semigroup is also a research problem in the theory of numerical semigroups. Indeed, if S is a numerical semigroup, then A.S. Wilf conjectures in [20] that $\mathrm{e}(S)\mathrm{g}(S) \leq (\mathrm{e}(S)-1)(\mathrm{F}(S)+1)$. Currently unsolved, this problem stands as a cornerstone of numerical semigroup theory. However, the conjecture has been validated for numerous specific classes of semigroups (see, for example, [21–25]).

If $g \in \mathbb{N}$, then denote by $\mathrm{S}(g) = \{S \mid S \text{ is a numerical semigroup and } \mathrm{g}(S) = g\}$. This set has been widely considered in the literature (see [26–30]). Many of these works are motivated by the conjecture presented in [27], in which it is asserted that the sequence $\{\#\mathrm{S}(g)\}_{g\in\mathbb{N}}$ is increasing and has a behavior similar to the Fibonacci sequence. In [31] it is shown that $\lim_{g\to\infty} \frac{\#\mathrm{S}(g)}{\#\mathrm{S}(g-1)}$ is the golden number, and therefore the asymptotic behavior of the sequence $\{\#\mathrm{S}(g)\}_{g\in\mathbb{N}}$ is similar to the behavior of the Fibonacci sequence. However, it is currently an open problem to demonstrate that $\#\mathrm{S}(g-1) \leq \#\mathrm{S}(g)$ for every $g \in \mathbb{N}\backslash\{0\}$.

If $n \in \mathbb{N}\backslash\{0,1\}$, then the radical of n, denoted by $\mathrm{r}(n)$, is the product of all positive prime numbers that divide n. Thus, if $n = P_1^{\alpha_1} \cdot \ldots \cdot P_k^{\alpha_k}$ is the expression of an integer n greater than or equal to two, as a product of prime numbers, then $\mathrm{r}(n) = P_1 \cdot \ldots \cdot P_k$. This concept is used in different parts of Number Theory, such as in the formulation of the abc conjecture, also known as the Oesterlé–Masser conjecture (see [32–35]). This conjecture is considered the most important unsolved problem in Diophantine analysis.

Given S a numerical semigroup, if $s + \mathrm{r}(s) \in S$ for all $s \in S\backslash\{0\}$, then we say that S is radical. The main purpose of this work will be to explore this kind of numerical semigroups.

Denote by $\mathscr{R} = \{S \mid S \text{ is a radical numerical semigroup}\}$. We begin Section 2 by showing that $\mathscr{R}$ is a Frobenius variety with infinite cardinality. This fact, together with the results of [36], allows us to construct a tree whose set of vertices is $\mathscr{R}$. As an application, we will present an algorithm that enables us to calculate all radical numerical semigroups with a given genus.

If $X \subseteq \mathbb{N}$, then we denote by $\mathscr{R}[X]$ the intersection of all elements of $\mathscr{R}$ that contain X. In Section 3, we will see that $\mathscr{R} = \{\mathscr{R}[X] \mid X \subseteq \mathbb{N}\backslash\{0\}, X \text{ finite and } \gcd(X) = 1\}$.

https://doi.org/10.3390/axioms15010036

Moreover, we will show an algorithm that computes $\mathscr{R}[X]$ from a finite subset X of $\mathbb{N}\backslash\{0\}$ such that $\gcd(X) = 1$.

For any positive integer F, let $\mathscr{R}(F) = \{S \in \mathscr{R} \mid \mathrm{F}(S) = F\}$. At the beginning of Section 4, we show that $\mathscr{R}(F)$ constitutes a covariety. This property, combined with the findings in [37], enables the construction of a tree rooted whose set of vertices is $\mathscr{R}(F)$. Consequently, we designed an algorithm to compute all the elements of $\mathscr{R}(F)$.

Let $m \in \mathbb{N} \setminus \{0, 1\}$. We define $\mathscr{R}_m$ as the set of elements in $\mathscr{R}$ with multiplicity m. After proving in Section 5 that $\mathscr{R}_m$ is an infinite Frobenius pseudo-variety, we apply the results from [38] to organize $\mathscr{R}_m$ into a tree structure. Finally, we propose an algorithm to find all semigroups in $\mathscr{R}_m$ with a given genus g.

In this paper, all the algorithms presented are illustrated with examples in order to demonstrate how they work as well as to facilitate their understanding. Furthermore, they can be implemented using the numerical SGP package in the GAP System (see [39,40]).

2. The Tree of Radical Numerical Semigroups

We say that a non-empty family $\mathscr{V}$ of numerical semigroups is a Frobenius variety if it verifies the following:

1. If $\{S_1, S_2\} \subseteq \mathscr{V}$, then $S_1 \cap S_2 \in \mathscr{V}$.
2. If $T \in \mathscr{V}$ and $T \neq \mathbb{N}$, then $T \cup \{\mathrm{F}(T)\} \in \mathscr{V}$.

Our first aim in this section will be to prove that $\mathscr{R} = \{S \mid S \text{ is a radical numerical semigroup}\}$ is a Frobenius variety. Note that $\{0, m, \rightarrow\} \in \mathscr{R}$, where the symbol $\rightarrow$ means that every integer greater than m belongs to the set, for all $m \in \mathbb{N}$. Consequently, $\mathscr{R}$ is a set with infinite cardinality.

It is clear that $\mathrm{F}(\mathbb{N}) = -1$ and $\mathrm{F}(S) \in \mathbb{N}\backslash\{0\}$ for all numerical semigroup S such that $S \neq \mathbb{N}$.

The following result has an easy proof:

Lemma 1. *The following is verified:*

1. *Let S be a numerical semigroup such that $S \neq \mathbb{N}$. Then $S \cup \{\mathrm{F}(S)\}$ is also a numerical semigroup.*
2. *If S_1 and S_2 are numerical semigroups, then $S_1 \cap S_2$ is also a numerical semigroup. Moreover, $\mathrm{F}(S_1 \cap S_2) = \max\{\mathrm{F}(S_1), \mathrm{F}(S_2)\}$ and $\mathrm{m}(S_1 \cap S_2) \geq \max\{\mathrm{m}(S_1), \mathrm{m}(S_2)\}$.*

Proposition 1. *$\mathscr{R}$ is a Frobenius variety.*

Proof. As $\mathbb{N} \in \mathscr{R}$, then $\mathscr{R} \neq \emptyset$. If $\{S, T\} \subseteq \mathscr{R}$, then by Lemma 1, we know that $S \cap T$ is a numerical semigroup. If $x \in (S \cap T)\backslash\{0\}$, then $x \in S\backslash\{0\}$ and $x \in T\backslash\{0\}$. Thus, $x + \mathrm{r}(x) \in S \cap T$ and so $S \cap T \in \mathscr{R}$. Finally, if $S \in \mathscr{R}$ and $S \neq \mathbb{N}$, then by Lemma 1, we have that $S \cup \{\mathrm{F}(S)\}$ is a numerical semigroup. If $x \in (S \cup \{F(S)\})\backslash\{0\}$, then we consider the following two cases:

1. If $x \in S$, then $x + \mathrm{r}(x) \in S \subseteq S \cup \{\mathrm{F}(S)\}$.
2. If $x = \mathrm{F}(S)$, then $x + \mathrm{r}(x) > \mathrm{F}(S)$, and so $x + \mathrm{r}(x) \in S \cup \{\mathrm{F}(S)\}$.

□

A graph G is defined as a pair (V, E) where V is a non-empty set and E is a subset of $\{(u, v) \in V \times V \mid u \neq v\}$. We will call the elements of V and E vertices and edges of the graph G, respectively.

A path of length n, connecting the vertices u and v of G, is a sequence of different edges of the form $(v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n)$ such that $v_0 = u$ and $v_n = v$.

https://doi.org/10.3390/axioms15010036

We will say that a graph G is a tree if there exists a vertex a (known as *the root* of G) such that for any other vertex v of G there exists a unique path connecting v and a. If (u, v) is an edge of the tree G, we say that u is a child of v.

Consider the graph $\mathrm{G}(\mathscr{R})$, defined in the following way: The set of vertices is $\mathscr{R}$ and $(S, T) \in \mathscr{R} \times \mathscr{R}$ is an edge if and only if $T = S \cup \{\mathrm{F}(S)\}$.

By Proposition 1 and ([36], Theorem 27), the following result is obtained. In it we can find a description of the children of the vertices in the tree $\mathrm{G}(\mathscr{R})$.

Theorem 1. *$\mathrm{G}(\mathscr{R})$ is a tree rooted at $\mathbb{N}$. In addition, the set formed by the children of a vertex S of $\mathrm{G}(\mathscr{R})$ is $\{S\backslash\{x\} \mid x \in \mathrm{msg}(S), x > \mathrm{F}(S)$ and $S\backslash\{x\} \in \mathscr{R}\}$.*

The next result can be consulted in ([1], Lemma 2.3).

Lemma 2. *Let S be a numerical semigroup and $x \in S$. Then, $S\backslash\{x\}$ is a numerical semigroup if and only if $x \in \mathrm{msg}(S)$.*

Proposition 2. *Let $S \in \mathscr{R}$ and $x \in \mathrm{msg}(S)$. Then, $S\backslash\{x\} \in \mathscr{R}$ if and only if $s + \mathrm{r}(s) \neq x$ for all $s \in S$ such that $\frac{x}{2} \leq s < x$.*

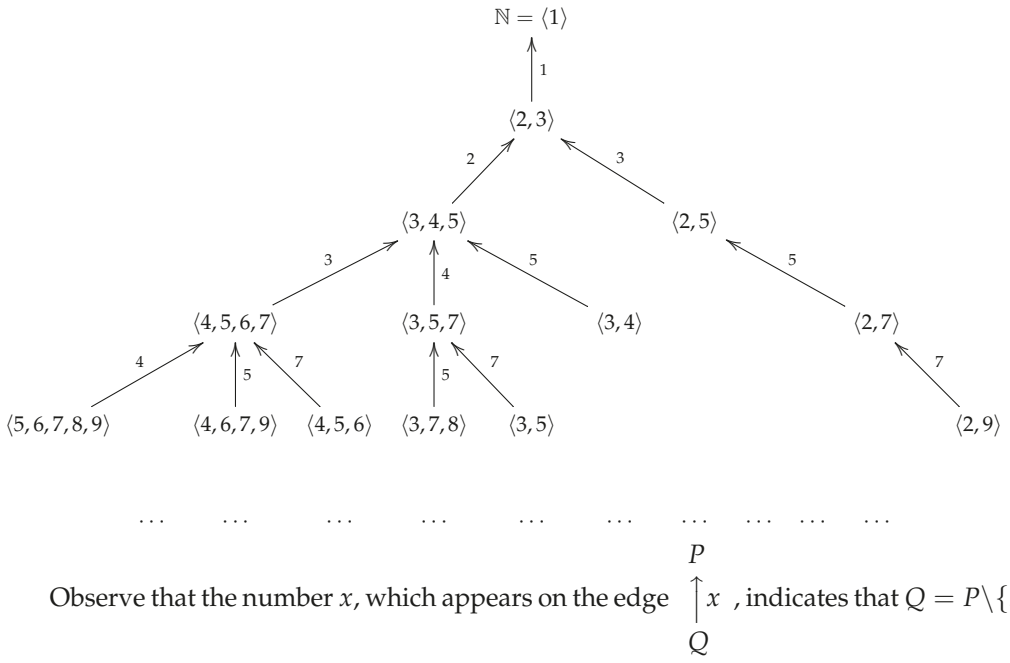
Proof. *(Necessity).* If $s \in S$ and $\frac{x}{2} \leq s < x$, then $s \in S\backslash\{0, x\}$. As $S\backslash\{x\} \in \mathscr{R}$, then $s + \mathrm{r}(s) \in S\backslash\{x\}$, and so $s + \mathrm{r}(s) \neq x$.

(Sufficiency). By Lemma 2, we know that $S\backslash\{x\}$ is a numerical semigroup. We will see that $S\backslash\{x\} \in \mathscr{R}$. In fact, let $s \in S\backslash\{x, 0\}$ and we will consider the following three cases:

(1) If $s < \frac{x}{2}$, then by applying that $\mathrm{r}(s) \leq x$, we deduce that $s + \mathrm{r}(s) \in S\backslash\{x\}$.
(2) If $\frac{x}{2} \leq s < x$, then by hypothesis $s + \mathrm{r}(s) \in S\backslash\{x\}$.
(3) If $s > x$, then it is clear that $s + \mathrm{r}(s) > x$ and so $s + \mathrm{r}(s) \in S\backslash\{x\}$.

As a consequence of (1), (2) and (3) we have that if $s \in S\backslash\{x, 0\}$, then $s + \mathrm{r}(s) \in S\backslash\{x\}$. Hence, $S\backslash\{x\} \in \mathscr{R}$. □

Recursively, we can construct a tree starting from its root and connecting, by means of an edge, each vertex already constructed with each of its children. By using this idea, Theorem 1 and Proposition 2, we can build the tree $\mathrm{G}(\mathscr{R})$ as shown below.



Observe that the number x, which appears on the edge $\begin{array}{c} P \\ \uparrow x \\ Q \end{array}$, indicates that $Q = P\backslash\{x\}$.

In addition, observe that $\mathrm{F}(Q) = x$. The ellipsis indicates that the tree continues.

https://doi.org/10.3390/axioms15010036

It is not possible to give an algorithm that computes all the elements of $\mathscr{R}$, because its cardinality is infinite. Therefore, our next objective in this section will be to design an algorithm that allows us to obtain all the elements of $\mathscr{R}$ with a specific genus.

Let $G = (V, E)$ be a rooted tree. We will call the depth of a vertex $v \in V$ in G the length of the only path that connects v with its root. It will be denoted by $\mathrm{d}(v)$. Let $n \in \mathbb{N}$; we denote by $\mathrm{N}(G, n) = \{x \in V \mid \mathrm{d}(x) = n\}$. The height of G, denoted by $\mathrm{h}(G)$, is the maximum of the set $\{\mathrm{d}(v) \mid v \in V\}$. Note that $\mathrm{h}(G) = \max\{n \in \mathbb{N} \mid \mathrm{N}(G, n) \neq \emptyset\}$.

The following result is easily demonstrated:

Proposition 3. *Let $n \in \mathbb{N}$. The following statements are verified:*

1. $\mathrm{N}(G(S), n+1) = \{S \in \mathscr{R} \mid S$ *is a child of an element of* $\mathrm{N}(G(\mathscr{R}), n)\}$.
2. $\mathrm{N}(G(\mathscr{R}), n) = \{S \in \mathscr{R} \mid \mathrm{g}(S) = n\}$.
3. *The tree $G(\mathscr{R})$ has an infinite height.*

As a consequence of Proposition 3, we have the next result.

Corollary 1. *With the above notation, we have $\mathbb{N} = \{\mathrm{g}(S) \mid S \in \mathscr{R}\}$.*

Now, we are in conditions to present an algorithm that computes all the elements of $\mathscr{R}$ with a given genus.

Algorithm 1 Computation of $\{S \in \mathscr{R} \mid \mathrm{g}(S) = g\}$

INPUT: A non negative integer g.
OUTPUT: $\{S \in \mathscr{R} \mid \mathrm{g}(S) = g\}$.

(1) $A = \{\mathbb{N}\}$, $i = 0$.
(2) If $i = g$, then return A and stop.
(3) For all $S \in A$ compute $\alpha(S) = \{x \in \mathrm{msg}(S) \mid x > \mathrm{F}(S)$ and $s + \mathrm{r}(s) \neq x$ for all $s \in S$ such that $\frac{x}{2} \leq s < x\}$.
(4) $A := \bigcup_{S \in A} \{S \backslash \{x\} \mid x \in \alpha(S)\}$, $i := i + 1$ and go to Step (2).

In what follows, we illustrate the operation of this algorithm.

Example 1. *We will determine the set $\{S \in \mathscr{R} \mid \mathrm{g}(S) = 2\}$, by applying Algorithm 1 as follows:*

- $A = \{\mathbb{N}\}$, $i = 0$.
- $\alpha(\mathbb{N}) = \{1\}$.
- $A = \{\langle 2, 3\rangle\}$, $i = 1$.
- $\alpha(\langle 2, 3\rangle) = \{2, 3\}$.
- $A = \{\langle 3, 4, 5\rangle, \langle 2, 5\rangle\}$, $i = 2$.
- $\{S \in \mathscr{R} \mid \mathrm{g}(S) = 2\} = \{\langle 3, 4, 5\rangle, \langle 2, 5\rangle\}$.

We will end this section by posing the following two questions whose answers could be helped by Algorithm 1:

1. Do the elements of set $\mathscr{R}$ satisfy the conjecture of Bras-Amorós?. That is $\#\{S \in \mathscr{R} \mid \mathrm{g}(S) = g\} \leq \#\{S \in \mathscr{R} \mid \mathrm{g}(S) = g + 1\}$ for all $g \in \mathbb{N}$?
2. Do the elements of set $\mathscr{R}$ satisfy Wilf's conjecture? That is, if $S \in \mathscr{R}$, then $\mathrm{e}(S)\mathrm{g}(S) \leq (\mathrm{e}(S) - 1)(\mathrm{F}(S) + 1)$?

https://doi.org/10.3390/axioms15010036

3. $\mathscr{R}$-System of Generators

By Proposition 1, we know that the finite intersection of elements from $\mathscr{R}$ is again an element of $\mathscr{R}$. The intersection of infinite elements of $\mathscr{R}$ in general is not an element of $\mathscr{R}$, as we show in the following example:

Example 2. *For every $n \in \mathbb{N}$, let $S_n = \{0, n, \rightarrow\}$. It is clear that $S_n \in \mathscr{R}$ for all $n \in \mathbb{N}$ and $\bigcap_{n\in\mathbb{N}} S_n = \{0\} \notin \mathscr{R}$.*

Since the intersection of any collection of elements from $\mathscr{R}$, whether finite or infinite, is invariably a submonoid of $(\mathbb{N}, +)$, we are led to the following definition. An $\mathscr{R}$-monoid is a submonoid of $(\mathbb{N}, +)$ that is obtainable as the intersection of elements from $\mathscr{R}$.

Given $X \subseteq \mathbb{N}$, then the intersection of all elements of $\mathscr{R}$ that contains X, will be denoted by $\mathscr{R}[X]$.

The following result has an immediate proof.

Proposition 4. *If $X \subseteq \mathbb{N}$, then $\mathscr{R}[X]$ is the smallest $\mathscr{R}$-monoid that contains X.*

If $X \subseteq \mathbb{N}$ and $\mathscr{R}[X] = M$, then X is called a $\mathscr{R}$-system of generators of M. In addition, if $M \neq \mathscr{R}[Y]$ for every $Y \subsetneq X$, we will say that X is a $\mathscr{R}$-minimal system of generators of M.

By applying Proposition 1 and ([37], Theorem 18), we obtain the following result:

Theorem 2. *Every $\mathscr{R}$-monoid has a unique $\mathscr{R}$-minimal system of generators.*

Given M, an $\mathscr{R}$-monoid, denoted by $\mathscr{R}\mathrm{msg}(M)$, is the $\mathscr{R}$-minimal system of generators of M.

The next result is easily verified.

Proposition 5. *Let M be an $\mathscr{R}$-monoid. Then, $\mathscr{R}\mathrm{msg}(M) \subseteq \mathrm{msg}(M)$.*

If M is an $\mathscr{R}$-monoid, then the cardinality of $\mathscr{R}\mathrm{msg}(M)$ will be called the $\mathscr{R}$-rank of M, and we denote it by $\mathscr{R}\mathrm{rank}(M)$.

From Theorem 2 and Proposition 5, the following result can be obtained:

Corollary 2. *The set of all $\mathscr{R}$-monoids is $\{\mathscr{R}[X] \mid X$ is a finite subset of $\mathbb{N}\backslash\{0\}\}$.*

Lemma 3. *Let M be an $\mathscr{R}$-monoid. Then, $M \in \mathscr{R}$ if and only if M is a numerical semigroup.*

Proof. *(Necessity).* If $M \in \mathscr{R}$, then by definition M is a numerical semigroup.

(Sufficiency). As M is an $\mathscr{R}$-monoid, then there is a family $\{S_i \mid i \in I\}$ of elements from $\mathscr{R}$ such that $M = \bigcap_{i\in I} S_i$. If $x \in M\backslash\{0\}$, then $x \in S_i\backslash\{0\}$ for all $i \in I$ and so $x + \mathrm{r}(x) \in S_i$ for all $i \in I$. Therefore, $x + \mathrm{r}(x) \in M$, and consequently $M \in \mathscr{R}$. □

For $a, b \in \mathbb{Z}$, we denote by $a \mid b$ if $b = ca$ for some $c \in \mathbb{Z}$. Or else, a is said not to divide b, which is represented by the notation $a \nmid b$.

Proposition 6. *Let $X \subseteq \mathbb{N}\backslash\{0\}$. Then, $\mathscr{R}[X]$ is an element of $\mathscr{R}$ if and only if* $\gcd(X) = 1$.

Proof. *(Necessity).* We suppose that $\gcd(X) = d \neq 1$. Then there is a positive prime p such that $p \mid d$. Let $S(p, n) = \langle p\rangle \cup \{n, \rightarrow\}$ for all $n \in \mathbb{N}$. It is clear that $S(p, n)$ is an element of

https://doi.org/10.3390/axioms15010036

$\mathscr{R}$ that contains X for all $n \in \mathbb{N}$. Therefore, $\mathscr{R}[X] \subseteq \bigcap_{n\in\mathbb{N}} S(p,n) = \langle p \rangle$ and so $\mathscr{R}[X]$ is not a numerical semigroup. Hence $\mathscr{R}[X]$ is not an element of $\mathscr{R}$.

(Sufficiency). As $\gcd(X) = 1$ and $X \subseteq \mathscr{R}[X]$, then we deduce that $\mathscr{R}[X]$ is a numerical semigroup. By applying Proposition 4 and Lemma 3, we can conclude that $\mathscr{R}[X]$ is an element of $\mathscr{R}$. □

The next result can be obtained by applying Corollary 2 and Proposition 6 and it gives us a complete description of the set of $\mathscr{R}$.

Corollary 3. *With the above notation,* $\mathscr{R} = \{\mathscr{R}[X] \mid X \subseteq \mathbb{N}\backslash\{0\}$, *X is finite and* $\gcd(X) = 1\}$.

We now aim to develop an algorithmic procedure for computing $\mathscr{R}[X]$ from a finite set $X \subset \mathbb{N}\backslash\{0\}$ such that $\gcd(X) = 1$. With this goal in mind, the following definition is required. An element x of a numerical semigroup S is called small if $x < \mathrm{F}(S)$. Denote by $\mathrm{N}(S) = \{s \in S \mid s < \mathrm{F}(S)\}$. Let $\mathrm{n}(S)$ denote the cardinality of $\mathrm{N}(S)$. It is obvious that $\mathrm{g}(S) + \mathrm{n}(S) = \mathrm{F}(S) + 1$.

Now we have all the necessary ingredients to show the algorithm that allows us to obtain set $\mathscr{R}[X]$.

Algorithm 2 Computation of $\mathscr{R}[X]$

INPUT: A finite subset X of $\mathbb{N}\backslash\{0\}$ such that $\gcd(X) = 1$.
OUTPUT: $\mathscr{R}[X]$.

(1) $S = \langle X \rangle$.
(2) $B(S) = \{s + \mathrm{r}(s) \mid s \in \mathrm{N}(S)\backslash\{0\}$ and $s + \mathrm{r}(s) \notin S\}$.
(3) If $B(S) = \emptyset$ then return S and stop.
(4) $S = \langle \mathrm{msg}(S) \cup B(S) \rangle$ and go to Step (2).

Below we show, with an example, how the previous algorithm works.

Example 3. *By applying Algorithm 2, we proceed to calculate the set* $\mathscr{R}[\{4,9\}]$ *as follows:*

- $S = \langle 4,9 \rangle = \{0,4,8,9,12,13,16,17,18,20,21,22,24,\rightarrow\}$.
- $B(S) = \{6,10\}$.
- $S = \langle 4,9,6,10 \rangle = \langle 4,6,9 \rangle = \{0,4,6,8,9,10,12,\rightarrow\}$.
- $B(S) = \emptyset$.
- $\mathscr{R}[\{4,9\}] = \langle 4,6,9 \rangle$.

Observe that $\{S \in \mathscr{R} \mid \mathscr{R}\mathrm{rank}(S) = 1\} = \{\mathbb{N}\}$. The following result is easy to prove and tells us what the set $\{S \in \mathscr{R} \mid \mathscr{R}\mathrm{rank}(S) = 2\}$ is like.

Proposition 7. *Let* $a, b \in \mathbb{N}\backslash\{0,1\}$ *with* $\gcd(a,b) = 1$. *Then* $\mathscr{R}[\{a,b\}]$ *is an element of* $\mathscr{R}$ *with* $\mathscr{R}$*-rank two. Moreover, every element of* $\mathscr{R}$ *with* $\mathscr{R}$*-rank two has this form.*

We will conclude this section by posing the following problem: If $\{a,b\} \subseteq \mathbb{N}\backslash\{0,1\}$ and $\gcd(a,b) = 1$, to find formulas based on a and b that calculate the Frobenius number, the genus and the embedding dimension of $\mathscr{R}[\{a,b\}]$.

4. Radical Numerical Semigroups with a Given Frobenius Number

We say that a family $\mathscr{C}$ of numerical semigroups is a covariety if it verifies the following conditions:

1. There is the minimum, with respect to inclusion order, of $\mathscr{C}$.
2. If $\{S_1, S_2\} \subseteq \mathscr{C}$, then $S_1 \cap S_2 \in \mathscr{C}$.

https://doi.org/10.3390/axioms15010036

3. Let $S \in \mathscr{C}$ with $S \neq \min(\mathscr{C})$, then $S\backslash\{\mathrm{m}(S)\} \in \mathscr{C}$.

Denote by $\mathscr{R}(F) = \{S \in \mathscr{R} \mid \mathrm{F}(S) = F\}$, where F is a positive integer.

Proposition 8. *$\mathscr{R}(F)$ is a covariety for every positive integer F as follows:*

Proof.

1. It is trivial that the minimum of $\mathscr{R}(F)$ is $\{0, F+1, \rightarrow\}$.
2. If $\{S, T\} \subseteq \mathscr{R}(F)$, then by Lemma 1, we know that $S \cap T$ is a numerical semigroup and $\mathrm{F}(S \cap T) = F$. By Proposition 1, we have that $S \cap T \in \mathscr{R}$ and so $S \cap T \in \mathscr{R}(F)$.
3. If $S \in \mathscr{R}(F)$ and $S \neq \{0, F+1, \rightarrow\}$, then $\mathrm{m}(S) < F$. By applying Lemma 2, we have that $S\backslash\{\mathrm{m}(S)\}$ is a numerical semigroup. As $\mathrm{m}(S) < F$, then $\mathrm{F}(S\backslash\{\mathrm{m}(S)\}) = F$. If $s \in S\backslash\{0, \mathrm{m}(S)\}$, then $s > \mathrm{m}(S)$ and thus $s + \mathrm{r}(s) \in S\backslash\{\mathrm{m}(S)\}$. Therefore, $S\backslash\{\mathrm{m}(S)\} \in \mathscr{R}(F)$.

□

We define the graph $\mathrm{G}(\mathscr{R}(F))$ in the following way: $\mathscr{R}(F)$ is its set of vertices, and $(S, T) \in \mathscr{R}(F) \times \mathscr{R}(F)$ is an edge if and only if $T = S\backslash\{\mathrm{m}(S)\}$.

The next result is a direct consequence from Proposition 8 and ([37], Proposition 2.3).

Theorem 3. *If $F \in \mathbb{N}\backslash\{0\}$, then $\mathrm{G}(\mathscr{R}(F))$ is a tree and the set $\{0, F+1, \rightarrow\}$ is its root.*

We now proceed to characterize the children of an arbitrary vertex in the tree $\mathrm{G}(\mathscr{R}(F))$. To this end, we introduce the following definition. An integer x is a special gap of a numerical semigroup S if $x \notin S$ and $S \cup \{x\}$ is a numerical semigroup. The set formed by the special gaps of S will be denoted by $\mathrm{SG}(S)$.

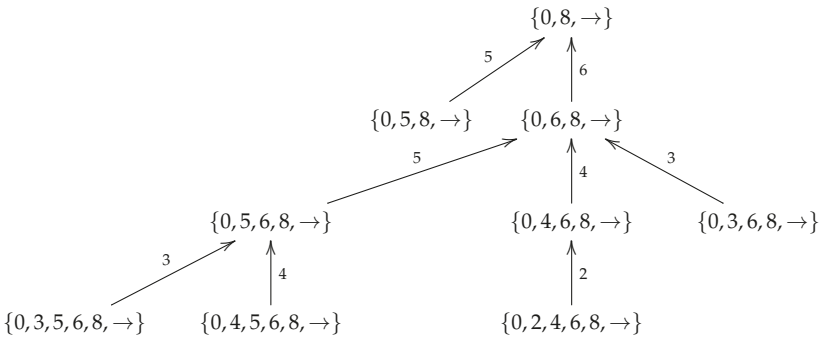
The following result, derived from Proposition 8 and ([37], Proposition 2.4), identifies the children of any given vertex in $\mathrm{G}(\mathscr{R}(F))$.

Proposition 9. *If $F \in \mathbb{N}\backslash\{0\}$ and $S \in \mathscr{R}(F)$, then the set formed by the children of S in the tree $\mathrm{G}(\mathscr{R}(F))$ is $\{S \cup \{x\} \mid x \in \mathrm{SG}(S),\ x < \mathrm{m}(S)$ and $S \cup \{x\} \in \mathscr{R}(F)\}$.*

A straightforward verification shows the following result:

Proposition 10. *Let $F \in \mathbb{N}\backslash\{0\}$, $S \in \mathscr{R}(F)$ and $x \in \mathrm{SG}(S)$ such that $x \neq F$. Then $S \cup \{x\} \in \mathscr{R}(F)$ if and only if $x + \mathrm{r}(x) \in S$.*

By applying the comment after the Proposition 2, Theorem 3 and Propositions 9 and 10, we can build the tree $\mathrm{G}(\mathscr{R}(7))$ which is shown below.



https://doi.org/10.3390/axioms15010036

Note that the label x on the edge $\begin{array}{c} P \\ \uparrow x \\ Q \end{array}$ serves to indicate that $Q = P \cup \{x\}$. Moreover, observe that $\mathrm{m}(Q) = x$.

Let S be a numerical semigroup and $n \in S\backslash\{0\}$. The Apéry set of n in S (see [41]) is defined as $\mathrm{Ap}(S,n) = \{s \in S \mid s - n \notin S\}$.

By ([1], Lemma 2.4), we obtain the following:

Lemma 4. *Let S be a numerical semigroup and $n \in S\backslash\{0\}$. Then, $\mathrm{Ap}(S,n) = \{0 = w(0), w(1), \ldots, w(n-1)\}$, where $w(i)$ is the least element of S congruent with i modulo n for all $i \in \{0, \ldots, n-1\}$.*

Note 1. *Let S be a numerical semigroup, and we assume known $\mathrm{Ap}(S,n)$ for some $n \in S\backslash\{0\}$. Then we conclude the following:*

1. *We can readily determine $\mathrm{SG}(S)$, by applying ([37], Remark 1).*
2. *It is straightforward to compute $\mathrm{Ap}(S \cup \{x\}, n)$ for all $x \in \mathrm{SG}(S)$ by using ([37], Remark 2).*

All the required conditions are now in place to present the algorithm that computes the set $\mathscr{R}(F)$.

Algorithm 3 Computation of $\mathscr{R}(F)$

INPUT: A positive integer F.
OUTPUT: $\mathscr{R}(F)$.

(1) $A = B = \{\{0, F+1, \to\}\}$ and $\mathrm{Ap}(\{0, F+1, \to\}, F+1) = \{0, F+2, F+3, \cdots, 2F+1\}$.
(2) For every $S \in B$ computes $\theta(S) = \{x \in \mathrm{SG}(S) \mid x \neq F,\ x < \mathrm{m}(S)$ and $x + \mathrm{r}(x) \in S\}$.
(3) $C = \bigcup_{S \in B} \{S \cup \{x\} \mid x \in \theta(S)\}$.
(4) If $C = \emptyset$, then return A and stop.
(5) $A := A \cup C$ and $B := C$.
(6) For all $S \in B$ computes $\mathrm{Ap}(S, F+1)$ and go to Step (2).

In the example below, we apply the above algorithm.

Example 4. *We are going to compute the set $\mathscr{R}(7)$, by applying Algorithm 3 as follows:*

- $A = B = \{\{0, 8, \to\}\}$ *and* $\mathrm{Ap}(\{0, 8, \to\}, 8) = \{0, 9, 10, \cdots, 15\}$.
- $\theta(\{0, 8, \to\}) = \{5, 6\}$.
- $A = \{\{0, 8, \to\}, \{0, 5, 8, \to\}, \{0, 6, 8, \to\}\}$ *and* $B = \{\{0, 5, 8, \to\}, \{0, 6, 8, \to\}\}$.
- $\mathrm{Ap}(\{0, 5, 8, \to\}, 8) = \{0, 5, 9, 10, 11, 12, 14, 15\}$ *and* $\mathrm{Ap}(\{0, 6, 8, \to\}, 8) = \{0, 6, 9, 10, 11, 12, 13, 15\}$.
- $\theta(\{0, 5, 8, \to\}) = \emptyset$ *and* $\theta(\{0, 6, 8, \to\}) = \{3, 4, 5\}$.
- $A = \{\{0, 8, \to\}, \{0, 5, 8, \to\}, \{0, 6, 8, \to\}, \{0, 3, 6, 8, \to\}, \{0, 4, 6, 8, \to\}, \{0, 5, 6, 8, \to\}\}$ *and* $B = \{\{0, 3, 6, 8, \to\}, \{0, 4, 6, 8, \to\}, \{0, 5, 6, 8, \to\}\}$.
- $\mathrm{Ap}(\{0, 3, 6, 8, \to\}, 8) = \{0, 3, 6, 9, 10, 12, 13, 15\}$, $\mathrm{Ap}(\{0, 4, 6, 8, \to\}, 8) = \{0, 4, 6, 9, 10, 11, 13, 15\}$ *and* $\mathrm{Ap}(\{0, 5, 6, 8, \to\}, 8) = \{0, 5, 6, 9, 10, 11, 12, 15\}$.
- $\theta(\{0, 3, 6, 8, \to\}) = \emptyset$, $\theta(\{0, 4, 6, 8, \to\}) = \{2\}$ *and* $\theta(\{0, 5, 6, 8, \to\}) = \{3, 4\}$.
- $A = \{\{0, 8, \to\}, \{0, 5, 8, \to\}, \{0, 6, 8, \to\}, \{0, 3, 6, 8, \to\}, \{0, 4, 6, 8, \to\}, \{0, 5, 6, 8, \to\}, \{0, 2, 4, 6, 8, \to\}, \{0, 3, 5, 6, 8, \to\}, \{0, 4, 5, 6, 8, \to\}\}$ *and* $B = \{\{0, 2, 4, 6, 8, \to\}, \{0, 3, 5, 6, 8, \to\}, \{0, 4, 5, 6, 8, \to\}\}$.
- $\mathrm{Ap}(\{0, 2, 4, 6, 8, \to\}, 8) = \{0, 2, 4, 6, 9, 11, 13, 15\}$, $\mathrm{Ap}(\{0, 3, 5, 6, 8, \to\}, 8) = \{0, 3, 5, 6, 9, 10, 12, 15\}$ *and* $\mathrm{Ap}(\{0, 4, 5, 6, 8, \to\}, 8) = \{0, 4, 5, 6, 9, 10, 11, 15\}$.

https://doi.org/10.3390/axioms15010036

- $\theta(\{0,2,4,6,8,\rightarrow\}) = \emptyset$, $\theta(\{0,3,5,6,8,\rightarrow\}) = \emptyset$ *and* $\theta(\{0,4,5,6,8,\rightarrow\}) = \emptyset$.
- $\mathscr{R}(7) = \{\{0,8,\rightarrow\}, \{0,5,8,\rightarrow\}, \{0,6,8,\rightarrow\}, \{0,3,6,8,\rightarrow\}, \{0,4,6,8,\rightarrow\}, \{0,5,6,8,\rightarrow\}, \{0,2,4,6,8,\rightarrow\}, \{0,3,5,6,8,\rightarrow\}, \{0,4,5,6,8,\rightarrow\}\}$.

In ([1], Lemma 2.14), appears the following result:

Lemma 5. *Let S be a numerical semigroup. Then,* $\mathrm{g}(S) \geq \dfrac{\mathrm{F}(S)+1}{2}$.

For a given rational number q, consider the set $\lceil q \rceil = \min\{z \in \mathbb{Z} \mid q \leq z\}$. From Lemma 5, we can deduce the below result.

Proposition 11. *If $F \in \mathbb{N}\backslash\{0\}$, then the height of the tree $\mathrm{G}(\mathscr{R}(F))$ is less than or equal to* $F - \left\lceil \dfrac{F+1}{2} \right\rceil$.

It is clear that if F is odd, then $\langle 2, F+2\rangle \in \mathscr{R}(F)$ and $\mathrm{g}(\langle 2, F+2\rangle) = \dfrac{F+1}{2}$. Therefore, if F is odd, we achieve the equality in Proposition 11. However, the bound that appears in Proposition 11, in general, is not achieved when F is even, since if we consider the tree $\mathrm{G}(\mathscr{R}(6))$,

$$\begin{array}{c} \{0,7,\rightarrow\} \\ \uparrow 5 \\ \{0,5,7,\rightarrow\} \end{array}$$

its height is 1 and $6 - \left\lceil \dfrac{6+1}{2} \right\rceil = 2$.

5. Radical Numerical Semigroups with Fixed Multiplicity

A Frobenius pseudo-variety is a family $\mathscr{P}$ of numerical semigroups verifying the following conditions:

1. $\mathscr{P}$ has a maximum with respect to inclusion order.
2. If $\{S, T\} \subseteq \mathscr{P}$, then $S \cap T \in \mathscr{P}$.
3. If $S \in \mathscr{P}$ and $S \neq \max(\mathscr{P})$, then $S \cup \{\mathrm{F}(S)\} \in \mathscr{P}$.

Our first aim in this section will be to prove that if $m \in \mathbb{N}\backslash\{0\}$, then $\mathscr{R}_m = \{S \in \mathscr{R} \mid \mathrm{m}(S) = m\}$ is a Frobenius pseudo-variety.

Proposition 12. *If $m \in \mathbb{N}\backslash\{0\}$, then $\mathscr{R}_m$ is a Frobenius pseudo-variety.*

Proof. We are going to verify the conditions to be a Frobenius pseudo-variety as follows:

1. It is trivial to see that $\{0, m, \rightarrow\}$ is the maximum of $\mathscr{R}_m$.
2. If $\{S, T\} \subseteq \mathscr{R}_m$, then by Lemma 1, we know that $S \cap T$ is a numerical semigroup. By Proposition 1, we have $S \cap T \in \mathscr{R}$ and it is clear that $\mathrm{m}(S \cap T) = m$. Therefore, $S \cap T \in \mathscr{R}_m$.
3. If $S \in \mathscr{R}_m$ and $S \neq \{0, m, \rightarrow\}$, then $\mathrm{F}(S) > m$. By using Lemma 1, we deduce that $S \cup \{\mathrm{F}(S)\}$ is a numerical semigroup with multiplicity m. By Proposition 1, we know that $S \cup \{\mathrm{F}(S)\} \in \mathscr{R}$ and so $S \cup \{\mathrm{F}(S)\} \in \mathscr{R}_m$.

□

https://doi.org/10.3390/axioms15010036

It is evident that $\mathscr{R}_1 = \{\mathbb{N}\}$. In the next result we will see that if $m \in \mathbb{N}\backslash\{0,1\}$, then $\mathscr{R}_m$ is a set with infinite cardinality.

Proposition 13. *If $m \in \mathbb{N}\backslash\{0,1\}$, then $\mathscr{R}_m$ has infinite cardinality.*

Proof. If $m \in \mathbb{N}\backslash\{0,1\}$, then there is a positive prime p such that $p \mid m$. For all $l \in \mathbb{N}\backslash\{0\}$, denote by $\mathrm{S}(p,l,m) = \{0\} \cup \{m + kp \mid k \in \mathbb{N}\} \cup \{lm, \to\}$. It is clear that $\mathrm{S}(p,l,m) \in \mathscr{R}_m$ and $\mathrm{F}(\mathrm{S}(p,l,m)) = lm - 1$. Therefore, $\mathscr{R}_m$ is a set with infinite cardinality. □

Define the graph $\mathrm{G}(\mathscr{R}_m)$ in the following way: $\mathscr{R}_m$ is its set of vertices and $(S,T) \in \mathscr{R}_m \times \mathscr{R}_m$ is an edge if and only if $T = S \cup \{\mathrm{F}(S)\}$.

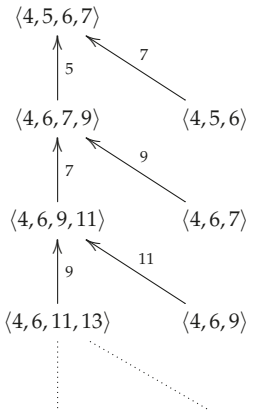
By applying Proposition 12 and ([38], Theorem 3), we obtain the following result:

Theorem 4. *If $m \in \mathbb{N}\backslash\{0,1\}$, then $\mathrm{G}(\mathscr{R}_m)$ is a tree and $\{0, m, \to\}$ is its root. Moreover, the set formed by the children of a vertex S of this tree is $\{S\backslash\{x\} \mid x \in \mathrm{msg}(S), x > \mathrm{F}(S)$ and $S\backslash\{x\} \in \mathscr{R}_m\}$.*

By applying Lemma 2 and Proposition 2, it is easy to deduce the following result:

Proposition 14. *Let $S \in \mathscr{R}_m$ and $x \in \mathrm{msg}(S)$. Then, $S\backslash\{x\} \in \mathscr{R}_m$ if and only if $x \neq m$ and $s + \mathrm{r}(s) \neq x$ for all $s \in S$ such that $\frac{x}{2} \leq s < x$.*

By using the comment after Proposition 2, Theorem 4 and Proposition 14, we can recurrently build the tree $\mathrm{G}(\mathscr{R}_4)$ shown below,



The number x appearing on the edge $\begin{array}{c} P \\ \uparrow x \\ Q \end{array}$ signifies that $Q = P\backslash\{x\}$. Furthermore, note that $\mathrm{F}(Q) = x$. The ellipsis signifies that the tree continues indefinitely.

By applying Proposition 13 and that $\{0, m, \to\}$ is the maximum of $\mathscr{R}_m$, we can easily deduce the next result.

Proposition 15. *If $m \in \mathbb{N}\backslash\{0,1\}$, then $\{\mathrm{g}(S) \mid S \in \mathscr{R}_m\} = \{m-1, \to\}$.*

Applying all the previous results, we can now show an algorithm that allows us to obtain all the elements of $\mathscr{R}_m$ with a given genus.

https://doi.org/10.3390/axioms15010036

Algorithm 4 Computation of $\{S \in \mathscr{R}_m \mid \mathrm{g}(S) = g\}$

INPUT: $m \in \mathbb{N}\backslash\{0,1\}$ and $g \in \{m-1, \to\}$.
OUTPUT: $\{S \in \mathscr{R}_m \mid \mathrm{g}(S) = g\}$.

(1) $A = \{\{0, m, \to\}\}$, $i = m-1$.
(2) If $i = g$, then return A and stop.
(3) For every $S \in A$ computes $\gamma(S) = \{x \in \mathrm{msg}(S)\backslash\{m\} \mid x > \mathrm{F}(S) \text{ and } s + \mathrm{r}(s) \neq x \text{ for all } s \in S, \frac{x}{2} \leq s < x\}$.
(4) $A = \bigcup_{S \in A} \{S\backslash\{x\} \mid x \in \gamma(S)\}$, $i = i+1$ and go to Step (2).

We finish the paper showing how the previous algorithm works.

Example 5. *We are going to compute the set* $\{S \in \mathscr{R}_4 \mid \mathrm{g}(S) = 5\}$*, by using Algorithm 4 as follows:*

- $A = \{\langle 4,5,6,7\rangle\}$, $i = 3$.
- $\gamma(\langle 4,5,6,7\rangle) = \{5,7\}$.
- $A = \{\langle 4,6,7,9\rangle, \langle 4,5,6\rangle\}$, $i = 4$.
- $\gamma(\langle 4,6,7,9\rangle) = \{7,9\}$ *and* $\gamma(\langle 4,5,6\rangle) = \emptyset$.
- $A = \{\langle 4,6,9,11\rangle, \langle 4,6,7\rangle\}$, $i = 5$.
- $\{S \in \mathscr{R}_4 \mid \mathrm{g}(S) = 5\} = \{\langle 4,6,9,11\rangle, \langle 4,6,7\rangle\}$.

6. Conclusions

In this work, and encouraged by some results from Number Theory and, in particular, the abc conjecture, we introduce the concept of a radical numerical semigroup.

We have proven that the set formed by all radical numerical semigroups is a Frobenius variety, and, as a consequence, we give an algorithm that computes all radical numerical semigroups with a given genus.

The paper also demonstrates that the set of radical numerical semigroups with Frobenius number F forms a covariety. Leveraging this fact, we develop an algorithm that computes all the radical numerical semigroups having F as their Frobenius number.

We have shown that the set formed by all the radical numerical semigroups of multiplicity m is a pseudo-Frobenius variety. This fact has allowed us to present an algorithm that computes all the radical numerical semigroups with fixed multiplicity and genus.

If $X \subseteq \mathbb{N}$ and $\gcd(X) = 1$, then in this work, we prove that there exists the smallest (with respect to inclusion order) radical numerical semigroup containing X. Furthermore, we have given an algorithm for obtaining such a numerical semigroup.

Finally, we have linked the study carried out with two important conjectures current in the theory of numerical semigroups: Wilf's conjecture and Bras-Amorós conjecture. Specifically, we have left open the question of whether the family of radical numerical semigroups satisfies these conjectures.

Author Contributions: The authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No public involvement in any aspect of this research.

Acknowledgments: The authors would like to thank the referees for their valuable comments and suggestions that helped to improve this work. This work has been partially supported by ProyExcel_00868 and by Junta de Andalucía groups FQM-298 and FQM-343.

Conflicts of Interest: The authors declare no conflicts of interest.

https://doi.org/10.3390/axioms15010036

References

1. Rosales, J.C.; García-Sánchez, P.A. *Numerical Semigroups*; Springer: New York, NY, USA, 2009; Volume 20.
2. Brauer, A. On a problem of partitions. *Am. J. Math.* **1942**, *64*, 299–312. [CrossRef]
3. Brauer, A.; Schockley, J.E. On a problem of Frobenius. *J. Reine Angew. Math.* **1962**, *211*, 215–220.
4. Curtis, F. On formulas for the Frobenius number of a numerical semigroup. *Math. Scand.* **1990**, *67*, 190–192. [CrossRef]
5. Davison, J.L. On the linear Diophantine problem of Frobenius. *J. Number Theory* **1994**, *48*, 353–363. [CrossRef]
6. Djawadi, M.; Hofmeister, G. Linear Diophantine problem. *Arch. Math.* **1996**, *66*, 19–29. [CrossRef]
7. Johnson, S.M. A linear diophantine problem. *Can. J. Math.* **1960**, *12*, 390–398. [CrossRef]
8. Selmer, E.S. On a linear diophantine problem. *J. Reine Angew. Math.* **1977**, *293/294*, 1–17.
9. Sylvester, J.J. Mathematical questions with their solutions. *Educ. Times* **1884**, *41*, 21.
10. Barucci, V.; Dobbs, D.E.; Fontana, M. Maximality Properties in Numerical Semigroups and Applications to One-Dimensional Analitycally Irreducible Local Domains. *Mem. Am. Math. Soc.* **1997**, *598, 1–78.*
11. Bertin, J.; Carbonne, P. Semi-groupes d'entiers et application aux branches. *J. Algebra.* **1977**, *49*, 81–95. [CrossRef]
12. Castellanos, J. A relation between the sequence of multiplicities and the semigroups of values of an algebroid curve. *J. Pure Appl. Algebra* **1986**, *43*, 119–127. [CrossRef]
13. Delorme, C. Sous-monoïdes d'intersection complète de $\mathbb{N}$. *Ann. Sci. École Norm. Super.* **1976**, *9*, 145–154. [CrossRef]
14. Fröberg, R.; Gottlieb, G.; Häggkvist, R. On numerical semigroups. *Semigroup Forum* **1987**, *35*, 63–83. [CrossRef]
15. Kunz, E. The value-semigroup of a one-dimensional Gorenstein ring. *Proc. Am. Math. Soc.* **1973**, *25*, 748–751. [CrossRef]
16. Teissier, B. *Appendice "Le Probléme des Modules Pour le Branches Planes", Course Donné par O. Zariski au Centre de Math*; Hermann, Éditeurs Dessciences et des Arts; de L'École Polytechnique: Paris, France, 1973.
17. Watanabe, K. Some examples of one dimensional Gorenstein domains. *Nagoya Math. J.* **1973**, *49*, 101–109. [CrossRef]
18. Ramírez Alfonsín, J.L. *The Diophantine Frobenius Problem*; Oxford University Press: London, UK, 2005.
19. Sylvester, J.J. Problem 7382. In *Educational Times and Journal of the College of Preceptors*; New Ser; C.F. Hodgson & Son: Harrow, UK, 1883; Volume 36, p. 177.
20. Wilf, H.S. A circle-of-lights algorithm for the "money-change problem". *Am. Math. Mon.* **1978**, *85*, 562–565.
21. Delgado, M. *Conjeture of Wilf: A Survey Numerical Semigroups*; Springer INdAM Series; Springer: Berlin/Heidelberg, Germany, 2018; Volume 40, pp. 39–62. [CrossRef]
22. Delgado, M.; Eliahou, S.; Fromentin, A. A verification of Wilf's conjeture up to genus 100. *J. Algebra* **2025**, *664*, 150–163. [CrossRef]
23. Eliahou, S. Wilf's conjeture and Macaulay's Theorem. *J. Eur. Math. Soc.* **2018**, *20*, 2105–2129. [CrossRef]
24. Eliahou, S. A graph-theoretic approach to Wilf's conjeture. *Electron. J. Comb.* **2020**, *27*, 15–31.
25. Eliahou, S.; Fromentin, J. Near-misses in Wilf's conjeture. *Semigroup Forum* **2019**, *98*, 285–298. [CrossRef]
26. Bras-Amorós, M. Bound on the number of numerical semigroups of a given genus. *J. Pure Appl. Algebra* **2008**, *213*, 997–1001. [CrossRef]
27. Bras-Amorós, M. Fibonacci-like behavior of the number of numerical semigroups of a given genus. *Semigroup Forum* **2008**, *76*, 379–384. [CrossRef]
28. Elizalde, S. Improved bounds on the number of numerical semigroup of a given genus. *J. Pure Appl. Algebra* **2010**, *214*, 1862–1873. [CrossRef]
29. Kaplan, N. Counting numerical semigroups by genus and some cases of a question of Wilf. *J. Pure Appl. Algebra* **2012**, *216*, 1016–1032. [CrossRef]
30. Blanco, V.; Rosales, J.C. The set of numerical semigroups of a given genus. *Semigroup Forum* **2012**, *85*, 255–267. [CrossRef]
31. Zhai, A. Fibonacci-like growth of numerical semigroups with a given genus. *Semigroup Forum* **2013**, *86*, 634–662. [CrossRef]
32. Baker, A. Experiments on the abc-conjecture. *Publ. Math. Debr.* **2012**, *65*, 253–260. [CrossRef]
33. Nitaj, A. La conjecture abc. *Enseign. Math.* **1996**, *42*, 3–24.
34. Oesterlé, J. Nouvelles approches du théorème de Fermat. *Astérisque Séminaire Bourbaki exp 694* **1988**, *161*, 165–186.
35. Pasten, H.; Sepúlveda-Manzo, R. On the abc and the abcd conjectures. *Bull. Braz. Math. Soc.* **2025** *56*, 54. [CrossRef]
36. Rosales, J.C. Families of numerical semigroups closed under finite intersection and for the Frobenius number. *Houst. J. Math.* **2008**, *34*, 339–348.
37. Moreno-Frías, M.A.; Rosales, J.C. The The covariety of numerical semigroups with fixed Frobenius number. *J. Algebr. Comb.* **2024**, *60*, 555–568. [CrossRef]
38. Robles-Pérez, A.M.; Rosales, J.C. Frobenius pseudo-varieties in numerical semigroups. *Ann. Mat. Pura Appl.* **2015**, *194*, 275–287. [CrossRef]
39. Delgado, M.; García-Sánchez, P.A.; Morais, J. *NumericalSgps, A Package for Numerical Semigroups*, Version 1.3.1; Refereed GAP Package. 2022. Available online: https://gap-packages.github.io/numericalsgps (accessed on 25 October 2025).

https://doi.org/10.3390/axioms15010036

40. The GAP Group. *GAP–Groups, Algorithms, and Programming*, Version 4.15.1. 2025. Available online: https://www.gap-system.org (accessed on 25 October 2025).
41. Apéry, R. Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris* **1946**, *222*, 1198–2000.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

MDPI AG
Grosspeteranlage 5
4052 Basel
Switzerland
Tel.: +41 61 683 77 34

Axioms Editorial Office
E-mail: axioms@mdpi.com
www.mdpi.com/journal/axioms



Disclaimer/Publisher's Note: The title and front matter of this reprint are at the discretion of the Guest Editor. The publisher is not responsible for their content or any associated concerns. The statements, opinions and data contained in all individual articles are solely those of the individual Editor and contributors and not of MDPI. MDPI disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.





Academic Open
Access Publishing

mdpi.com

ISBN 978-3-7258-8066-9