CONGRUENCE LATTICES OF FINITE UNARY ALGEBRAS

By

Supharat Thiranantanakorn

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics

Graduate School

SILPAKORN UNIVERSITY

2009

CONGRUENCE LATTICES OF FINITE UNARY ALGEBRAS

By

Supharat Thiranantanakorn

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics

Graduate School

SILPAKORN UNIVERSITY

2009

แลตทิซคอนกรูเอนซ์ของพีชคณิตเอกนามจำกัด

โดย
นางสาวสุภารัตน์ ถิรนันทนากร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2552

The Graduate School, Silpakorn University has approved and accredited the Thesis title of "Congruence Lattices of Finite Unary Algebras" submitted by Miss Supharat Thiranantanakorn as a partial fulfillment of the requirements for the degree of Master of Science in Mathematics

……..

(Associate Professor Sirichai Chinatangkul, Ph.D.)

Dean of Graduate School

........../..................../..........

The Thesis Advisor

Professor Chawewan Ratanaprasert, Ph.D.

The Thesis Examination Committee

.... Chairman

(Associate Professor Nawarat Ananchuen, Ph.D.)

............/......................../.............

.... Member

(Associate Professor Pattanee Udomkavanich, Ph.D.)

............/......................../.............

.... Member

(Professor Chawewan Ratanaprasert, Ph.D.)

............/......................../.............

49305208 : MAJOR : MATHEMATICS
KEY WORDS : CONGRUENCE LATTICES / FINITE UNARY ALGEBRAS / CONGRUENCE DISTRIBUTIVE / CONGRUENCE MODULAR

SUPHARAT THIRANANTANAKORN : CONGRUENCE LATTICES OF FINITE UNARY ALGEBRAS. THESIS ADVISOR : PROF.CHAWEWAN RATANAPRASERT,Ph.D. 55 pp.

For a finite set A, let f be a unary operation on A and let $\lambda(f)$ denote the least non-negative integer with $\operatorname{Im} f^{\lambda(f)} = \operatorname{Im} f^{\lambda(f)+1}$. We call $\lambda(f)$ the pre-period of f. Denecke and Wismath [3] have characterized all unary operations f on a finite set A with $\lambda(f) = |A| - 1$ and have proved that $\lambda(f) = |A| - 1$ if and only if there exists a $d \in A$ such that $A = \{d, f(d), \ldots, f^{n-1}(d)\}$. Furthermore, C.Ratanaprasert and K.Denecke [9] have characterized all unary operations f on a finite set A with $\lambda(f) = |A| - 2$ for all finite sets A with $|A| \geq 3$; and by the form of all elements in a finite set A which classifies by $\lambda(f)$, C.Ratanaprasert and K.Denecke [9] have characterized all equivalence relations on A which are invariant under a unary operation f with $\lambda(f) = |A| - 1$ and $\lambda(f) = |A| - 2$.

In this thesis, we study finite unary algebras $(A; f)$ with $\lambda(f) = 0$ and $\lambda(f) = 1$ for $|A| \geq 3$ which are called symmetric algebras and near-symmetric algebras, respectively. We characterize all unary operations f whose $(A; f)$ is congruence distributive and congruence modular. And also, we characterize all congruence modular symmetric and near-symmetric algebras by proving that:

1. A symmetric algebra $(A; f)$ is congruence modular if and only if the lattice of all congruence relations on $(A; f)$ is either a product of chains or a linear sum of a product of chains with one element chain or a M_3- head lattice.

2. A near-symmetric algebra $(A; f)$ is congruence modular if and only if the lattice of all congruence relations on $(A; f)$ is one of the following forms:

$\underline{2} \times P$ or $\underline{2} \times (P \oplus \underline{1})$ or $\underline{2} \times L$ or
$M_3 \times P$ or $M_3 \times (P \oplus \underline{1})$ or $M_3 \times L$

where P is a product of chains and L is a M_3- head lattice.

Department of Mathematics Graduate School, Silpakorn University Academic Year 2009

Student's signature ....

Thesis Advisor's signature ....

49305208 : สาขาวิชาคณิตศาสตร์

คำสำคัญ : แลตทิซคอนกรูเอนซ์ / พีชคณิตเอกนามจำกัด / พีชคณิตสมภาคแจกแจง / พีชคณิตสมภาค มอดุล่าร์

สุภารัตน์ ถิรนันทนากร : แลตทิซคอนกรูเอนซ์ของพีชคณิตเอกนามจำกัด. อาจารย์ที่ปรึกษาวิทยานิพนธ์ : ศ.ดร.ฉวีวรรณ รัตนประเสริฐ. 55 หน้า.

สำหรับแต่ละเซตจำกัด A ให้ f แทนการดำเนินการเอกภาคบน A และให้ $\lambda(f)$ แทนจำนวนเต็มไม่เป็นลบน้อยสุดที่ทำให้ $\operatorname{Im} f^{\lambda(f)} = \operatorname{Im} f^{\lambda(f)+1}$ โดยเรียก $\lambda(f)$ ว่า pre-period ของ f Denecke และ Wismath [3] ได้ให้ลักษณะเฉพาะของการดำเนินการเอกภาค f บนเซตจำกัด A ซึ่ง $\lambda(f) = |A| - 1$ โดยพิสูจน์ว่า $\lambda(f) = |A| - 1$ ก็ต่อเมื่อ มีสมาชิก $d \in A$ ซึ่งทำให้ $A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\}$ นอกจากนี้ C. Ratanaprasert และ K. Denecke [9] ได้ให้ลักษณะเฉพาะของการดำเนินการเอกภาค f บนเซตจำกัด A ซึ่ง $\lambda(f) = |A| - 2$ สำหรับทุกเซตจำกัด A ซึ่ง $|A| \geq 3$ และด้วยลักษณะของสมาชิกในเซตจำกัด A ซึ่งจำแนกโดย $\lambda(f)$ C. Ratanaprasert และ K. Denecke [9] ได้ให้ลักษณะเฉพาะของความสัมพันธ์สมมูลซึ่งยืนยง f บนเซต A สำหรับ f ซึ่ง $\lambda(f) = |A| - 1$ และ $\lambda(f) = |A| - 2$

ในวิทยานิพนธ์นี้ เราศึกษาพีชคณิตเอกนามจำกัด $(A; f)$ ซึ่ง $\lambda(f) = 0$ และ $\lambda(f) = 1$ สำหรับ $|A| \geq 3$ โดยเรียกว่าพีชคณิตสมมาตรและพีชคณิตเกือบสมมาตรตามลำดับ โดยได้พิสูจน์ลักษณะเฉพาะของการดำเนินการเอกภาค f ที่ทำให้ $(A; f)$ เป็นพีชคณิตสมภาคแจกแจงและพีชคณิตสมภาคมอดุล่าร์ และได้จำแนกพีชคณิตสมมาตรและพีชคณิตเกือบสมมาตรทั้งหมดซึ่งเป็นพีชคณิตสมภาคมอดุล่าร์ โดยพิสูจน์ว่า

1. พีชคณิตสมมาตร $(A; f)$ เป็นพีชคณิตสมภาคมอดุล่าร์ ก็ต่อเมื่อแลตทิซคอนกรูเอนซ์ของ $(A; f)$ อยู่ในรูปผลคูณของโซ่หรือผลรวมเชิงเส้นของผลคูณของโซ่กับโซ่ขนาด 1 หรือแลตทิซ M_3 - head

2. พีชคณิตเกือบสมมาตร $(A; f)$ เป็นพีชคณิตสมภาคมอดุล่าร์ก็ต่อเมื่อแลตทิซคอนกรูเอนซ์ของ $(A; f)$ อยู่ในรูป

$\underline{2} \times P$ หรือ $\underline{2} \times (P \oplus \underline{1})$ หรือ $\underline{2} \times L$ หรือ

$M_3 \times P$ หรือ $M_3 \times (P \oplus \underline{1})$ หรือ $M_3 \times L$

โดยที่ P แทนผลคูณของโซ่ และ L แทนแลตทิซ M_3 - head

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2552

ลายมือชื่อนักศึกษา..

ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์ ....

Acknowledgements

This thesis has been completed by the involvement of people about whom I would like to mention here.

I would like to thank Prof. Dr. Chawewan Ratanaprasert, my advisor for her valuable suggestions and excellent advices throughout the study with great attention.

I would like to thank Ass. Prof. Dr. Nawarat Ananchuen and Ass. Prof. Dr. Pattanee Udomkavanich, Chairman and Member of the thesis Committee, for their valuable comments and suggestions.

Finally, I would like to express my gratitude to my family and my friends for their understanding, encouragement and moral support during the study.

Contents

List of Figures

Chapter 1

Introduction

An algebra is a pair consisting of a nonempty set A of objects and a set F of operations defined on A which are called **fundamental operations**. An algebra is finite if A is a finite set and every fundamental operation is finitary. Finite algebras are important in many branches where finiteness plays a crucial role; for instance, in computer science (computer can work only with finite set of data). An importance area of activity has been tried to classify all finite algebras; for example, classification of all finite groups is a longstanding but to now unsolved mathematical problem.

At the beginning of the eighties, R.McKenzie and D.Hobby [8] developed a new theory, called " Tame Congruence Theory " which offers a structure theory for finite algebras.

For a fixed finite set A, let $n := |A| \geq 2$ denote the cardinality of A. Let denote by H_A the set of all unary operations (transformations) defined on A and by S_A the set of all permutations defined on A. If $f : A \longrightarrow A$ is not a permutation, then $|A| > |Imf|$ and there is a least natural number $\lambda(f)$ with $Im^{\lambda(f)} = Im^{\lambda(f)+1}$. For $f \in H_A$, let $Imf := \{f(a)|\, a \in A\}$ be the image of f and let $\lambda(f)$ be the least non-negative integer m such that $Imf^m = Imf^{m+1}$. The number $\lambda(f)$ is called the **pre-period** of f, sometimes also the **stabilizer** of f. Denecke and Wismath [3] proved the followings:-
(i) $0 \leq \lambda(f) \leq |Imf|$ and $\lambda(f) \leq n-1$,
(ii) $\lambda(f) = 0$ if and only if f is a permutation on A,
(iii) $\lambda(f) = n-1$ if and only if there exists an element $d \in A$ such that

$$A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\} \text{ where } f^{n-1}(d) = f^n(d).$$

Note that Condition (iii) shows a characterization of all longest pre-periods f.

It is well-known that the congruence lattice of an algebra is uniquely determined by the unary polynomial operations of the algebra.

Let A be a finite set with $|A| = n$ and let f be a unary operation on A. We call $(A; f)$ a finite **unary algebra** and if $|Imf| = |A|$ or $|Imf| = 1$, then $(A; f)$ is called a **permutation algebra**. Permutation algebras play an important role in tame congruence theory. C. Ratanaprasert and K. Denecke [9] have characterized all unary operations f on a finite set A with $\lambda(f) = n-2$ for $n \geq 3$ and they also have characterized all equivalence relations on A which are invariant under a unary operation f with $\lambda(f) = n-1$ for $n \geq 2$ and $\lambda(f) = n-2$ for $n \geq 3$. For applications, they showed that every finite group which has a unary polynomial operation with one of these properties is simple or has only normal subgroup of index 2. The results convince us that those pre-period of unary functions defined on a finite set will be a kind of notions for classifications of finite algebras.

In the thesis, we are interested in formulating a characterization of all unary operations defined on a finite set A with pre-period $\lambda(f) = 0$ and $\lambda(f) = 1$.

In chapter 2, we collect some important basic concepts which will be used in the sequel.

In chapter 3, we study those results from C. Ratanaprasert and K. Denecke [9] which have characterized all unary operations f on a finite set A with $\lambda(f) = n-1$ for $n \geq 2$ and $\lambda(f) = n-2$ for $n \geq 3$ and they have also characterized all equivalence relations on A which are invariant under such unary operations.

In chapter 4 and 5, we define a symmetric algebra and a near-symmetric algebra to be a unary algebra $(A; f)$ with $\lambda(f) = 0$ and $\lambda(f) = 1$, respectively; and then we prove necessary and sufficient conditions of f whose symmetric and near-symmetric algebra are congruence distributive and congruence modular. We characterize all congruence modular symmetric and near-symmetric algebras by proving that:

1. a symmetric algebra $(A; f)$ is congruence modular if and only if the lattice of all congruence relations on $(A; f)$ is either a product of chains or a linear sum of a product of chains with one element chain or a M_3-head lattice.

2. A near-symmetric algebra is congruence modular if and only if the lattice of all congruence relations on $(A; f)$ is one of the following forms:

$$\underline{2} \times P \ \ or \ \ \underline{2} \times (P \oplus \underline{1}) \ \ or \ \ \underline{2} \times L$$

or

$$M_3 \times P \ \ or \ \ M_3 \times (P \oplus \underline{1}) \ \ or \ \ M_3 \times L$$

where P is a product of chains and L is a M_3-head lattice.

Chapter 2

Basic Concepts

In this chapter, we study related topics which will be referred in sequel. All theorems are stated without proofs.

2.1 Basic Concepts in Universal Algebras

In this section, we will give some important concepts in algebra which will be referred in the sequel.

Definition 2.1. *Let A be a set. A* **partition** $\wp$ *of A is a system not containing $\emptyset$, satisfying the property that: every $a \in A$ is an element of exactly one $B \in \wp$. The members of $\wp$ are called* **blocks** *of the partition $\wp$.*

Definition 2.2. *Let A be a set. For a positive integer n, an* **n-ary relation** r *on A is defined as a subset of A^n.*

Definition 2.3. *A binary relation θ on a set A is called an* **equivalence relation** *on A if the following three conditions hold for all $a, b, c \in A$:*
(i) $a\theta a$, *(reflexivity)*
(ii) $a\theta b$ *implies* $b\theta a$, *(symmetry)*
(iii) $a\theta b$ *and* $b\theta c$ *imply* $a\theta c$. *(transitivity)*

Lemma 2.4. *Let A be a finite set.*
(i) *If E is an equivalence relation on A, then the set A/E of all equivalence classes with respect to E is a partition of A.*
(ii) *If $\wp$ is a partition of A, then the relation* $E_\wp = \{(x, y) \in A \times A \mid x, y \in P$ for some $P \in \wp\}$ *is an equivalence relation on A.*

Definition 2.5. *Let A be a set and n be a non-negative integer. An* n**-ary operation** *on the set A is a mapping f from A^n into A. If f is a mapping from A into A we called f a* **unary operation** *on A. Moreover, f is called a* **permutation** *on A if f is bijective.*

Remark 2.6. [3] *Any n-ary operation f on A can be regarded as an $(n+1)$-ary relation defined on A, called* **graph** *of f. This relation is defined by* $\{(a_1, \ldots, a_{n+1}) \in A^{n+1} \mid f(a_1, \ldots, a_n) = a_{n+1}\}$.

Definition 2.7. *Let A be a non-empty set. Let I be some non-empty index set, and let $(f_i^A)_{i\in I}$ be a function which assigns to every element of I an n_i-ary operation f_i^A defined on A. Then the pair $\bar{A} = (A; (f_i^A)_{i\in I})$ is called an* **(indexed) algebra** *(indexed by set I). The set A is called the* **base** *or* **carrier set** *or* **universe** *of $\bar{A}$, and $(f_i^A)_{i\in I}$ is called the* **sequence of fundamental operations** *of $\bar{A}$. For each $i \in I$ the natural number n_i is called the* **arity** *of f_i^A. The sequence $\tau := (n_i)_{i\in I}$ of all the arities is called the* **type** *of the algebra $\bar{A}$.*

An algebra $\bar{A} = (A; f)$ of type $\tau = (1)$ with one unary operation is called a **unary algebra**.

Definition 2.8. *Let $\bar{B} = (B; (f_i^B)_{i\in I})$ be an algebra of type τ. Then an algebra $\bar{A}$ is called a* **subalgebra** *of $\bar{B}$, written as $\bar{A} \subseteq \bar{B}$, if the following conditions are satisfied:*
(i) *$\bar{A} = (A; (f_i^A)_{i\in I})$ is an algebra of type τ,*
(ii) *$A \subseteq B$,*
(iii) *for each $i \in I$, the graph of f_i^A is a subset of the graph of f_i^B.*

Remark 2.9. [3] *Condition* (iii) *of the Definition refers to the graph of an operation, as defined in Remark 2.6. This condition means that the graph of f_i^A is the* **restriction** *of the graph f_i^B to $A^{n_i} \subseteq B^{n_i}$. We write $f_i^A = f_i^B|_{A^{n_i}}$ for all $i \in I$, using $f_i^B|_{A^{n_i}}$, or just $f_i^B|_A$ to denote the restriction of f_i^B to A^{n_i}.*

Definition 2.10. *Let A be a set, let $\theta \subseteq A\times A$ be an equivalence relation on A, and let f be an n-ary operation on A. Then f is said to be* **compatible** *with θ, or to* **preserve** *θ or θ is* **invariant with respect to** *f, if for all $a_1, \dots, a_n, b_1, \dots, b_n \in A$,*

$$(a_1, b_1) \in \theta, \dots, (a_n, b_n) \in \theta \text{ implies } (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta.$$

Definition 2.11. *Let $\bar{A} = (A; (f_i^A)_{i\in I})$ be an algebra of type τ. An equivalence relation θ on A is called a* **congruence relation** *on $\bar{A}$ if all fundamental operations f_i^A are compatible with θ. We denote by $Con\,\bar{A}$ the set of all congruence relations of the algebra $\bar{A}$.*

For every algebra $\bar{A} = (A; (f_i^A)_{i\in I})$, the trivial equivalence relations

$$\Delta_A := \{(a, a) \mid a \in A\} \text{ and } \nabla_A := A \times A$$

are congruence relations.

Theorem 2.12. [3] *The intersection $\theta_1 \cap \theta_2$ of two congruence relations on an algebra $\bar{A} = (A; (f_i^A)_{i\in I})$ is again a congruence relation on $\bar{A}$.*

Remark 2.13. [3] *Theorem 2.12 is also satisfied for arbitrary families of congruence relations on $\bar{A}$. But in general, the union of two congruence relations of an algebra $\bar{A}$ is not a congruence relation, since this does not hold even for equivalence relations, as the following example shows. Let $A = \{1, 2, 3\}$. Define*

$$\theta_1 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\} \text{ and } \theta_2 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}.$$

The relations θ_1 *and* θ_2 *are equivalence relations, but*

$$\theta_1 \cup \theta_2 = \{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}$$

is not an equivalence relation on A *since it is not transitive:*

$$(1,2) \in \theta_1 \cup \theta_2 \text{ and } (2,3) \in \theta_1 \cup \theta_2 \text{ but } (1,3) \notin \theta_1 \cup \theta_2.$$

But although the union of two congruence relations θ_1 and θ_2 need not be a congruence relation, as in the subalgebra case we can use intersections of congruences to define a smallest congruence generated by the union. This motivates the following definition.

Definition 2.14. *Let* $\bar{A}$ *be an algebra and let* θ *be a binary relation on* A. *We define the congruence relation* $\langle\theta\rangle_{Con\ \bar{A}}$ *on* $\bar{A}$ *generated by* θ *to be the intersection of all congruence relations* θ' *on* $\bar{A}$ *which contain* θ*:*

$$\langle\theta\rangle_{Con\ \bar{A}} := \cap\{\theta' \mid \theta' \in Con\ \bar{A} \text{ and } \theta \subseteq \theta'\}.$$

2.2 Number Theory

In this section, we introduce and present some basic properties of a number theory.

Theorem 2.15. [4] **The Division Algorithm**
Let a *be an integer and* b *a positive integer. Then there exist unique integers* q *and* r *such that*

$$a = bq + r$$

where $0 \le r < b$.

In particular, if $r = 0$ then $a = bq$.

Definition 2.16. *Let* d *and* n *be integers where* $d \neq 0$. *We say that* d **divides** n *if there is an integer* k *such that* $n = dk$ *and denoted by* $d|n$.

Definition 2.17. *Let* a, b *and* m *be integers with* $m > 0$. *We say that* a **is congruence to** b **modulo** m, *and we write* $a \equiv b \pmod{m}$, *if* m *divides the difference* $a - b$*; that is,* $m|(a-b)$. *The number* m *is called the* **modulus of the congruence**.

In particular, $a \equiv 0 \pmod{m}$ if and only if $m|a$. Hence, $a \equiv b \pmod{m}$ if and only if $a - b \equiv 0 \pmod{m}$.
If $m \nmid (a-b)$ we write $a \not\equiv b \pmod{m}$) and say that a and b are incongruent mod m.

Theorem 2.18. [4] *Let* a *and* b *be integers and let* m *and* d *be positive integers. If* $a \equiv b \pmod{m}$ *and* $d|m$, *then* $a \equiv b \pmod{d}$.

Theorem 2.19. [4] *Congruence is an equivalence relation on the set of all integers. That is, we have*
(i) $a \equiv a \pmod{m}$, *(reflexivity)*
(ii) $a \equiv b \pmod{m}$ *implies* $b \equiv a \pmod{m}$, *(symmetry)*
(iii) $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$ *imply* $a \equiv c \pmod{m}$. *(transitivity)*

Theorem 2.20. [4] *For arbitrary integers a and b, $a \equiv b \pmod{m}$ if and only if a and b leave the same non-negative remainder when divided by m.*

Definition 2.21. *Let m be a positive integer. If $ab \equiv 1 \pmod{m}$ then both a and b are* **relatively prime** *to m; that is, $gcd(a, m) = 1$ and $gcd(b, m) = 1$.*

Definition 2.22. *Let m be a positive integer. For each integer a we define*

$$[a] = \{x \mid x \equiv a \pmod{m}\}.$$

In other words, $[a]$ is the set of all integers that are congruent to a modulo m. We call $[a]$ **residue class of** *a* **modulo** *m. Some people call $[a]$ the congruence class or equivalence class of a modulo m.*

Theorem 2.23. [4] *For $m > 0$ we have*

$$[a] = \{mq + a \mid q \in \mathbb{Z}\}.$$

The following properties of residue classes are easy consequences of the definition.

Theorem 2.24. [4] *For a given modulus $m > 0$, we have:*
(i) *$[a] = [b]$ if and only if $a \equiv b \pmod{m}$.*
(ii) *Two integers x and y are in the same residue class if and only if $x \equiv y \pmod{m}$.*
(iii) *There are exactly m distinct residue classes modulo m, namely*

$$[0], [1], [2], \ldots, [m-1].$$

Moreover, their union is the set of all integers.

Remark 2.25. [4] *Theorem 2.24* (iii) *shows that $\{[0], [1], [2], \ldots, [m-1]\}$ is a partition of integer, $\mathbb{Z}$.*

Definition 2.26. *We define*

$$\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\},$$

that is, $\mathbb{Z}_m$ is the set of all residue classes modulo m.

From Theorem 2.24 (iii), we have

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

and since no two of the residue classes $[0], [1], [2], \ldots, [m-1]$ are equal we see that $\mathbb{Z}_m$ has exactly m elements. If we choose

$$a_0 \in [0], a_1 \in [1], \ldots, [m-1]$$

then

$$[a_0] = [0], [a_1] = [1], \ldots, [a_{m-1}] = [m-1].$$

So, we have

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

Definition 2.27. *A set of m integers*

$$\{a_0, a_1, \ldots, a_{m-1}\}$$

is called a **complete residue system modulo** m *if*

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

Example 1. *For $m > 0$, the set*

$$\{0, 1, 2 \ldots, m-1\}$$

is a complete residue system modulo m.

Theorem 2.28. [4] *Let a and b be integers and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if a and b have the same least residue modulo m.*

2.3 Ordered Sets

In this section, we introduce and present some basic properties of an ordered set.

Definition 2.29. *Let P be a nonempty set. An* **order** *(or* **partial order***) on P is a binary relation $\leq$ on P satisfying the following three conditions for all $x, y, z \in P$,*
(i) $x \leq x$, *(reflexivity)*
(ii) $x \leq y$ *and* $y \leq x$ *imply* $x = y$, *(anti-symmetry)*
(iii) $x \leq y$ *and* $y \leq z$ *imply* $x \leq z$. *(transitivity)*

A set P equipped with an order relation $\leq$ is said to be an **ordered set** (or **partially ordered set**) and denoted by $(P; \leq)$. Some authors use the shorthand **poset**.

Example 2. *The set of all non-negative integers $\mathbb{N}_0$ with division form an ordered set which denoted by $(\mathbb{N}_0; |)$.*

Definition 2.30. *Let P be an ordered set. Then P is a* **chain** *if for all $x, y \in P$, either $x \leq y$ or $y \leq x$ (that is, if any two elements of P are comparable). Alternative names for a chain are* **linearly ordered set** *and* **totally ordered set**. *At the opposite extreme from a chain is an anti-chain. The ordered set P is an* **anti-chain** *if $x \leq y$ in P only if $x = y$.*

Let P be the n-element set $\{0, 1, 2, \ldots, n-1\}$. We write $\underline{n}$ to denote the chain obtained by giving P the order in which $0 < 1 < 2 < \ldots < n-1$ and $\bar{n}$ for P regarded as an anti-chain.

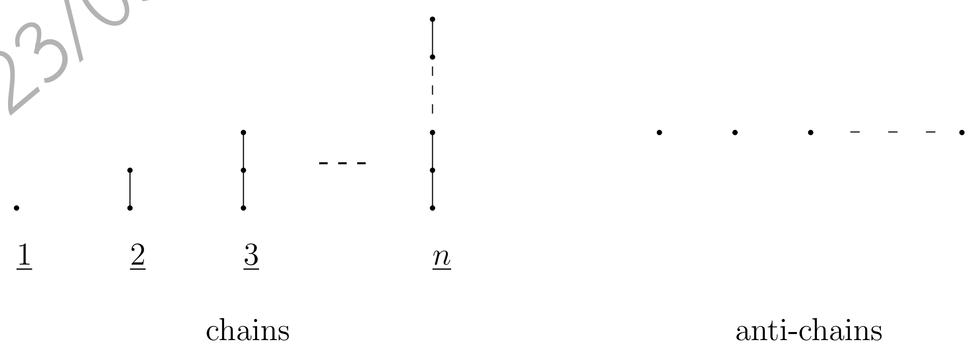


Figure 1. Chains and anti-chains

Definition 2.31. *Let P and Q be ordered sets. A map $\varphi : P \longrightarrow Q$ is said to be*
(i) **order-preserving** *(or, alternatively,* **monotone***) if $x \leq y$ in P implies $\varphi(x) \leq \varphi(y)$ in Q;*
(ii) *an* **order-embedding** *if $x \leq y$ in P if and only if $\varphi(x) \leq \varphi(y)$ in Q;*
(iii) *an* **order-isomorphism** *if it is an order-embedding mapping P onto Q.*

Whenever $\varphi : P \longrightarrow Q$ is an order-embedding we will write $\varphi : P \hookrightarrow Q$. And if there exists an order-isomorphism from P to Q, we say that P and Q are **order-isomorphic** and denote by $P \cong Q$.

Definition 2.32. *Let P be an ordered set and let $\varphi : P \longrightarrow P$ be a map. We say that $x \in P$ is a* **fixed point** *of φ if $\varphi(x) = x$.*

Remark 2.33. [2] (i) *An order-embedding is automatically a one-to-one mapping.*
(ii) *An order-isomorphism is bijective.*
(iii) *Ordered sets P and Q are order-isomorphic if and only if there exist order-preserving maps $\varphi : P \longrightarrow Q$ and $\psi : Q \longrightarrow P$ such that $\varphi \circ \psi = id_Q$ and $\psi \circ \varphi = id_P$ (where $id_S : S \longrightarrow S$ denotes the* **identity map** *on S given by $id_S(x) = x$ for all $x \in S$).*

Definition 2.34. *Let P be an ordered set and $Q \subseteq P$.*
(i) *Q is a* **down-set** *(alternative terms include* **decreasing set** *or* **order ideal***) if, whenever $x \in Q, y \in P$ and $y \leq x$, we have $y \in Q$.*
(ii) *Dually, Q is an* **up-set** *(alternative terms are* **increasing set** *or* **order filter***) if, whenever $x \in Q, y \in P$ and $y \geq x$, we have $y \in Q$.*

Given an arbitrary subset Q of P and $x \in P$, we define
$\downarrow Q = \{y \in P | (\exists x \in Q) y \leq x\}$ and $\uparrow Q = \{y \in P | (\exists x \in Q) y \geq x\}$,
$\downarrow x = \{y \in P | y \leq x\}$ and $\uparrow x = \{y \in P | y \geq x\}$.
These are read " down Q ", etc. It is easily checked that $\downarrow Q$ is the smallest down-set containing Q and that Q is a down-set if and only if $Q = \downarrow Q$, and dually for $\uparrow Q$. Clearly, $\downarrow \{x\} = \downarrow x$.

Definition 2.35. *Let P be an ordered set and $Q \subseteq P$. Then*
(i) *$a \in Q$ is a* **maximal** *element of Q if $a \leq x \in Q$ implies $a = x$;*
(ii) *$a \in Q$ is the* **greatest** *(or* **maximum***) element of Q if $a \geq x$ for every $x \in Q$, and in this case we write $a = maxQ$.*

Definition 2.36. *Let P and Q be ordered sets. The* **linear sum** *$P \oplus Q$ is defined by taking the following order relation on $P \cup Q : x \leq y$ if and only if*
(i) *$x, y \in P$ and $x \leq y$ in P,*
(ii) *$x, y \in Q$ and $x \leq y$ in Q,*
(iii) *$x \in P, y \in Q$.*

A diagram for $P \oplus Q$ is obtained by placing a diagram for P directly below a diagram for Q and then adding a line segment from each maximal element of P to each minimal element of Q. The lifting construction is a special case of a linear sum $1 \oplus P$. Similarly, $P \oplus 1$ represents P with a (new) top element added.

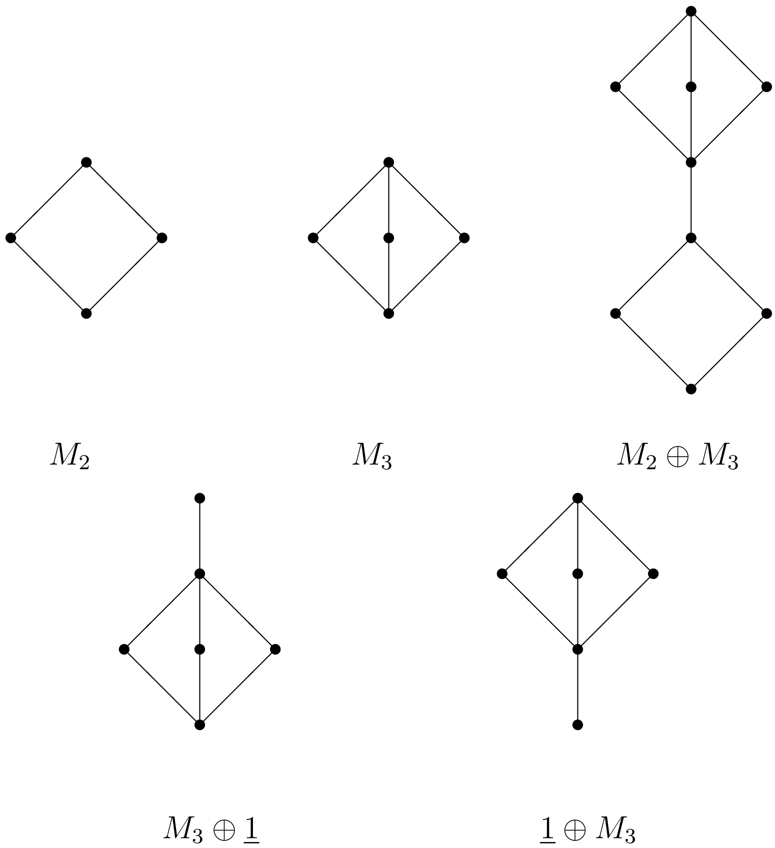
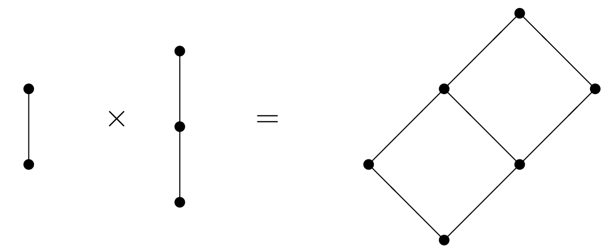


Figure 2. Linear sum

Definition 2.37. *Let $P_1, P_2, \ldots, P_n$ be ordered sets. The* **cartesian product** *$P_1 \times P_2 \times \ldots \times P_n$ can be made into an ordered set by imposing the coordinatewise order defined by*

$$(x_1, x_2, \ldots, x_n) \leq (y_1, y_2, \ldots, y_n) \Longleftrightarrow x_i \leq y_i \text{ in } P_i \text{ for all } i \in \{1, 2, \ldots, n\}.$$

Given an ordered set P, the notation P_n is used as shorthand for the n-fold product $P \times P \times \ldots \times P$.



$\underline{2}$ $\quad$ $\underline{3}$ $\quad$ $\underline{2} \times \underline{3}$

Figure 3. Some cartesian products

2.4 Lattices

It is a fundamental property of the real numbers, $\mathbb{R}$, that if I is a closed and bounded interval in $\mathbb{R}$, then every subset of I has both a least upper bound(or supremum) and a greatest lower bound(or infimum) in I. These concepts pertain to any ordered set.

Definition 2.38. *Let P be an ordered set and let $S \subseteq P$. An element $x \in P$ is an* **upper bound** *of S if $s \leq x$ for all $s \in S$. A* **lower bound** *is defined dually. The set of all upper bounds of S is denoted by S^u(read as 'S upper') and the set of all lower bounds of S is denoted by S^l(read as 'S lower'):*

$$S^u = \{x \in P | (\forall s \in S)\ s \leq x\} \text{ and } S^l = \{x \in P | (\forall s \in S)\ s \geq x\}.$$

If S^u has a least element, x, then x is called the **least upper bound** of S and is denoted by $supS$. Equivalently, x is the least upper bound of S if
(i) x is an upper bound of S, and
(ii) $x \leq y$ for all upper bound y of S.

Dually, if S^l has a largest element, x, then x is called the **greatest lower bound** of S or the **infimum** of S and is denoted by $infS$.
Notation: We write $\vee S$ instead of $supS$ whenever $supS$ exists, similarly we write $\wedge S$ instead of $infS$ whenever $infS$ exists.
Notation: We write $x \vee y$ (read as 'x joint y') in place of $sup\{x, y\}$ when it exists and $x \wedge y$ (read as 'x meet y') in place of $inf\{x, y\}$ when it exists.

Definition 2.39. *Let P be a non-empty ordered set.*
(i) *If $x \vee y$ and $x \wedge y$ exist for all $x, y \in P$, then P is called a* **lattice**.
(ii) *If $\vee S$ and $\wedge S$ exist for all $S \subseteq P$, then P is called a* **complete lattice**.

If P is a lattice, then $\vee$ and $\wedge$ can be considered as binary operations on P and we have an algebraic structure $(P; \vee, \wedge)$.
Recall that k is the greatest common divisor of m and n if
(i) k divides both m and n (that is, $k|m$ and $k|n$),
(ii) if l divides both m and n, then l divides k (that is, $l|k$ for all $k \in \{m, n\}^l$).
Thus the greatest common divisor of m and n is precisely the meet of m and n in $(\mathbb{N}_0; |\ )$. Dually, the join of m and n in $(\mathbb{N}_0; |\ )$ is given by their least common multiple. These statement remain valid when m or n equals 0. Thus $(\mathbb{N}_0; |\ )$ is a lattice in which

$$m \vee n = lcm\{m, n\} \text{ and } m \wedge n = gcd\{m, n\}.$$

Example 3. *Consider the ordered set $(\mathbb{N}_0; |\ )$ of non-negative integers ordered by division.*

Theorem 2.40. [3] *For every algebra $\bar{A}$, the structure $(Con\ \bar{A};\ \wedge, \vee)$ with*
$\wedge : Con\ \bar{A} \times Con\ \bar{A} \longrightarrow Con\ \bar{A}$ *define by* $(\theta_1, \theta_2) \longmapsto \theta_1 \cap \theta_2$,
$\vee : Con\ \bar{A} \times Con\ \bar{A} \longrightarrow Con\ \bar{A}$ *define by* $(\theta_1, \theta_2) \longmapsto \langle \theta_1 \cup \theta_2 \rangle_{Con\ \bar{A}}$
is a lattice, called the congruence lattice $Con(\bar{A})$ of $\bar{A}$.

Definition 2.41. *Let L be a lattice and $\emptyset \neq M \subseteq L$. Then M is a* **sublattice** *of L if $a, b \in M$ implies $a \vee b \in M$ and $a \wedge b \in M$.*

Definition 2.42. *Let L and K be lattices. Define $\vee$ and $\wedge$ coordinatewise on $L \times K$, as follows:*

$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee l_2, k_1 \vee k_2),$$
$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge l_2, k_1 \wedge k_2).$$

It is routine to check that $L \times K$ is a lattice. Also

$$\begin{aligned}(l_1, k_1) \vee (l_2, k_2) = (l_2, k_2) &\Longleftrightarrow l_1 \vee l_2 = l_2 \text{ and } k_1 \vee k_2 = k_2 \\ &\Longleftrightarrow l_1 \leq l_2 \text{ and } k_1 \leq k_2 \\ &\Longleftrightarrow (l_1, k_1) \vee (l_2, k_2), \text{ with respect to order on } L \times K.\end{aligned}$$

Definition 2.43. *Let L be a lattice with the greatest element 1 and let $c \in L$. We say that c is a* **co-atom** *of L if no elements $x \in L$ such that $c < x < 1$.*

Theorem 2.44. *Let L be a finite lattice. Then for each element $x \in L$, there exist a co-atom $a \in L$ such that $x \leq a$.*

Definition 2.45. *Let L and K be lattices. A map $f : L \longrightarrow K$ is said to be a* **homomorphism** *(or, for emphasis,* **lattice homomorphism***) if for all $a, b \in L$,*

$$f(a \vee b) = f(a) \vee f(b) \text{ and } f(a \wedge b) = f(a) \wedge \vee f(b).$$

A bijective homomorphism is a **(lattice-)isomorphism**.

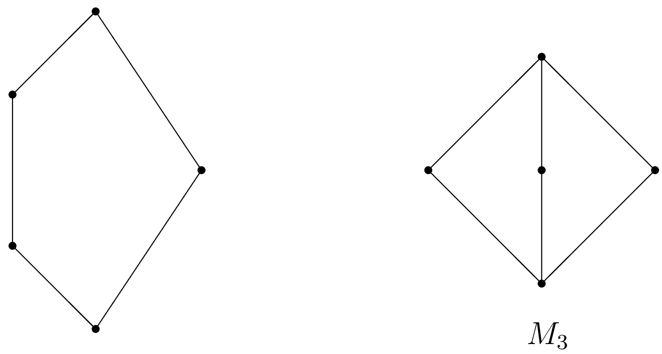
Definition 2.46. *Let L be a lattice.*
(i) *L is said to be* **distributive** *if it satisfies the distributive law,*

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \ \ for\ all\ \ a, b, c \in L.$$

(ii) *L is said to be* **modular** *if it satisfies the modular law,*

$$a \geq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c \ \ for\ all\ \ a, b, c \in L.$$

Theorem 2.47. [2] *The $M_3 - N_5$ Theorem.*
Let L be a lattice and let M_3 and N_5 be lattices as shown in Figure 4. Then
(i) *L is distributive if and only if L has no sublattices isomorphic to both N_5 and M_3.*
(ii) *L is modular if and only if L has no sublattices isomorphic to N_5.*



N_5 M_3

Figure 4. The $M_3 - N_5$

Lemma 2.48. [2] *Every chain is distributive.*

Theorem 2.49. [2] *If L is a distributive lattice, then L is a modular lattice.*

Proposition 2.50. [2]
(i) *If L is a modular (distributive) lattice, then every sublattice of L is modular (distributive).*
(ii) *If L is a modular (distributive) lattice and K is a lattice isomorphic to the lattice L, then K is modular (distributive).*
(iii) *If L and K are modular (distributive) lattices, then $L \times K$ is modular (distributive).*
(iv) *If L is a lattice isomorphic to a sublattice of a product of modular (distributive) lattice, then L is modular (distributive).*
(v) *If L is a modular (distributive) lattice and K is the image of L under a homomorphism, then K is modular (distributive).*

Definition 2.51. *Let $\bar{A}$ be an algebra.*
(i) *$\bar{A}$ is called* **congruence-distributive** *if its congruence lattice $Con(\bar{A})$ is distributive.*
(ii) *$\bar{A}$ is called* **congruence-modular** *if its congruence lattice $Con(\bar{A})$ is modular.*

Proposition 2.52. [2] *For each* $n \in \mathbb{N}$, *let* $n = p_1^{k_1}\, p_2^{k_2} \ldots p_r^{k_r}$ *where the* p_i *are pairwise distinct primes. Then*

$$\downarrow n \cong (k_1 \oplus 1) \times (k_2 \oplus 1) \times \ldots \times (k_r \oplus 1).$$

Chapter 3

Unary Algebras with Long Pre-periods

In 2002, K. Denecke and S.L. Wismath[3] have characterized all unary operations f on a finite set A with $\lambda(f) = |A| - 1$ and in 2007, C. Ratanaprasert and K. Denecke[9] have characterized all unary operations f on a finite set A with $\lambda(f) = |A| - 2$ and they have also characterized all equivalence relations on A which are invariant under a unary operation f with $\lambda(f) = |A| - 1$ and $\lambda(f) = |A| - 2$ which shown in the chapter.

3.1 Unary Operations with Long Pre-periods

In the section, we consider unary operations f on n - element set A with $\lambda(f) = n - 1$ and $\lambda(f) = n - 2$ and study some elementary properties.

Definition 3.1. *Let A be a finite set and let f be a unary operation on A. Then* **pre-period** (*or the stabilizer*) *of f is denoted by $\lambda(f)$, is the least non-negative integer such that $Imf^{\lambda(f)} = Imf^{\lambda(f)+1}$ where $f^0 = id_A$.*

Example 4. *Let $A = \{0, 1, 2, 3, 4, 5\}$ and let $f : A \longrightarrow A$ be defined on A by the following table:*

a	0	1	2	3	4	5
$f(a)$	1	2	3	4	2	4

Then, we have

	f	f^2	f^3
0	1	2	3
1	2	3	4
2	3	4	2
3	4	2	3
4	2	3	4
5	4	2	3

So, $Imf^2 = \{2, 3, 4\} = Imf^3$. It follows that the pre-period $\lambda(f) = 2$.

Lemma 3.2. [9] *Let A be a finite set with $|A| = n \geq 2$ and let f be a unary operation on A. Then*
(i) $Imf^{k+1} \subseteq Imf^k$ *for all integer* $k \geq 0$,
(ii) $0 \leq \lambda(f) \leq |Imf|$ *and* $\lambda(f) \leq n - 1$,
(iii) $\lambda(f) = 0$ *if and only if f is the permutation on A,*
(iv) $\lambda(f) = n - 1$ *if and only if there exists an element $d \in A$ such that*

$$A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\} \text{where} f^{n-1}(d) = f^n(d).$$

Proof. (i) Let k be a non-negative integer and $f^0 = id_A$. We will show that $Imf^{k+1} \subseteq Imf^k$. Let $y \in Imf^{k+1}$. Then there is a $x \in A$ such that $y = f^{k+1}(x) = f^k(f(x))$. Since f is a function from A into A and $x \in A$, we have $f(x) \in Imf \subseteq A$, it follows that $y \in Imf^k$. Hence $Imf^{k+1} \subseteq Imf^k$ for all integer $k \geq 0$.

(ii) Since $\lambda(f)$ is the least natural number such that $Imf^{\lambda(f)} = Imf^{\lambda(f)+1}$ and by part (i), we have $Imf^{k+1} \subset Imf^k$ for all $k \in \{0, 1, \ldots, \lambda(f) - 1\}$ and $0 \leq \lambda(f) \leq |Imf|$. If $Imf = A$, then $\lambda(f) = 0 < n - 1$. Assume that $Imf \subset A$. Then $|Imf| < |A| = n$. Thus $|Imf| \leq n - 1$, and so, $\lambda(f) \leq n - 1$.

(iii) Assume that $\lambda(f) = 0$. Then $A = Imid_A = Imf^0 = Imf^{0+1} = Imf$, which implies that f is surjective; and so, it is injective since A is finite. Hence f is bijective.

Conversely, assume that f is a permutation on A. Since f is onto, $Imf = A = Imid_A = Imf^0$. It follows that $\lambda(f) = 0$.

(iv) Assume that $\lambda(f) = n - 1$. Then $n - 1$ is the least natural number such that $Imf^{n-1} = Imf^n$. By the part (i), we have $Imf^{k+1} \subseteq Imf^k$ for $k \in \{0, 1, 2, \ldots\}$. If $Imf^{k+1} = Imf^k$ for some k, then by definition of preperiod of f we have $n - 1 \leq k$. Thus for $k < n - 1$, we have $Imf^{k+1} \subset Imf^k$. Since $Imf \subset A$, there is a $d \in A$ such that $d \notin Imf$ and $f^k(d) \in Imf^k$ for $k \in \{1, 2, \ldots, n - 1\}$. Therefore, $\{d, f(d), f^2(d), \ldots, f^{n-1}(d)\} \subseteq A$. Next, we want to show that $d, f(d), f^2(d), \ldots, f^{n-1}(d)$ are different. Suppose that there are integer i and j with $0 \leq i < j \leq n - 1$ such that $f^i(d) = f^j(d)$. Then $Imf^i = \{f^i(d), f^{i+1}(d), \ldots, f^{j-1}(d)\} = Imf^{i+1}$, which contradicts to the fact that $\lambda(f) = n - 1$. Therefore, $d, f(d), f^2(d), \ldots, f^{n-1}(d)$ are different. Since $|\{d, f(d), f^2(d), \ldots, f^{n-1}(d)\}| = n = |A|$, we have $\{d, f(d), f^2(d), \ldots, f^{n-1}(d)\} = A$. Also, since $Imf^{n-1} = Imf^n$, we get $f^{n-1}(d) = f^n(d)$.

Conversely, assume that $A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\}$ where $f^{n-1}(d) = f^n(d)$. Then $Imf^{n-1} = \{f^{n-1}(d)\} = \{f^n(d)\} = Imf^n$. It remain to show that $n - 1$ is the least natural number such that $Imf^{n-1} = Imf^n$. Suppose that there exists an integer $m < n - 1$ such that $Imf^m = Imf^{m+1}$. Since $A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\}$, we get $Imf^m = \{f^m(d), f^{m+1}(d), \ldots, f^{n-1}(d)\}$ and $Imf^{m+1} = \{f^{m+1}(d), f^{m+2}(d), \ldots, f^{n-1}(d)\}$. Also, since $Imf^m = Imf^{m+1}$, we get

$f^m(d) = f^k(d)$ for some integer k with $m+1 \leq k \leq n-1$, which is a contradiction. Therefore, $n-1$ is the least natural number such that $Imf^{n-1} = Imf^n$. Hence, $\lambda(f) = n-1$.

□

Definition 3.3. *A unary operation $f : A \longrightarrow A$ with $|A| = n \geq 2$ and $\lambda(f) = n-1$ is called a* **long-tailed function***, for short, LT-function.*

Note that Lemma 3.2 (iv) give a characterization of LT-functions.

Example 5. *Let $A = \{1, 2, 3, 4, 5\}$ and let $g : A \longrightarrow A$ be a unary operation defined by:*

a	1	2	3	4	5
$g(a)$	2	3	4	5	5

Then, we have

	g	g^2	g^3	g^4	g^5
1	2	3	4	5	5
2	3	4	5	5	5
3	4	5	5	5	5
4	5	5	5	5	5
5	5	5	5	5	5

So, $Img^4 = \{5\} = Img^5$. It follows that the pre-period $\lambda(g) = 4 = 5-1$. Therefore, g is a LT-function. By Lemma 3.2 (iv), there is $1 \in A$ such that

$$A = \{1, g(1), g^2(1), g^3(1), g^4(1)\}.$$

Definition 3.4. *Let A be a finite set with $|A| = n \geq 3$. Then a unary operation f defined on A with $\lambda(f) = n-2$ is said to be* LT_1**-function**.

The following lemma shows some properties of LT_1-function.

Lemma 3.5. [9] *Let A be a finite set with $|A| = n \geq 3$ and let f be a LT_1-function on A. Then the following properties are satisfied :*
(i) $A \supset Imf \supset Imf^2 \supset \ldots \supset Imf^{n-2}$,
(ii) $|Imf^k| = |Imf^{k+1}| + 1$ *for* $k = 1, \ldots, n-3$,
(iii) $|Imf^{n-2}| = 1$ *or* $|Imf^{n-2}| = 2$,
(iv) *if* $|Imf^{n-2}| = 1$, *then* $|A| = |Imf| + 2$,
(v) *if* $|Imf^{n-2}| = 2$, *then* $|A| = |Imf| + 1$.

Proof. (i) By Lemma 3.2(i), we have $A \supseteq Imf \supseteq Imf^2 \supseteq \ldots \supseteq Imf^{n-2}$. If $Imf^{k+1} = Imf^k$ for some $k \in \{0, 1, \ldots, n-2\}$, then the pre-period of f implies that $k = n-2$. Therefore, $A \supset Imf \supset Imf^2 \supset \ldots \supset Imf^{n-2}$.

(ii) By part (i), we have $|Imf^{k+1}| \leq |Imf^k| - 1$ for all $0 \leq k < n-2$. Thus $|Imf^{k+1}| + 1 \leq |Imf^k|$ for all $0 \leq k < n-2$. Suppose that there is an integer k

with $1 \leq k < n-2$ such that $|Imf^k| > |Imf^{k+1}|+1$. Then $|Imf^k| \geq |Imf^{k+1}|+2$. So, there are $a \neq b$ and $c \neq d$ in Imf^k such that $f(a) = f(b)$ and $f(c) = f(d)$ in Imf^{k+1}. Since $a, b, c, d \in Imf^k$ with $a \neq b$ and $c \neq d$, there are $x \neq y$ and $u \neq v$ in A such that $a = f^k(x), b = f^k(y), c = f^k(u)$ and $d = f^k(v)$. Thus $f^k(x) = a \neq b = f^k(y)$ and $f^k(u) = c \neq d = f^k(v)$ in A with $f(a) = f(b)$ and $f(c) = f(d)$ in Imf. Hence $|A| \geq |Imf| + 2$.
Therefore,

$$\begin{aligned}|A| &\geq |Imf| + 2 \geq |Imf^2| + 2 + 1 \geq \ldots \geq |Imf^k| + k + 1\\ &\geq |Imf^{k+1}| + 2 + k + 1\\ &\geq |Imf^{k+2}| + k + 2 + 2 \geq \ldots \geq |Imf^{n-2}| + (n-2) + 2\\ &\geq 1 + n - 2 + 2\\ &= n + 1\\ &> n,\end{aligned}$$

which is a contradiction. Thus $|Imf^{k+1}| + 1 \geq |Imf^k|$ for all $1 \leq k < n-2$. Hence, $|Imf^k| = |Imf^{k+1}| + 1$ for all $1 \leq k < n-2$.

(iii) Suppose that $|Imf^{n-2}| \geq 3$. Since $Imf \subset A$ and by part (ii), we have

$$\begin{aligned}|A| &\geq |Imf| + 1 = |Imf^2| + 2 = \ldots = |Imf^{n-2}| + (n-2)\\ &\geq 3 + (n-2) = n + 1 > n,\end{aligned}$$

which is a contradiction. Therefore, $|Imf^{n-2}| \leq 2$; that is, $|Imf^{n-2}| = 1$ or $|Imf^{n-2}| = 2$.

(iv) Assume that $|Imf^{n-2}| = 1$. Let $Imf^{n-2} = \{a\}$. By part (i) and part (ii), we get $|Imf^k| = |Imf^{k+1}|+1$ and $Imf^{k+1} \subset Imf^k$ for all $k \in \{1, 2, \ldots, n-3\}$. We claim that there are distinct elements $a_1, a_2, \ldots, a_{j-1}$ such that $Imf^{n-j} = \{a_1, a_2, \ldots, a_{j-1}\}$ for all $j = 2, 3, \ldots, n-1$. If $j = 2$, then $Imf^{n-2} = \{a\}$. Let m be a positive integer such that $m \geq 2$ and assume that there are distinct elements $a_1, a_2, \ldots, a_{m-1}$ such that $Imf^{n-m} = \{a_1, a_2, \ldots, a_{m-1}\}$. Since $Imf^{n-m} \subset Imf^{n-(m+1)}$, there is a $a_m \in Imf^{n-(m+1)}$ such that $a_m \notin Imf^{n-m}$. Also, since $Imf^{n-m} = \{a_1, a_2, \ldots, a_{m-1}\}$, it follows that $Imf^{n-(m+1)} = \{a_1, a_2, \ldots, a_{m-1}, a_m\}$ where $a_1, a_2, \ldots, a_{m-1}, a_m$ are distinct elements of $Imf^{n-(m+1)}$. Hence by mathematical induction, there are distinct elements $a_1, a_2, \ldots, a_{j-1}$ such that $Imf^{n-j} = \{a_1, a_2, \ldots, a_{j-1}\}$ for all $j = 2, 3, \ldots, n-1$. Therefore, $Imf = Imf^{n-(n-1)} = \{a_1, a_2, \ldots, a_{n-2}\}$ where $a_1, a_2, \ldots, a_{n-2}$ are distinct elements of A; so, $|Imf| = n - 2 = |A| - 2$. Hence, $|A| = |Imf| + 2$.

(v) Assume that $|Imf^{n-2}| = 2$. By part (i), we have $|Imf| < |A|$. Then $|Imf| \leq |A| - 1$; that is, $|Imf| + 1 \leq |A|$. Next, we claim that $|Imf^{n-k}| \geq k$ for $k = 2, 3, \ldots, n-1$. For $k = 2$, we have $|Imf^{n-2}| = 2$. Let m be a positive integer such that $m \geq 2$. Assume that $|Imf^{n-m}| \geq m$. Then $|Imf^{n-(m+1)}| \geq |Imf^{n-m}|+$

$1 = m+1$. Hence, by mathematical induction, $|Imf^{n-k}| \geq k$ for $k = 2, 3, \ldots, n-1$. So $|Imf| = |Imf^{n-(n-1)}| \geq n-1 = |A| - 1$; that is, $|Imf| + 1 \geq |A|$. Hence $|A| = |Imf| + 1$.

□

Remark 3.6. [9] *Let A be a finite set with $|A| = n \geq 3$ and let f be a LT_1-function on A with $|Imf^{n-2}| = 1$. Then*
(i) *$|A| = |Imf| + 2$; so, there are distinct elements $a, b, c, d \in A$ such that $f(a) = f(b) = s$ and $f(c) = f(d) = t$ in Imf.*
(ii) *if $n = 3$ or $s = t$ then $c = d$ and $f(a) = f(b) = f(c) = s$; and if $n \geq 4$ then $c \neq d$ if and only if $s \neq t$.*
(iii) *there are different elements $u, v \in A$ such that $f(t^{'}) \notin \{u, v\}$ for all $t^{'} \in A$; hence, the function $f|_{A\backslash\{a,b,c,d\}} : A\backslash\{a, b, c, d\} \longrightarrow A\backslash\{s, t, u, v\}$ is a bijection.*
(iv) *if $n = 3$, then f is a constant function.*

Lemma 3.7. [9] *Let A be a finite set with $|A| = n \geq 4$. Assume that f is a unary operation on A with $f(a) = f(b) = s$, $f(c) = f(d) = t$ where $a, b, c, d \in A$ and $|A| = |Imf| + 2$. If $s, t \notin \{a, b, c, d\}$ and either $f(s) \notin \{a, b, c, d\}$ or $f(t) \notin \{a, b, c, d\}$ then $|Imf^k| \geq 2$ for all $k \geq 1$.*

Proof. Suppose that $s, t \notin \{a, b, c, d\}$ and $f(s) \notin \{a, b, c, d\}$. Since $|A| = |Imf|+2$, there are two different elements $u, v \in A$ such that $u, v \notin Imf$. Thus $f|_{A\backslash\{a,b,c,d\}} : A\backslash\{a, b, c, d\} \longrightarrow A\backslash\{s, t, u, v\}$ is bijective. And since $s, t \notin \{a, b, c, d\}$, we get $f(s) \notin \{s, t, u, v\}$. Thus $f(s) \neq s$ and $\{s = f^0(s), f(s)\}$ is a two-element subset of Imf. Inductively, assume that $\{f^{k-1}(s), f^k(s)\}$ is a two-element subset of Imf^k. We consider the following cases:

Case 1: $f^k(s) \notin \{a, b, c, d\}$ and $f^{k-1}(s) \notin \{a, b, c, d\}$. Then by the injectivity of $f|_{A\backslash\{a,b,c,d\}}$ and $f^{k-1}(s) \neq f^k(s)$, we get $f^k(s) \neq f^{k+1}(s)$.

Case 2: $f^k(s) \notin \{a, b, c, d\}$ and $f^{k-1}(s) \in \{a, b, c, d\}$. Then $f^k(s) = f(f^{k-1}(s)) \in \{s, t\}$ and $f^{k+1}(s) = f(f^k(s)) \notin \{s, t\}$. Therefore, $f^k(s) \neq f^{k+1}(s)$.

Case 3: $f^k(s) \in \{a, b, c, d\}$. Then $f^{k+1}(s) \in \{s, t\}$. Since $s, t \notin \{a, b, c, d\}$, we have $f^k(s) \notin \{s, t\}$. Thus $f^k(s) \neq f^{k+1}(s)$.
It follows that $\{f^k(s), f^{k+1}(s)\} \subseteq Imf^{k+1}$ for all $k \geq 1$. Therefore, $|Imf^k| \geq 2$ for all $k \geq 1$.

□

Lemma 3.8. [9] *Let A be a finite set with $|A| = n \geq 3$ and let f be a unary operation on A with $f(a) = f(b) = s$ and $f(c) = f(d) = t$ where $a, b, c, d \in A$. Assume that $\lambda(f) = n-2$ and $|Imf^{n-2}| = 1$. Then*
(i) *if $s, t \notin \{a, b, c, d\}$, then either $f(s) \notin \{a, b, c, d\}$ or $f(t) \notin \{a, b, c, d\}$,*
(ii) *$s \in \{a, b, c, d\}$ or $t \in \{a, b, c, d\}$,*
(iii) *if $s \in \{a, b\}$ and $s \neq t$, there exists a positive integer m such that $f^m(c) \in \{a, b\}\backslash\{s\}$ and $\{c, d\} \cap \{u, v\} \neq \emptyset$ where $u, v \in A\backslash Imf$,*
(iv) *if $|A| \geq 4$ and $s = t = a$, then $\{u, v\} \neq \{b, c\}$ and $\{u, v\} \cap \{b, c\} \neq \emptyset$.*

Proof. (i) Suppose that $s, t \notin \{a, b, c, d\}$ and $f(s) \in \{a, b, c, d\}$. Then $f(s), f(t) \notin \{s, t\}$. If $f(s) \in \{a, b\}$ or $f(t) \in \{c, d\}$, then $f^2(s) = s$ or $f^2(t) = t$. That is $s \in Imf^{n-2}$ or $t \in Imf^{n-2}$. Thus $f(s) \neq s \in Imf^{n-2}$ or $f(t) \neq t \in Imf^{n-2}$. Therefore $|Imf^{n-2}| \geq 2$, a contradiction. Hence $f(s) \notin \{a, b\}$ and $f(t) \notin \{c, d\}$. If $f(s) \in \{c, d\}$ and $f(t) \in \{a, b\}$, then $f^2(s) = t$ and $f^2(t) = s$. Thus $f(f^2(c)) = f^2(a)$ and $f(f^2(a)) = f^2(c)$. Therefore $f^2(a)$ and $f^2(c)$ are two elements of A which are mapped to each other and thus they belong to Imf^k for all $k \geq 1$. Since $f(s) \neq f(t)$, we have $|Imf^{n-2}| \geq 2$, a contradiction. That is $f(s) \notin \{c, d\}$ or $f(t) \notin \{a, b\}$. Therefore $f(s) \notin \{a, b, c, d\}$ or $f(t) \notin \{a, b, c, d\}$.

(ii) Suppose that $s \notin \{a, b, c, d\}$ and $t \notin \{a, b, c, d\}$. By part (i), we get either $f(s) \notin \{a, b, c, d\}$ or $f(t) \notin \{a, b, c, d\}$. Thus by Lemma 3.7, we have $|Imf^k| \geq 2$ for all $k \geq 1$. It follows that $|Imf^{n-2}| \geq 2$, which is a contradiction. Therefore $s \in \{a, b, c, d\}$ or $t \in \{a, b, c, d\}$.

(iii) Assume that $s \in \{a, b\}$ and $s \neq t$. Since $c \in A$ and $|Imf^{n-2}| = 1$, we have $f^{n-2}(c) \in Imf^{n-2}$ and $f^{n-2}(c) = s$. Let r be the least positive integer such that $f^r(c) = s$. Then $1 < r \leq n-2$. Thus $1 \leq r-1 < n-2$ and $f^{r-1}(c) \in \{a, b\}$ (if $f^{r-1}(c) \notin \{a, b\}$, then $|Imf| \leq |A| - 3$, a contradiction). Since r is the least positive integer such that $f^r(c) = s$, we have $f^{r-1}(c) \in \{a, b\} \backslash \{s\}$ with $r - 1 \geq 1$. So, there exists a positive integer $m = r - 1$ such that $f^m(c) \in \{a, b\} \backslash \{s\}$.
Next, let $u, v \in A \backslash Imf$ and assume that $\{c, d\} \cap \{u, v\} = \emptyset$. Then $\{c, d\} \subseteq Imf$. Therefore, there are $p, q \in A$ such that $f(p) = c$ and $f(q) = d$. Since $a, b, c, d \in Imf$ with $f(a) = f(b)$ and $f(c) = f(d)$, it implies that $|Imf^2| \leq |Imf| - 2$. This is a contradiction. Hence $\{c, d\} \cap \{u, v\} \neq \emptyset$.

(iv) Assume that $|A| \geq 4$ and $s = t = a$. We want to show that $\{u, v\} \neq \{b, c\}$ and $\{u, v\} \cap \{b, c\} \neq \emptyset$. Suppose that $\{u, v\} = \{b, c\}$ or $\{u, v\} \cap \{b, c\} = \emptyset$.

Case 1: $\{u, v\} = \{b, c\}$. Then $A \backslash \{s, u, v\} = A \backslash \{a, b, c\}$ and $f|_{A \backslash \{a,b,c\}}$ is permutation on $A \backslash \{a, b, c\}$. Since $|A| \geq 4$, we have $|A \backslash \{a, b, c\}| \geq 1$ and $\emptyset \neq A \backslash \{a, b, c\} \subseteq Imf^k$ for $k \geq 1$. Since $a \in Imf^{n-2}$, we have $|Imf^{n-2}| \geq 2$, which is a contradiction.

Case 2: $\{u, v\} \cap \{b, c\} = \emptyset$. Then $\{b, c\} \subseteq Imf$. Thus there are elements $p, q \in A$ such that $f(p) = b \neq c = f(q)$, which implies that $\{f(a) = a, f(p) = b, f(q) = c\}$ is a subset of Imf. Since $f(a) = f(b) = s$, we get $f^2(a) = f(a) = s$ and $f^2(p) = f(b) = s$ and since $f(c) = t$ and $s = t$, we have $f^2(q) = f(c) = t = s$. Therefore $f^2(a) = f^2(p) = f^2(q) = s \in Imf^2$, which implies that $|Imf^2| \leq |Imf| - 2 < |Imf| - 1$, a contradiction.
Hence, $\{u, v\} \neq \{b, c\}$ and $\{u, v\} \cap \{b, c\} \neq \emptyset$.

$\square$

Theorem 3.9. [9] *Let A be a finite set with $|A| = n \geq 3$ and let f be an operation on A. Then f is a LT_1-function with $|Imf^{n-2}| = 1$ if and only if there are distinct* *elements* $u, v \in A$ *such that* $A = \{u, v, f(v), \ldots, f^{n-2}(v)\}$ *and there is an integer* k *with* $0 \leq k < n-2$ *such that* $f(u) = f^{k+1}(v)$ *and a number* m *with* $m + k = n-2$ *such that* $f^{m+1}(u) = f^m(u)$.

Proof. Assume that f is a LT_1-function with $|Imf^{n-2}| = 1$. Then Lemma 3.5 (iv) implies that $|A| = |Imf| + 2$. Thus there are two distinct elements $u, v \in A$ such that $u, v \notin Imf$. Let g be the restriction function of f on the $(n-2)$-element set Imf(i.e. $g = f|_{Imf} : Imf \longrightarrow A$) such that $|Im(f|_{Imf})^{n-3}| = |f^{n-3}(Imf)| = |Imf^{n-2}| = 1$. Thus $\lambda(f|_{Imf}) = \lambda(f) - 1 = (n-2) - 1 = |Imf| - 1$. Hence $f|_{Imf}$ is a LT-function. Then by Lemma 3.2 (iv), there is an element $d \in Imf$ such that $Imf = \{d, g(d), \ldots, g^{n-3}(d)\} = \{d, f|_{Imf}(d), \ldots, (f|_{Imf})^{n-3}(d)\}$ with $g^{n-3}(d) = g^{n-2}(d)$ and $d \notin Im(f|_{Imf}) = Imf^2$. Since $d \in Imf$, there is an element $q \in A$ such that $d = f(q)$. If $q \in Imf$, then $d \in Imf^2$, a contradiction. So, $q \notin Imf$ which implies that $q = v$ or $q = u$. Without loss of generality, let $q = v$. Since $u, v \notin Imf$, we get u cannot be mapped to u or v. Thus u is mapped to one of the elements $d, g(d), \ldots, g^{n-3}(d)$. Let $f(u) = g^k(d)$ for some k where $0 \leq k \leq n-3$. Since $d = f(q)$ and $q = v$, we have $d = f(v)$. Thus $g^k(d) = (f|_Imf)^k(d) = f^k(d) = f^k(f(v)) = f^{k+1}(v)$. Therefore, $f(u) = g^k(d) = f^{k+1}(v)$. Then $A = \{u, v, f(v), \ldots, f^{n-2}(v)\} = \{v, f(v), \ldots, f^k(v)\} \cup \{u, f(u), \ldots, f^m(u)\}$ with $m + k = n-2$. Since $|Imf^{n-2}| = 1$, we have $f^m(u) = f^{m+1}(u)$.

Conversely, assume that there are difference elements $u, v \in A$ such that $A = \{u, v, f(v), \ldots, f^{n-2}(v)\}$ and there is an exponent k with $0 \leq k < n-2$ such that $f(u) = f^{k+1}(v)$ and a number m with $m + k = n-2$ such that $f^{m+1}(u) = f^m(u)$. Then we can write $A = \{u, f(u), \ldots, f^m(u)\} \cup \{v, f(v), \ldots, f^k(v)\}$ where $m + k = n-2$, $f(u) = f^{k+1}(v)$ and $f^{m+1}(u) = f^m(u)$. Since $m + k = n-2$, all elements $u, v, f(u), \ldots, f^m(u), f(v), \ldots, f^k(v)$ are distinct. Thus, we have $a = f^m(u) \neq f^{m-1}(u) = b$ and $c = f^k(v) \neq u$. So $f(a) = f^{m+1}(u) = f^m(u) = f(b)$ and $f(c) = f^{k+1}(v) = f(u)$. Therefore $|A| = |Imf| + 2$. Thus $A \supset Imf$. And, by part (i) of Lemma 3.2, we have $A \supset Imf \supseteq Imf^2 \supseteq \ldots \supseteq Imf^{n-2}$.
We claim that $Imf^t \supset Imf^{t+1}$ for all $1 \leq t < n-2$.

Case 1: $m = 1$ and $k \geq 0$. Then $A = \{u, f(u)\} \cup \{v, f(v), \ldots, f^k(v)\}$.
If $k = 0$, then $A = \{v, u, f(u)\}$ and $Imf = \{f(u)\} \subset A$ with $n-2 = 1$.
If $k > 0$, then $f^k(v) \in Imf^s$ for all $1 \leq s \leq k$ with $n-2 = k+1$. Thus, for all $1 \leq t < n-2$, $f^t(v) \in Imf^t$ but $f^t(v) \notin Imf^{t+1}$. So, $Imf^{t+1} \subset Imf^t$ for all $1 \leq t < n-2$.

Case 2: $m > 1$ and $k \geq 0$. Then $f^{k+1}(v) = f(u)$. Thus $f^{m-1}(u) = f^{m-2}(f(u)) = f^{m-2}(f^{k+1}(v)) = f^{m+k-1}(v) = f^{n-3}(v) \in Imf^{n-3}$. Since $Imf^{n-3} \subseteq Imf^t$ for all $1 \leq t \leq n-3$, we have $f^{m-1}(u) \in Imf^t$ for all $1 \leq t < n-2$. Now, $f^{m-1}(u) \neq f^m(u)$ in Imf^t whereas $f(f^{m-1}(u)) = f(f^m(u))$ in Imf^{t+1} for all $1 \leq t < n-2$. It follows that $Imf^t \supset Imf^{t+1}$ for all $1 \leq t < n-2$, which complete the proof of the claim.
Therefore, $|Imf^t| \geq |Imf^{t+1}| + 1$ for all $1 \leq t < n-2$. Since $f^m(u) = f^{n-2}(u) \in$

Imf^{n-2}, we have $|Imf^{n-2}| \geq 1$. If $|Imf^{n-2}| \geq 2$, then we have

$$\begin{aligned}|A| &\geq |Imf| + 2 \geq |Imf^2| + 1 + 2 \geq \ldots \geq |Imf^{n-2}| + (n-3) + 2 \\ &\geq 2 + (n-3) + 2 \\ &= n + 1 \\ &> n,\end{aligned}$$

which is a contradiction. Thus $|Imf^{n-2}| \leq 1$. So, $|Imf^{n-2}| = 1$ which implies that $Imf^{n-2} = Imf^{n-2+t}$ for all $t \geq 1$. Thus $n-2$ is the least positive integer such that $Imf^{n-2} = Imf^{n-1}$; that is, $\lambda(f) = n-2$. Hence, f is a LT_1-function. □

Theorem 3.10. [9] *Let A be a finite set with $|A| = n \geq 3$ and let f be an operation on A. Then f is a LT_1-function with $|Imf^{n-2}| = 2$ if and only if there are different elements $u, v \in A$ such that either*
(i) $A = \{v, u, f(u), \ldots, f^{n-2}(u)\}$ *with* $v = f(v)$ *and* $f^{n-1}(u) = f^{n-2}(u)$,
or
(ii) $A = \{u, f(u), f^2(u), \ldots, v = f^{n-2}(u), f^{n-1}(u)\}$ *where* $v = f^n(u) = f^{n-2}(u)$.

Proof. Assume that f is a LT_1-function with $|Imf^{n-2}| = 2$. By Lemma 3.5 (v), we have $|A| = |Imf| + 1$. Thus there are exactly two distinct elements $a, b \in A$ such that $f(a) = f(b) = s \in Imf$ and there is an element $y \in A$ such that $y \notin Imf$. Then the mapping $f|_{A\backslash\{a,b\}} : A\backslash\{a,b\} \longrightarrow A\backslash\{s,y\}$ is bijective. We consider two cases $s \in \{a,b\}$ and $s \notin \{a,b\}$.

Case 1: $s \in \{a,b\}$. Without loss of generality, we may assume that $s = a$. Then $f(s) = f(a) = s \in Imf^{n-2}$. Now we consider two subcases $y \in \{a,b\}$ and $y \notin \{a,b\}$.

Subcase 1.1: $y \in \{a,b\}$. Since $y \neq s$, we have $y = b$, and so, $\{a,b\} = \{s,y\}$. Thus $f|_{A\backslash\{a,b\}}$ is a permutation, and so, $|A\backslash\{a,b\}| = |Imf|_{A\backslash\{a,b\}}| = |Im(f|_{A\backslash\{a,b\}})^{n-2}|$. Since $f|_{A\backslash\{a,b\}}$ is a permutation and $s \notin Imf|_{A\backslash\{a,b\}}$, we have $s \notin Im(f|_{A\backslash\{a,b\}})^{n-2}$. Since $s \notin Im(f|_{A\backslash\{a,b\}})^{n-2}$ and $s \in Imf^{n-2}$, we have $|Im(f|_{A\backslash\{a,b\}})^{n-2}| < |Imf^{n-2}|$. Also, since $|Imf^{n-2}| = 2$, we have $|A\backslash\{a,b\}| = |Imf|_{A\backslash\{a,b\}}| = |Im(f|_{A\backslash\{a,b\}})^{n-2}| < |Imf^{n-2}| = 2$; that is $|A\backslash\{a,b\}| \leq 1$. And, since $|A| \geq 3$, we get $|A\backslash\{a,b\}| \geq 1$. Thus $|A\backslash\{a,b\}| = 1$. So, $|A| = 3$ and there exists $c \in A\backslash\{a,b\}$ such that $f(c) = c$. Therefore, $A = \{c, y, f(y)\}$ where $f(c) = c$ and $f^2(y) = f(y)$. This corresponds to (i).

Subcase 1.2: $y \notin \{a,b\}$. Then $y \neq b$. Since $s = a$ and $a \neq b$, we get $s \neq b$. Thus $b \in A\backslash\{s,y\}$. By the surjectivity of $f|_{A\backslash\{a,b\}}$ onto $A\backslash\{s,y\}$ and the finiteness of A, we can choose $q-1$ pairwise distinct elements $x_1, x_2, \ldots, x_{q-1} \in A\backslash\{a,b,y\}$ and $x_q = y$ such that $f(x_i) = x_{i-1}$ for $1 < i \leq q$ with $f(x_1) = b$. Let $X = \{x_q = y, f(x_q), \ldots, f^q(x_q) = b, f^{q+1}(x_q) = a\}$. Then $X \subseteq A$. If $X = A$, then this give (i). Assume that $X \neq A$. Thus $A\backslash X \neq \emptyset$. It follows that $|A\backslash X| \geq 1$. Since $f|_{A\backslash\{a,b\}}$ is a bijection, $f|_{A\backslash X}$ is a permutation. Thus $|A\backslash X| = |Imf|_{A\backslash X}| = |Im(f|_{A\backslash X})^{n-2}| \leq |Imf^{n-2}|$. Since $s \in Imf^{n-2}$ and $s \notin Im(f|_{A\backslash X})^{n-2}$, we get $|Im(f|_{A\backslash X})^{n-2}| < |Imf^{n-2}|$. Also, since $|Imf^{n-2}| = 2$, we have $|A\backslash X| = |Imf|_{A\backslash X}| = |Im(f|_{A\backslash X})^{n-2}| < |Imf^{n-2}| = 2$; that is $|A\backslash X| \leq 1$. Thus $|A\backslash X| = 1$. So, there exists $c \in A\backslash X$ such that $f(c) = c$. Since $|X| = q+2$ and $|A\backslash X| = 1$, we have $|A| = q+3$. It follows that $A = \{c, y, f(y), \ldots, f^{q+1}(y)\}$ where $c \in A\backslash X$, $f(c) = c$ and $f^{q+2}(y) = f^{q+1}(y)$. This corresponds to (i).

Case 2: $s \notin \{a,b\}$. If $f(s) = s$, then $f(a) = f(b) = f(s) = s$, which implies that $|A| \geq |Imf| - 2$, a contradiction. Thus $f(s) \neq s$. We consider two subcases $f(s) \notin \{a,b\}$ and $f(s) \in \{a,b\}$.

Subcase 2.1: $f(s) \notin \{a,b\}$. Since $s \notin \{a,b\}$ and $f(s) \notin \{a,b\}$,we have $\{s, f(s)\} \subseteq A\backslash\{a,b\}$. For a positive integer $k \geq 1$, assume that $\{s, f(s), \ldots, f^k(s)\}$ is a subset of $A\backslash\{a,b\}$ of distinct elements. If $f^{k+1}(s) = f^t(s)$ for some $1 \leq t \leq k$, then by the injectivity of $f|_{A\backslash\{a,b\}}$, we have $f^k(s) = f^{t-1}(s)$ for some $0 \leq t-1 \leq k-1$, a contradiction. Thus $f^{k+1}(s) \neq f^t(s)$ for all integer t with $1 \leq t \leq k$. And, if $f^{k+1}(s) = s$, then $f^k(s) \in \{a,b\}$, a contradiction. Thus $f^{k+1}(s) \neq s$. Next, we assume that $f^{k+1}(s) \in \{a,b\}$. Without loss of generality we may assume that $f^{k+1}(s) = a$. If $b = y$, then $|A| \geq k+3$ and $Imf = A\backslash\{b\} = Imf^2$. It follows that $\lambda(f) = 1$. Since $\lambda(f) = n-2 = |A|-2$ and $|A| \geq k+3$, we have $\lambda(f) \geq (k+3)-2 = k+1 \geq 1+1 = 2$, a contradiction. If $b \neq y$, then $b \in A\backslash\{s,y\}$. By the surjectivity of $f|_{A\backslash\{a,b\}}$ onto $A\backslash\{s,y\}$, there is a $x_1 \in A\backslash\{a,b\}$ such that $f(x_1) = b$. If $x_1 = s$, then $f(s) = b$, a contradiction. Thus $x_1 \neq s$. If $x_1 = y$, then $f(y) = b$. Thus $|A| \geq k+4$ and $Imf^2 = A\backslash\{b,y\} = Imf^3$. So, $\lambda(f) = 2$. Since $\lambda(f) = n-2 = |A|-2$ and $|A| \geq k+4$, we have $\lambda(f) \geq (k+4)-2 = k+2 \geq 1+2 = 3$, a contradiction. Therefore, $x_1 \neq y$. It follows that $x_1 \in A\backslash\{s,y\}$. By the surjectivity of $f|_{A\backslash\{a,b\}}$ onto $A\backslash\{s,y\}$, there exists a $x_2 \in A\backslash\{a,b\}$ such that $f(x_2) = x_1$. If $x_2 = s$, then $f(s) = f(x_2) = x_1$, which implies that $f^2(s) = f(x_1) = b$, a contradiction. Thus $x_2 \neq s$. If $x_2 = y$, then $f(y) = x_1$. So, $|A| \geq k+5$ and $Imf^3 = A\backslash\{b,y,x_1\} = Imf^4$. Therefore, $\lambda(f) = 3$. Since $\lambda(f) = n-2 = |A|-2$ and $|A| \geq k+5$, we have $\lambda(f) \geq (k+5)-2 = k+3 \geq 1+3 = 4$, a contradiction. Thus $x_2 \neq y$. So, $x_2 \in A\backslash\{s,y\}$. Continuing in this way, since A is finite, there is integer q with $1 \leq q \leq n-2$ such that $y = x_q$ and $x_1, x_2, \ldots, x_{q-1} \in A\backslash\{a,b,y\}$ where $f(x_i) = x_{i-1}$ for all $1 < i \leq q$ and $f(x_1) = b$. Thus $|A| \geq k+q+3$ and $Imf^{q+1} = \{a, s, f(s), \ldots, f^k(s)\} = Imf^{q+2}$, which implies that $\lambda(f) = q+1$. Since $\lambda(f) = n-2 = |A|-2$ and $|A| \geq k+q+3$, we have $\lambda(f) \geq (k+q+3)-2 = k+q+1 > 1+(q+1)$, a contradiction. So, $f^{k+1}(s) \notin \{a,b\}$. Therefore, $X = \{s, f(s), \ldots, f^k(s), f^{k+1}(s) \ldots\}$ is a infinite subset of $A\backslash\{a,b\}$, which contradicts to the fact that A is finite.

Subcase 2.2: $f(s) \in \{a,b\}$. Without loss of generality, we may assume that $f(s) = a$. Since $f(a) = s$ and $f(s) = a$, we have $a, s \in Imf^{n-2}$. Also, since $|A| = |Imf| + 1$, we get $f(t) \notin \{a,s\}$ for all $t \notin \{a,b,s\}$.

If $y = b$, then $A\backslash\{a, b, s\} = A\backslash\{a, y, s\}$. Thus $f|_{A\backslash\{a,b,s\}}$ is a permutation, which implies that $|A\backslash\{a, b, s\}| = |Imf|_{A\backslash\{a,b,s\}}| = |Im(f|_{A\backslash\{a,b,s\}})^{n-2}| \leq |Imf^{n-2}| = 2$. Since $a, s \in Imf^{n-2}$ and $a, s \notin A\backslash\{a, b, s\}$, we have $|A\backslash\{a, b, s\}| = 0$. Thus $A = \{a, b, s\} = \{b, f(b) = s, f^2(b) = a\}$ where $f^3(b) = f(f^2(b)) = f(a) = s = f(b)$, this corresponds to (ii).
If $y \neq b$, then $b \in A\backslash\{y, s\}$. By the surjectivity of $f|_{A\backslash\{a,b\}}$ onto $A\backslash\{y, s\}$ and the finiteness of A, we may choose $q - 1$ pairwise distinct elements $x_1, x_2, \ldots, x_{q-1} \in A\backslash\{y, s, a, b\}$ and $x_q = y$ such that $f(x_i) = x_{i-1}$ for $1 < i \leq q$ with $f(x_1) = b$. Therefore, $X = \{x_q, f(x_q), \ldots, f^q(x_q) = b, f^{q+1}(x_q) = s, f^{q+2}(x_q) = a\} \subseteq A$. Since $f|_{A\backslash\{a,b\}}$ is a bijection, $f|_{A\backslash X}$ is a permutation. Thus $|A\backslash X| = |Imf|_{A\backslash X}| = |Im(f|_{A\backslash X})^{n-2}| \leq |Imf^{n-2}| = 2$. Since $a, s \notin A\backslash X$ but $a, s \in Imf^{n-2}$, we get $|A\backslash X| = 0$. Therefore, $A = X$ and $n = |A| = |X| = q + 3$; that is, $q = n - 3$. Let $u = x_q$. Then $A = \{u, f(u), \ldots, f^{n-1}(u)\}$ with $f^n(u) = f^{n-2}(u)$. This corresponds to (ii).

Conversely, let A be a finite set with $|A| = n \geq 3$ and let f be a unary operation on A satisfying either (i) or (ii).
In case (i), we have $f^{n-2}(u) \neq f^{n-3}(u)$ but $f(f^{n-2}(u)) = f^{n-1}(u) = f^{n-2}(u) = f(f^{n-3}(u))$ and in case (ii), we have $f^{n-1}(u) \neq f^{n-3}(u)$ but $f(f^{n-1}(u)) = f^n(u) = f^{n-2}(u) = f(f^{n-3}(u))$. Thus in either cases, we have $A \supset Imf$.

If $n = 3$, then either $A = \{v, u, f(u)\}$ where $f(v) = v$ and $f^2(u) = f(u)$ in case (i) or $A = \{u, v = f(u), f^2(u)\}$ where $v = f(u) = f^3(u)$ in case (ii). Thus in case (i), we have $Imf = \{v, f(u)\} = Imf^2$ and in case (ii), we have $Imf = \{f(u), f^2(u)\} = Imf^2$. So, in either cases, $\lambda(f) = 1 = 3 - 2$ and $|Imf| = 2$. Therefore, we may assume that $n \geq 4$. Now, we want to show that $A \supset Imf \supset Imf^2 \supset \ldots \supset Imf^{n-2}$. By Lemma 3.2 part (i) and $A \supset Imf$, we have $A \supset Imf \supseteq Imf^2 \supseteq \ldots \supseteq Imf^{n-2}$. In case (i), we have $f^{n-3}(u)$ and $f^{n-2}(u)$ are distinct elements in Imf^t which have the same image in Imf^{t+1} for all $1 \leq t \leq n-3$. Similarly, in case (ii), we have $f^{n-3}(u)$ and $f^{n-1}(u)$ are distinct elements in Imf^t having the same image in Imf^{t+1} for all $1 \leq t \leq n-3$. It follows that $|Imf^t| \geq |Imf^{t+1}| + 1$ which implies that $Imf^t \supset Imf^{t+1}$ for all $1 \leq t \leq n-3$. Next, we want to show that $|Imf^{n-2}| = 2$.

In case (i), v and $f^{n-2}(u)$ are distinct elements in Imf^{n-2}. So, $|Imf^{n-2}| \geq 2$. We want to show that $|Imf^{n-2}| \leq 2$. Assume that $|Imf^{n-2}| \geq 3$. Then
$|A| \geq |Imf| + 1 \geq \ldots \geq |Imf^{n-2}| + (n-2) \geq 3 + n - 2 = n + 1$, a contradiction. Thus $|Imf^{n-2}| \leq 2$. Hence, $|Imf^{n-2}| = 2$.

In case (ii), $f^{n-1}(u)$ and $f^{n-2}(u)$ are distinct elements in Imf^{n-2}.
So, $|Imf^{n-2}| \geq 2$. Similar to case (i), we have $|Imf^{n-2}| = 2$.
Finally, we want to show that $Imf^{n-2} = Imf^{n-1}$.
In case (i), we have v and $f^{n-2}(u)$ are the only two elements in Imf^{n-2} with $v = f(v)$ and $f^{n-1}(u) = f^{n-2}(u)$. Thus v and $f^{n-2}(u)$ are both in Imf^t for all $t \geq n-2$. Similarly, in case (ii), we have $f^{n-1}(u)$ and $f^{n-2}(u)$ are the only two elements in Imf^{n-2} with $f^n(u) = f^{n-2}(u)$. Thus $f^{n-1}(u)$ and $f^{n-2}(u)$ are both in Imf^t for all $t \geq n-2$. So, $Imf^{n-2} = Imf^{n-1}$. It follows that $n-2$ is the least

positive integer such that $Imf^{n-2} = Imf^{n-1}$. Therefore, $\lambda(f) = n-2$; that is f is a LT_1-function.

□

3.2 Invariant Equivalence Relation

Definition 3.11. *Let $\theta \subseteq A \times A$ be an equivalence relation on the finite set A with $|A| = n \geq 2$ and let f be an arbitrary unary operation defined on A. Then we say, f* **preserves** *θ or θ is* **invariant with respect to** *f if for each $a, b \in A$ such that $(a, b) \in \theta$, then $(f(a), f(b)) \in \theta$.*

Let $pol^{(1)}\theta$ be the set of all functions defined on A which preserve θ. Now we have the following question: which equivalence relations are invariant with respect to LT or LT_1-function?

For LT-function the answer is given by the following theorem.

Theorem 3.12. [9] *Let A be a finite set with $|A| = n \geq 2$ and let θ be a non-trivial equivalence relation defined on A. Then there exists a LT-function f which preserves θ if and only if there is only one block with respect to θ which has more than one element.*

Proof. Assume that $f : A \longrightarrow A$ is a LT-function which preserves θ. Then $\lambda(f) = n-1$. By Lemma 3.2 (iv), there exists an element $d \in A$ such that

$$A = \{d, f(d), f^2(d), \ldots, f^{n-1}(d)\} \text{ and } f^{n-1}(d) = f^n(d).$$

Since θ is a non-trivial equivalence relation, there exist $x \neq y \in A$ such that $(x, y) \in \theta$. Thus there exist integers $i, j \in \{0, 1, \ldots, n-1\}$ with $i < j$ such that $x = f^i(d)$ and $y = f^j(d)$. So, $(f^i(d), f^j(d)) \in \theta$. Since $f \in pol^{(1)}\theta$ and $(f^i(d), f^j(d)) \in \theta$, we have $(f(f^i(d)), f(f^j(d))) \in \theta$; that is $(f^{i+1}(d), f^{j+1}(d)) \in \theta$. It follows that $(f^{i+k}(d), f^{j+k}(d)) \in \theta$ for all integer $k \geq 0$. So, $(f^{i+(j-i)}(d) = f^j(d), f^{j+(j-i)}(d)) \in \theta$. Since $(f^i(d), f^j(d)) \in \theta$ and $(f^j(d), f^{j+(j-i)}(d)) \in \theta$, by transitivity of θ, we have $(f^i(d), f^{j+(j-i)}(d)) \in \theta$. If $(j-i) > (n-1)-j$, then $j+(j-i) > j+(n-1)-j = n-1$, which implies that $f^{j+(j-i)}(d) = f^{n-1}(d)$. Thus $(f^i(d), f^{n-1}(d)) \in \theta$. If $(j-i) < (n-1)-j$, then there is an integer t such that $t(j-i) \geq (n-1)-j$. Thus $j+t(j-i) \geq j+(n-1)-j = n-1$, which implies that $f^{j+t(j-i)}(d) = f^{n-1}(d)$. Since $(f^j(d), f^{j+(j-i)}(d)) \in \theta$ and f preserves θ, we get $(f^{j+m(j-i)}(d), f^{j+(m+1)(j-i)}(d)) \in \theta$ for all integers $m \geq 1$. Thus $(f^{j+m(j-i)}(d), f^{j+(m+1)(j-i)}(d)) \in \theta$ for all integers $m \geq 0$. And, since θ is transitive, $(f^i(d), f^{j+(m+1)(j-i)}(d)) \in \theta$ for all integers $m \geq 0$. Thus $(f^i(d), f^{j+t(j-i)}(d)) \in \theta$. Since $f^{j+t(j-i)}(d) = f^{n-1}(d)$, we have $(f^i(d), f^{n-1}(d)) \in \theta$. For a positive integer $k \geq i$, assume that $(f^k(d), f^{n-1}(d)) \in \theta$. Since f preserves θ and $f^n(d) = f^{n-1}(d)$, we get $(f^{k+1}(d), f^{n-1}(d)) \in \theta$. Hence, by Mathematical Induction, we have $(f^s(d), f^{n-1}(d)) \in \theta$ for all $s \geq i$. Thus $\{f^i(d), f^{i+1}(d), \ldots, f^{n-1}(d)\}$ is a block with respect to θ which has more than one element. Let $B = \{f^i(d), f^{i+1}(d), \ldots, f^{n-1}(d)\}$. If i is the least non-negative integer such that $f^i(d) \in B$, then for each element of $\{d, f(d), f^2(d), \ldots, f^{i-1}(d)\}$

form singleton blocks and B is the only block with respect to θ which has more than one element. If i is not the least non-negative integer such that $f^i(d) \in B$, then there exists an integer p with $p < i$ such that $f^p(d) \in B$. Thus there is an integer $q \in \{i, i+1, \ldots, n-1\}$ such that $(f^p(d), f^q(d)) \in \theta$, which implies that $\{f^p(d), f^{p+1}(d), \ldots, f^{n-1}(d)\}$ is a block with respect to θ which has more than one element. Let $C = \{f^p(d), f^{p+1}(d), \ldots, f^{n-1}(d)\}$. If p is the least non-negative integer such that $f^p(d) \in C$, then for each element of $\{d, f(d), f^2(d), \ldots, f^{p-1}(d)\}$ form singleton blocks and C is the only block with respect to θ which has more than one element. If p is not the least non-negative integer such that $f^p(d) \in C$, then continuing in this way, we have the least non-negative integer $r \in \{0, 1, \ldots, n-1\}$ such that $\{f^r(d), f^{r+1}(d), \ldots, f^{n-1}(d)\}$ is the only block with respect to θ which has more than one element and for each element of $\{d, f(d), f^2(d), \ldots, f^{r-1}(d)\}$ form singleton blocks.

Conversely, let θ be a non-trivial equivalence relation defined on A. Assume that there is only one block with respect to θ which has more than one element. Since A is finite, there is an integer n such that $A = \{a_0, a_1, \ldots, a_{n-1}\}$. We may assume that $\{a_i, a_{i+1}, \ldots, a_{n-1}\}$, where $0 \leq i \leq n-1$, is the only one block with respect to θ which has more than one element. Then we define the operation $f : A \longrightarrow A$ by $f(a_j) = a_{j+1}$ for $0 \leq j < n-1$ and $f(a_{n-1}) = a_{n-1}$. Now, we will show that f preserves θ. Let $a, b \in A$ such that $(a, b) \in \theta$. If $a = b$, then $f(a) = f(b)$. Since θ is reflexive, $(f(a), f(b)) \in \theta$. If $a \neq b$, then there are integers l and k with $i \leq l < k \leq n-1$ such that $a = a_l$ and $b = a_k$. Thus $f(a) = f(a_l) = a_{l+1}$ and $f(b) = f(a_k) = a_{k+1}$ if $k \neq n-1$ and $f(b) = f(a_k) = f(a_{n-1}) = a_{n-1}$ if $k = n-1$. So, $f(a)$ and $f(b)$ belong to the set $\{a_i, a_{i+1} \ldots, a_{n-1}\}$. Thus $(f(a), f(b)) \in \theta$. Therefore, f preserves θ; that is, $f \in pol^{(1)}\theta$. Since $A = \{a_0, a_1, \ldots, a_{n-1}\}$ and by definition of f, we have $A = \{a_0, f(a_0), f^2(a_0), \ldots, f^{n-1}(a_0)\}$ and $f^{n-1}(a_0) = a_{n-1} = f^n(a_0)$. By Lemma 3.2 (iv), we have $\lambda(f) = n-1$. Hence, f is a LT-function.

□

Proposition 3.13. [9] *Let A be a finite set with $|A| = n \geq 3$ and let θ be a non-trivial equivalence relation on A. Then there is a LT_1-function f with $|Imf^{n-2}| = 1$ which preserves θ if and only if either*
(i) *there exists only one block B with respect to θ which has more than one element, or*
(ii) *there are exactly two blocks B and C with respect to θ which have more than one element and one of them consists of exactly two elements.*

Proof. Assume that f is a LT_1-function with $|Imf^{n-2}| = 1$. By Theorem 3.9, there are distinct elements $u, v \in A$ such that $A = \{u, v, f(v), \ldots, f^{n-2}(v)\}$ and there is an exponent k with $0 \leq k < n-2$ such that $f(u) = f^{k+1}(v)$ and a number m with $m+k = n-2$ such that $f^{m+1}(u) = f^m(u)$. Thus $A = \{v, f(v), \ldots, f^k(v)\} \cup \{u, f(u), \ldots, f^m(u)\}$ where $f^{k+1}(v) = f(u)$ and $f^{m+1}(u) = f^m(u)$.
Let θ be a non-trivial equivalence relation defined on A which is invariant with

respect to f. Let $X = \{v, f(v), \dots, f^{n-2}(v)\}$ and $Y = \{u, f(u), \dots, f^m(u)\}$. Since $|A| = n \geq 3$, we have $|X| \geq 2$ and $|Y| \geq 2$. Next, we will show that $f|_X$ and $f|_Y$ are LT-functions. Note that $f|_X(a) = f(a)$ for all $a \in X$ and $f|_Y(b) = f(b)$ for all $b \in Y$. Thus $X = \{v, f|_X(v), \dots, (f|_X)^{n-2}(v)\}$ where $(f|_X)^{n-1}(v) = (f|_X)^{n-2}(v)$ and $Y = \{u, f|_Y(u), \dots, (f|_Y)^m(u)\}$ where $(f|_Y)^{m+1}(u) = (f|_Y)^m(u)$. By Lemma 3.2 (iv), we have $\lambda(f|_X) = n-2 = (n-1)-1 = |X|-1$ and $\lambda(f|_Y) = m = (m+1)-1 = |Y|-1$. Therefore, $f|_X$ and $f|_Y$ are LT-functions. Now, let $\bar{\theta} = \theta|_{X\times X}$ and $\bar{\bar{\theta}} = \theta|_{Y\times Y}$. We claim that $f|_X$ preserves $\bar{\theta}$ and $f|_Y$ preserves $\bar{\bar{\theta}}$. Let $a, b \in X$ such that $(a,b) \in \bar{\theta}$. Then there are $r, s \in \{0, 1, \dots, n-2\}$ such that $a = f^r(v)$, $b = f^s(v)$ and $(a,b) \in \theta$. Thus $f(a) = f(f^r(v)) = f^{r+1}(v)$ and $f(b) = f(f^s(v)) = f^{s+1}(v)$ are in X. Since f preserves θ and $(a,b) \in \theta$, we have $(f(a), f(b)) \in \theta$. Since $f(a)$ and $f(b)$ are in X, we get $(f|_X(a), f|_X(b)) \in \bar{\theta}$. Hence $f|_X$ preserves $\bar{\theta}$. Similarly, $f|_Y$ preserves $\bar{\bar{\theta}}$. By Theorem 4.6, there is only one block with respect to $\bar{\theta}$ which has more than one element and there is only one block with respect to $\bar{\bar{\theta}}$ which has more than one element. Consider the following cases:

Case 1: If the block of u with respect to θ consists only of one element, then $\theta = \bar{\theta} \cup \{(u,u)\}$. Thus there exists only one block with respect to θ which has more than one element, this corresponds to (i).

Case 2: $(u, f^t(v)) \in \theta$ for some $0 \leq t < k$.
If $t = 0$, then $(u, v) \in \theta$. Since f preserves θ, we have $(f(u), f(v)) \in \theta$. Since $f(u) = f^{k+1}(v)$, we get $(f^{k+1}(v), f(v)) \in \theta$. It follows that $(f^{tk+1}(v), f^{(t-1)k+1}(v)) \in \theta$ for all $t \geq 1$, and since f is transitive, $(f^{tk+1}(v), f(v)) \in \theta$ for all $t \geq 1$.
We claim that $(f^{k+m}(v), f^i(v)) \in \theta$ for all $i \geq 1$.
If $k \geq m-1$, then $2k+1 = (k+1)+k \geq (k+1)+(m-1) = k+m$. Thus $f^{2k+1}(v) = f^{k+m}(v)$. Since $(f^{tk+1}(v), f(v)) \in \theta$ for all $t \geq 1$, we have $(f^{2k+1}(v), f(v)) \in \theta$. And, since $f^{2k+1}(v) = f^{k+m}(v)$, we get $(f^{k+m}(v), f(v)) \in \theta$. Assume that $k < m-1$. Then there is a positive integer s such that $sk \geq m-1$. Thus $(k+1)+sk \geq (k+1)+(m-1) = k+m$; that is $(s+1)k+1 \geq k+m$, which implies that $f^{(s+1)k+1}(v) = f^{k+m}(v)$. Since $(f^{tk+1}(v), f(v)) \in \theta$ for all $t \geq 1$, we have $(f^{(s+1)k+1}(v), f(v)) \in \theta$. And, since $f^{(s+1)k+1}(v) = f^{k+m}(v)$, we have $(f^{k+m}(v), f(v)) \in \theta$. For a positive integer $j \geq 1$, assume that $(f^{k+m}(v), f^j(v)) \in \theta$. Since f preserves θ and $f^{k+m+1}(v) = f^{k+m}(v)$, we get $(f^{k+m}(v), f^{j+1}(v)) \in \theta$. Hence, by Mathematical Induction, we have $(f^{k+m}(v), f^i(v)) \in \theta$ for all integers $i \geq 1$. So, $\{f(v), \dots, f^{m+k}(v)\} = X \backslash \{v\}$ is a subset of the block C of the element $f(v)$ with respect to $\bar{\theta} = \theta|_{X\times X}$ and also with respect to θ. If $u \in C$, then $\theta = A \times A$, a contradiction since θ is a non-trivial. Thus $u \notin C$. It follows that $B = \{u, v\}$ and $C = X \backslash \{v\}$ are the only two blocks with respect to θ which have more than one element. Since $k > 0$, this gives (ii).
If $t > 0$ then $k > 0$ and $f(u) \neq f^k(v)$. So, $\{f^{t+1}(v), \dots f^{k+1}(v) = f(u), \dots, f^{m+k}(v)\}$ is a subset of the block C of the element $f(u)$ with respect to $\bar{\theta}$ (and also with respect to θ) containing $f^k(v)$ and $f(u)$, hence $|C| > 1$. If $u \in C$, then C is the

only block with respect to θ with cardinality greater than 1, this corresponds to (i). And if $u \notin C$, then $\{u, f^t(u)\}$ and C are the only blocks with respect to θ having cardinalities greater than 1 and $|\{u, f^t(v)\}| = 2$, this corresponds to (ii).

Case 3: $(u, f^t(u)) \in \theta$ for some $0 \leq t \leq m$ and $(u, f^s(v)) \notin \theta$ for all $0 \leq s < k$. Then Y is a block with respect to θ and the block of each $f^s(v)$ for $0 \leq s < k$ is singleton. Therefore, Y is the only block with respect to θ with $|Y| \geq 2$, this corresponds to (i).

Case 4: $(u, f^k(v)) \in \theta$. If $(c, d) \notin \theta$ for all $c \neq d$ in $A \backslash \{u, f^k(v)\}$, then $\{u, f^k(v)\}$ is the only block with respect to θ having more than one element. We consider the case that there are $c \neq d$ in $A \backslash \{u, f^k(v)\}$ such that $(c, d) \in \theta$. If c or d belongs to $X \backslash Y$, then $\{c, d, f^k(v)\}$ is a subset of the only block C with respect to $\bar{\theta}$ (also with respect to θ) with $|C| > 1$ and so, $C \cup \{u\}$ is the only block with respect to θ which has more than one element. But, if c and d both are in $Y \backslash \{u\}$, then they are in the only block C with respect to $\bar{\bar{\theta}}$ (also with respect to θ) with $|C| > 1$, so, in this case, C and $\{u, f^k(v)\}$ are the only blocks having more than one element and one of them has cardinality 2.

Conversely, let A be a set with $|A| = n \geq 3$ and let θ be a non-trivial equivalence relation on A satisfy either (i) or (ii). We may assume that $A = \{a_0, a_1, \ldots, a_{n-1}\}$ and either $B = \{a_i, a_{i+1}, \ldots, a_{n-1}\}$ for some $0 < i < n-1$ in case (i) or $B = \{a_0, a_i\}$ and $C = \{a_{i+1}, \ldots, a_{n-1}\}$ for some $0 < i < n-1$ in case (ii) are the blocks with respect to θ. In either case, we define $f : A \longrightarrow A$ by $f(a_j) = a_{j+1}$ if $j \notin \{0, n-1\}$, $f(a_0) = a_{i+1}$ and $f(a_{n-1}) = a_{n-1}$. In both cases, f preserves θ. Further, we have $f(a_i) = a_{i+1} = f(a_0)$ and $f(a_{n-2}) = a_{n-1} = f(a_{n-1})$ for $a_i \neq a_0$ and $a_{n-2} \neq a_{n-1}$ and there are no other elements $c \neq d$ in A such that $f(c) = f(d)$. Thus $|Imf| = |A| - 2$. Since $a_{n-1} \neq a_{n-2}$ and $a_{n-1}, a_{n-2} \in Imf^k$ for all $1 \leq k < n-2$ and $f(a_{n-1}) = f(a_{n-2})$, we have $Imf^k \supset Imf^{k+1}$ for all $1 \leq k < n-2$. Together with $|A| = |Imf| + 2$, we get $|Imf^{n-2}| \leq 1$. Since $a_{n-1} \in Imf^{n-2}$, we have $|Imf^{n-2}| \geq 1$. Thus $|Imf^{n-2}| = 1$, and so, $Imf^{n-2} = Imf^{n-1}$. Hence, $\lambda(f) = n-2$; that is f is a LT_1-function.

$\square$

Chapter 4

All Congruence-modular Symmetric Algebras

In chapter 3, we studied a characterization of all unary operations f on a finite set A with long pre-period; that is, $\lambda(f) = n - 1$ for $n \geq 2$ and $\lambda(f) = n - 2$ for $n \geq 3$. In contrary, we are interested in studying a unary operation f on a finite set A with $\lambda(f) \in \{0, 1\}$ which we will call a unary operation with short pre-period.

In this chapter, we characterize all unary operations f on a finite set A with $\lambda(f) = 0$ such that the unary algebra $(A; f)$ is congruence-distributive or congruence-modular.

Note that $\lambda(f) = 0$ if and only if f is a permutation on A. In the theory of groups, the set of all permutations on a set A together with composition is called a symmetric group. And it is known that every permutation can be decomposed into simple parts called cycles.

Let A be a finite set and let f be a permutation on A. Then the algebra $(A; f)$ is called a **symmetric algebra**.

If A is a singleton or a two-element set, the congruence lattice of $(A; f)$ is also singleton chain $\{\Delta_A\}$ or two-element chain $\{\Delta_A, A \times A\}$, respectively. So, $(A; f)$ is congruence-distributive (see Figure 5). We are interested in the case that the cardinality of A is more than two.

Figure 5. The singleton chain and two-element chain

We begin by considering necessary conditions for a permutation f on A whose $(A; f)$ is congruence-distributive.

Proposition 4.1. *Let $(A; f)$ be a symmetric algebra with $|A| \geq 3$. If $(A; f)$ is congruence-distributive, then either*
(i) f is a cycle having at most one fixed point, or
(ii) f has no fixed points and f is a product of two disjoint cycles whose lengths are relatively prime.

Proof. We will prove by the contrapositive. Suppose that (i) and (ii) are not true. Then f is a product of at least three disjoint cycles. Let $f = \alpha_1\alpha_2 \ldots \alpha_r$ where $r \geq 3$ and all α_i are cycles (can be of length 1) and α_i and α_j are disjoint for each $1 \leq i \neq j \leq r$. For each $1 \leq i \leq r$, let $\alpha_i = (a_{i1}\, a_{i2} \ldots a_{im_i})$ and define $B_i = \{a_{i1}, a_{i2}, \ldots, a_{im_i}\}$ for some non-negative integer m_i. Then $B_i \cap B_j = \emptyset$ for all $1 \leq i \neq j \leq r$.
Because $r \geq 3$, we let $\sigma = (123)$ and define $\theta_j \subseteq A \times A$ for each $j \in \{1, 2, 3\}$ by

$$\theta_j = \Delta_A \cup \{(x, y) |\ \{x, y\} \subseteq B_j \cup B_{\sigma(j)} \text{ or } \{x, y\} \subseteq B_{\sigma^2(j)}\}.$$

Since $f(x) \in B_i$ for all $x \in B_i$ and for all $i \in \{1, 2, 3\}$, we have that θ_i is invariant under f for each $i \in \{1, 2, 3\}$.
Let $\phi := \Delta_A \cup (\bigcup_{k=1}^{3} \{(x, y) |\ x, y \in B_k\})$. By cyclically of σ and $B_i \cap B_j = \emptyset$ for all $1 \leq i \neq j \leq 3$, we have $\theta_j \wedge \theta_{\sigma(j)} = \phi$ for each $j \in \{1, 2, 3\}$.

Let $\theta := \Delta_A \cup \{(x, y) |\ x, y \in B_1 \cup B_2 \cup B_3\}$. Then $\theta_j \subseteq \theta$ for all $j \in \{1, 2, 3\}$. Thus $\theta_j \cup \theta_{\sigma(j)} \subseteq \theta$ for all $j \in \{1, 2, 3\}$ which implies that $\theta_j \vee \theta_{\sigma(j)} \subseteq \theta$ for all $j \in \{1, 2, 3\}$. On the other hand, let $(a, b) \in \theta$. Then $a = b$ or $a, b \in B_1 \cup B_2 \cup B_3$. If $a = b$, then $(a, b) \in \theta_j \cup \theta_{\sigma(j)}$ for all $j \in \{1, 2, 3\}$. So, $\theta \subseteq \theta_j \vee \theta_{\sigma(j)}$ for all $j \in \{1, 2, 3\}$. In other cases, if $a, b \in B_1 \cup B_2 \cup B_3$ then $\{a, b\} \subseteq B_j \cup B_{\sigma(j)}$ for some $j \in \{1, 2, 3\}$ which implies that $(a, b) \in \theta_j \cup \theta_{\sigma(j)}$. So, $\theta \subseteq \theta_j \vee \theta_{\sigma(j)}$. Hence, $\theta_j \vee \theta_{\sigma(j)} = \theta$.
So, $\{\theta_1, \theta_2, \theta_3, \phi, \theta\}$ is a sublattice of the congruence lattice of $(A; f)$ which is isomorphic to M_3 (see Figure 6). Hence, $M_3 - N_5$ Theorem implies that the congruence lattice of the symmetric algebra $(A; f)$ is not distributive.

□

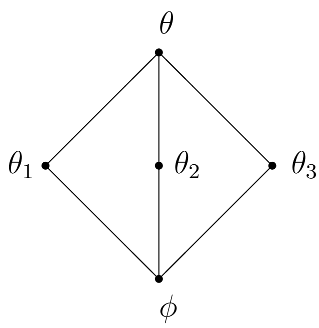


Figure 6. A sublattice of the congruence lattice of $(A; f)$ which is isomorphic to M_3

Remark 4.2. *From Proposition 4.1, the congruence lattice of* $(A; f)$ *is not distributive if* f *is an identity on a set* A *whose cardinality is more than two. Moreover, if the cardinality of* A *is three, the congruence lattice of* $(A; f)$ *is the modular lattice* M_3.

Lemma 4.3. *Let* $(B; f^B)$ *be a subalgebra of* $(A; f^A)$.
(i) *If* $\theta \in Con(A; f^A)$, *then the restriction* $\theta|_B$ *of* θ *onto* B *is a congruence relation on* $(B; f^B)$.
(ii) *If* $\theta \in Con(B; f^B)$, *then the relation* $\theta \cup \{(x,x) | x \in A\}$ *is a congruence relation on* $(A; f^A)$.

The proofs of Lemma 4.3 are straight forward. We will denote the relations $\theta|_B$ and $\theta \cup \{(x,x) | \, x \in A\}$ in Lemma 4.3 by θ_B and θ^A, respectively.

Lemma 4.4. *Let* $\bar{A} := (A; f)$ *be a symmetric algebra and let* $(a\, f(a) \ldots \, f^{p-1}(a))$ *and* $(b\, f(b) \ldots \, f^{q-1}(b))$ *be cycles in a product of* f *for some positive integers* p *and* q. *Let* $\theta \in Con(\bar{A})$.
(i) *If* $(a, f^r(a)) \in \theta$ *for some* $0 < r \leq p-1$, *then* $(a, f^{kr}(a)) \in \theta$ *for all non-negative integer* k.
(ii) *If there exists integer* $0 < r \leq p-1$ *such that* $(a, f^r(a)) \in \theta$ *and* r *is not a factor of* p, *then* $\{a, f(a), \ldots, f^{p-1}(a)\}$ *is a subset of a block of* A/θ.
(iii) *If* $(p,q) = 1$ *and* $(a,b) \in \theta$, *then* $\{a, f(a), \ldots, f^{p-1}(a), b, f(b), \ldots, f^{q-1}(b)\}$ *is a subset of a block of* A/θ.

Proof. (i) Assume that $(a, f^r(a)) \in \theta$ for some $0 < r \leq p-1$. If $k = 0$ then $(a, f^0(a)) = (a,a) \in \theta$. We assume that $k \neq 0$. Then (i) follows by taking f^r to $(a, f^r(a))$ for k times for all non-negative integer k and by the transitivity of θ.

(ii) Assume that there exists integer $0 < r \leq p-1$ such that $(a, f^r(a)) \in \theta$ and r is not a factor of p. Then the division algorithm implies that there are integers t_1 and $0 \leq s_1 < r$ such that $p = rt_1 + s_1$. Since $(a, f^r(a)) \in \theta$ and by (i), we have $(a, f^{rt_1}(a)) \in \theta$. Let $r_1 = r - s_1$. Then $0 < r_1 < r$. After applying f^r to $(a, f^r(a))$ for t_1 times, we will get $(f^{rt_1}(a), f^{r_1}(a)) \in \theta$; hence, the transitivity of θ implies that $(a, f^{r_1}(a)) \in \theta$. By repeating the same process, we will get a decreasing sequence of non-negative integers $0 < \ldots < r_1 < r < p$ such that $(a, f^{r_i}(a)) \in \theta$ for all integers $i \geq 1$. Hence, the process will be stop after finite steps; that is, there is a positive integer k such that $r_k > 0$ and $r_{k+1} = 0$.
It is easily see that $r_k \neq 1$ implies the continuation of the process; so, $r_k = 1$. Hence, $(a, f(a)) \in \theta$ which implies by applying f and the transitivity of θ that $(a, f^t(a)) \in \theta$ for all $0 \leq t \leq p-1$.

(iii) Assume that $(p,q) = 1$ and $(a,b) \in \theta$. Without loss of generality, we may assume that $p < q$. By the division algorithm and $(p,q) = 1$, we have $q = pk + r$ for some integers k and r where $0 < r < p$. Then $(f^r(a), b) = (f^q(a), f^q(b)) \in \theta$. Since $(a,b) \in \theta$, the transitivity of θ implies that $(a, f^r(a)) \in \theta$ for some $0 < r < p$. By part(ii), $(a, f^t(a)) \in \theta$ for all $0 \leq t \leq p-1$. Since $(a,b) \in \theta$

and by the transitivity of θ, we have $(b, f^t(a)) \in \theta$ for all $0 \leq t \leq p-1$. After applying f to $(b, f^t(a))$ for all $0 \leq t \leq p-1$, we can get $(f^t(a), f^s(b)) \in \theta$ for all $0 \leq t \leq p-1$ and $0 \leq s \leq q-1$.

□

In the following proposition, we will show that the converse of Proposition 4.1 is also true by showing that the congruence lattice of $(A; f)$ is a product of chains; or, a linear sum of a product of chains and a one-element chain.

Recall that a linear sum of an ordered set P with a one-element chain $\underline{1}$ is an ordered set $P \oplus \underline{1}$ which can represent P with a new top element added.

Proposition 4.5. *If f satisfies* (i) *or* (ii) *of Proposition 4.1, then the congruence lattice of $(A; f)$ is a product of chains; or, a linear sum of a product of chains P with a one-element chain $\underline{1}$.*

Proof. Assume that f is a cycle having no fixed point. Let $a \in A$. Then, we may consider $f = (a\ f(a) \ldots f^{n-1}(a))$.
We will prove that $Con(A; f)$ is dually isomorphic to $\downarrow n$.
Let $m \in \downarrow n$. Then $0 < m \leq n$; hence, there exists an integer c_m such that $n = mc_m$. By Remark 2.25, $\mathbb{Z}$ can be partitioned into the set $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$ of all residue classes modulo m where $[j]$ is the class of integers which is congruence to j modulo m for all $j \in \{0, 1, 2, \ldots, m-1\}$; that is, $[j] = \{x | \ x \equiv j \pmod{m}\}$ for all $j \in \{0, 1, 2, \ldots, m-1\}$. We define $f^{[j]_m}(a) := \{f^s(a) \mid s \equiv j \pmod{m}$ for some integer $s\}$. Then $\wp_m := \{f^{[j]_m}(a) \mid j \in \{0, 1, 2, \ldots, m-1\}\}$ is a partition of A. It is clear that $\wp_m$ corresponds to the congruence modulo m restriction to A which will be denoted by θ_m. Hence, $\theta_m = \{(x, y) | x, y \in f^{[j]_m}(a)$ for some $j \in \{0, 1, 2, \ldots, m-1\}\}$.

Note that: (i) if $m = 1$, then $c_1 = n$. Thus $\wp_1 = \{A\}$ and so, $\theta_1 = A \times A$ and
(ii) if $m = n$, then $c_n = 1$. Thus $\wp_n = \{\{1\}, \{2\}, \ldots, \{n\}\}$ and so, $\theta_n = \Delta_A$.

Now, we define $\alpha : \downarrow n \longrightarrow Con\ (A; f)$ by $\alpha(m) = \theta_m$ for all $m \in \downarrow n$.
Let $u, v \in \downarrow n$ be such that $u|v$ and let $(x, y) \in \theta_v$. Then there exists $j \in \{0, 1, \ldots, v-1\}$ such that $x, y \in f^{[j]_v}(a)$. Thus there are integers s and t with $s \equiv j \pmod{v}$ and $t \equiv j \pmod{v}$ such that $x = f^s(a)$ and $y = f^t(a)$. Since $u|v$, Theorem 2.18 implies that $s \equiv j \pmod{u}$ and $t \equiv j \pmod{u}$. Thus $x, y \in f^{[j]_u}(a)$ for some $j \in \{0, 1, \ldots, u-1\}$; and so, $(x, y) \in \theta_u$. Conversely, let $u, v \in \downarrow n$ be such that $\theta_v \subseteq \theta_u$. Then the partition A/θ_v is finer than A/θ_u which means $u = |A/\theta_u| \leq |A/\theta_v| = v$. If $u = v$, then clearly, $u|v$. We assume that $u < v$. Since $v|v$, we have $v \equiv 0 \pmod{v}$. So, $f^v(a) \in f^{[o]_v}(a)$. Since $f^0(a) \in f^{[o]_v}(a)$, we have $(f^v(a), f^0(a)) \in \theta_v \subseteq \theta_u$. So, $f^0(a) \in f^{[o]_u}(a)$ implies that $f^v(a) \in f^{[o]_u}(a)$. Therefore, $v \equiv 0 \pmod{u}$; hence, $u|v$. Thus α is an order-embedding.
It remains to show that α is onto.
Let $\theta \in Con\ (A; f)$. If θ is an identity relation on A, then $\theta = \theta_0 = \theta_n$. We consider the case that there exist $x \neq y \in A$ such that $(x, y) \in \theta$. Since f is

a cycle of length n, we can write $f = (x\ f(x)\dots f^{n-1}(x))$; hence, there exists $0 < r \leq n-1$ such that $y = f^r(x)$. If r is not a factor of n, Lemma 4.4(ii) implies that $\theta = A \times A = \theta_1$. But, if r is a factor of n, Lemma 4.4(i) and the transitivity of θ implies that $(f^s(x), f^t(x)) \in \theta$ if and only if $s \equiv t \pmod r$; hence, $\theta = \theta_r$. In either cases, there exists $0 \leq r \leq n-1$ such that $\theta = \theta_r$. Thus, $\alpha(r) = \theta_r = \theta$. Therefore, α is onto.
Hence, $Con(A; f)$ is dually isomorphic to $\downarrow n$ which is a product of chains. So, the congruence lattice of $(A; f)$ is a product of chains.

Now, we assume that f is a cycle with one fixed point or f satisfies (ii) of Proposition 4.1. In either cases, we may assume that $f = \alpha_1\alpha_2$ where α_1 and α_2 are disjoint cycles whose lengths are relatively prime whenever both of them are of lengths more than one. Let B_i be a subset of A whose elements are in α_i for each $i \in \{1, 2\}$. Then, $f|_{B_i}$ is a cycle on B_i for all $i \in \{1, 2\}$. By condition (i), the congruence lattice of $(B_i; f|_{B_i})$ is a product of chains for all $i \in \{1, 2\}$.

For each $\theta_i \in Con(B_i; f|_{B_i})$ for $i \in \{1, 2\}$, we define $\theta_i^A := \theta_i \cup \{(x, x) |\ x \in A\}$ for each $i \in \{1, 2\}$. Then θ_i^A is a congruence relation on $(A; f)$ for all $i \in \{1, 2\}$.

Now, we define $\beta : Con(B_1; f|_{B_1}) \times Con(B_2; f|_{B_2}) \longrightarrow Con(A; f)$ by $\beta(\theta_1, \theta_2) = \theta_1^A \vee \theta_2^A$ for each $\theta_i \in Con(B_i; f|_{B_i})$ and for all $i \in \{1, 2\}$.

Let θ_i and ϕ_i be congruence relations on $(B_i; f|_{B_i})$ for each $i \in \{1, 2\}$. Since $B_1 \cap B_2 = \emptyset$ and $B_1 \cup B_2 = A$, we have $\theta_1^A \cup \theta_2^A$ and $\phi_1^A \cup \phi_2^A$ are congruence relations on $(A; f)$. It is clear that $\theta_1^A \vee \theta_2^A = \theta_1^A \cup \theta_2^A$ and $\phi_1^A \vee \phi_2^A = \phi_1^A \cup \phi_2^A$. Thus

$$\begin{aligned}
(\theta_1, \theta_2) \subseteq (\phi_1, \phi_2) &\iff \theta_i \subseteq \phi_i \ \text{ for each } i \in \{1, 2\},\\
&\iff \theta_i^A \subseteq \phi_i^A \ \text{ for each } i \in \{1, 2\},\\
&\iff \theta_1^A \cup \theta_2^A \subseteq \phi_1^A \cup \phi_2^A,\\
&\iff \theta_1^A \vee \theta_2^A \subseteq \phi_1^A \vee \phi_2^A,\\
&\iff \beta(\theta_1, \theta_2) \subseteq \beta(\phi_1, \phi_2).
\end{aligned}$$

So, β is an order-embedding.
Therefore, $Con(B_1; f|_{B_1}) \times Con(B_2; f|_{B_2})$ can be embedded as a sublattice of $Con(A; f)$.
Now, we will show that $\theta_1^A \vee \theta_2^A \neq A \times A$ for each $\theta_i \in Con(B_i; f|_{B_i})$ and for all $i \in \{1, 2\}$.
Let $\theta_i \in Con(B_i; f|_{B_i})$ for $i \in \{1, 2\}$. Since $B_1 \cap B_2 = \emptyset$, we have $(x, y) \notin \theta_1^A \vee \theta_2^A$ for each $x \in B_1$ and $y \in B_2$. Since $B_i \neq \emptyset$ for $i \in \{1, 2\}$, it is clear that $\theta_1^A \vee \theta_2^A \subset A \times A$. It follows that $Im\beta \subseteq Con(A; f) \backslash \{A \times A\}$. Let $\theta \in Con(A; f) \backslash \{A \times A\}$. Then θ_{B_i} is a congruence relation on $(B_i; f|_{B_i})$ such that $\theta_{B_i}^A \subseteq \theta$ for each $i \in \{1, 2\}$. Since $B_1 \cap B_2 = \emptyset$ and $f(B_i) = B_i$ for all $i \in \{1, 2\}$, we have $\theta_{B_1}^A \cup \theta_{B_2}^A$ is a congruence relation on $(A; f)$; so, $\theta_{B_1}^A \vee \theta_{B_2}^A = \theta_{B_1}^A \cup \theta_{B_2}^A \subseteq \theta$. Conversely, let $(a, b) \in \theta$. We

suppose that $a \in B_1$ and $b \in B_2$. Since the lengths of α_1 and α_2 are relatively prime, Lemma 4.4(iii) implies that $B_1 \cup B_2$ is a subset of a block of A/θ. Since $B_1 \cup B_2 = A$, we have $\theta = A \times A$, a contradiction. Thus $\{a, b\} \subseteq B_i$ for some $i \in \{1, 2\}$. So, $(a, b) \in \theta_{B_i} \subseteq \theta^A_{B_i} \subseteq \theta^A_{B_1} \cup \theta^A_{B_2}$. Therefore, $\theta = \theta^A_{B_1} \vee \theta^A_{B_2}$; that is, $\theta = \beta(\theta_{B_1}, \theta_{B_2})$. So, $\theta \in Im\beta$. Therefore, $Con(A; f)\backslash\{A \times A\} \subseteq Im\beta$.
Hence, $Im\beta = Con(A; f)\backslash\{A \times A\}$.
Therefore, $Con(B_1; f|_{B_1}) \times Con(B_2; f|_{B_2}) \cong Con(A; f)\backslash\{A \times A\}$. Since $Con(B_i; f|_{B_i})$ is a product of chains for each $i \in \{1, 2\}$, we have that $Con(B_1; f|_{B_1}) \times Con(B_2; f|_{B_2})$ is a product of chains which implies that $Con(A; f)\backslash\{A \times A\}$ is a product of chains. Hence, the congruence lattice of $(A; f)$ is a linear sum of a product of chains P and a one-element chain $\underline{1}$. □

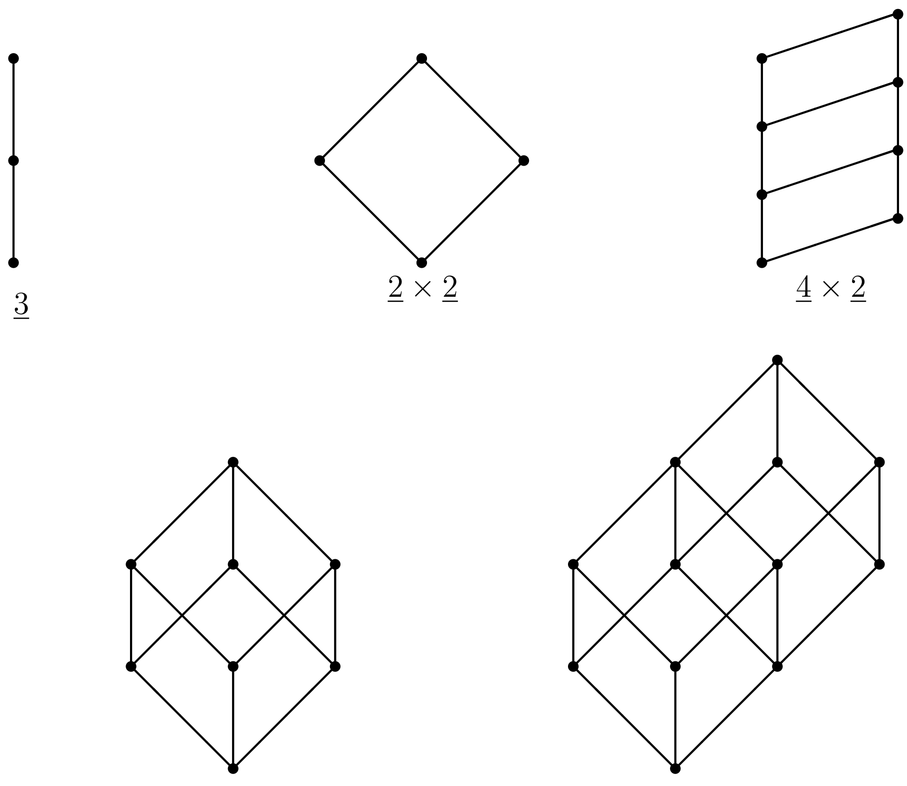


Figure 7. The congruence lattices of some symmetric algebras whose the permutation operation is a cycle having no fixed point.

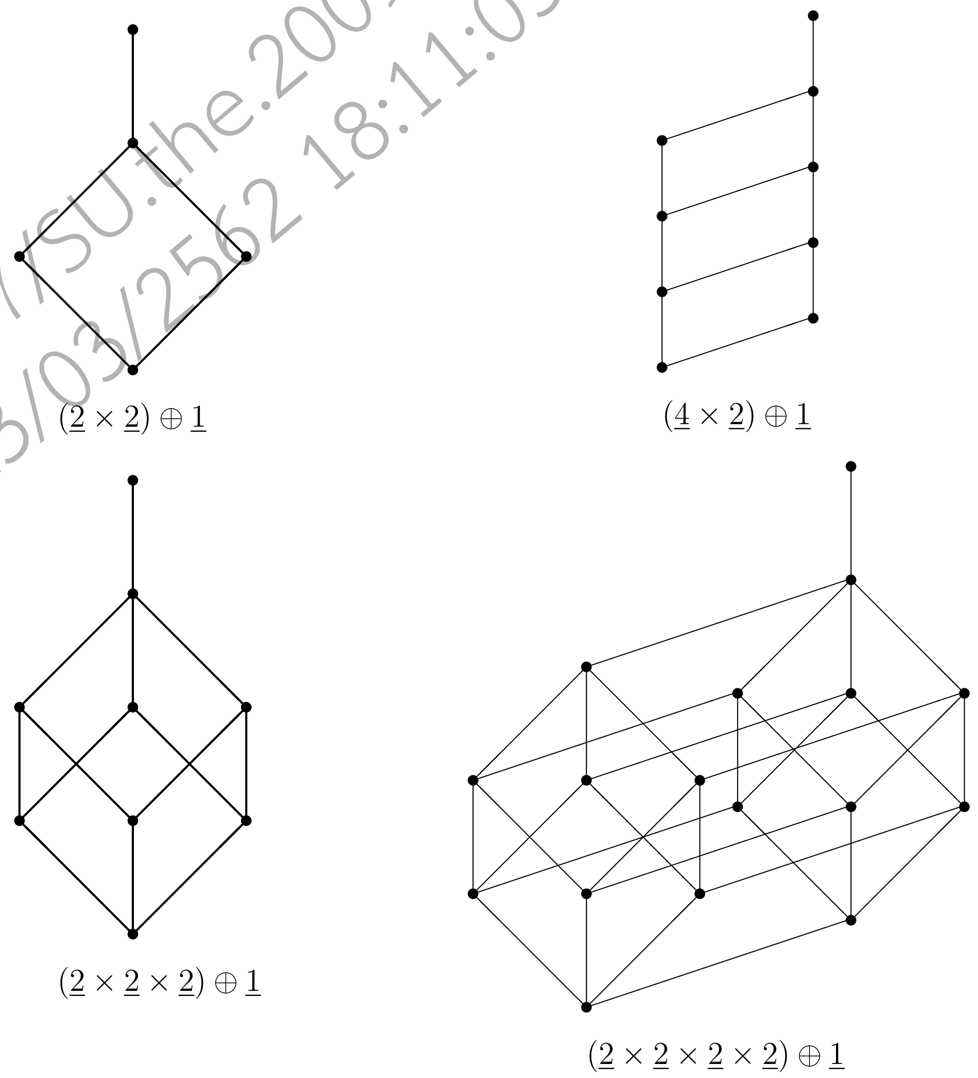


Figure 8. The congruence lattices of some symmetric algebras whose the permutation operation is a product of atmost two disjoint cycles whose lengths are relatively prime and one of them can be of length 1.

The following theorem shows a characterization of all symmetric algebras which are congruence-distributive and the proof of the theorem is followed directly by Proposition 4.1 and Proposition 4.5.

Theorem 4.6. *Let $\bar{A} := (A; f)$ be a symmetric algebra. Then the followings are equivalent:*
(i) *$\bar{A}$ is congruence-distributive.*
(ii) *Conditions* (i) *or* (ii) *of Proposition 4.1 are satisfied.*
(iii) *$Con(\bar{A})$ is either a product of chains or a linear sum of a product of chains with a one-element chain $\underline{1}$.*

Now, we are looking for conditions on f whose symmetric algebra $(A; f)$ is congruence-modular. It is known that if A is singleton or a two-element set then $(A; f)$ is congruence-distributive and so, $(A; f)$ is congruence-modular. In the case A having cardinality 3, if f is an identity on A then the congruence lattice of $(A; f)$ is modular and if f is not an identity then Theorem 4.6 implies that the congruence lattice of $(A; f)$ is distributive which implies that it is congruence-modular. Therefore, we will study the case that the cardinality of A is more than three.

In the following proposition, we will prove necessary conditions for a permutation f on A which $(A; f)$ is congruence-modular.

Proposition 4.7. *Let $(A; f)$ be a symmetric algebra with $|A| \geq 4$. If $(A; f)$ is congruence-modular, then f is either one of the followings:*
(i) *f is a cycle having at most two fixed points, or*
(ii) *f has at most one fixed point and f is a product of two disjoint cycles whose lengths are relatively prime, or*
(iii) *f has no fixed point and f is a product of three disjoint cycles whose lengths are relatively prime.*

Proof. We will prove by the contrapositive. Suppose that (i), (ii) and (iii) are not true. Then f is a product of at least four disjoint cycles. Let $f = \alpha_1\alpha_2 \dots \alpha_r$ where $r \geq 4$ and all α_i are cycles (can be of length 1) and α_i and α_j are disjoint for each $1 \leq i \neq j \leq r$. Let B_i be a subset of A whose elements are in α_i for each $i \in \{1, 2, \dots, r\}$. Because $r \geq 4$, let $\sigma = (1234)$ and let $i \in \{1, 2, 3, 4\}$.
Now, let define $\theta_j \subseteq A \times A$ for each $j \in \{1, 2, 3\}$ as follows:
$\theta_1 = \Delta_A \cup \{(x, y) | \{x, y\} \subseteq B_i \cup B_{\sigma(i)}$ or $\{x, y\} \subseteq B_{\sigma^2(i)}$ or $\{x, y\} \subseteq B_{\sigma^3(i)}\}$,
$\theta_2 = \Delta_A \cup \{(x, y) | \{x, y\} \subseteq B_i \cup B_{\sigma(i)}$ or $\{x, y\} \subseteq B_{\sigma^2(i)} \cup B_{\sigma^3(i)}\}$, and
$\theta_3 = \Delta_A \cup \{(x, y) | \{x, y\} \subseteq B_i \cup B_{\sigma^2(i)}$ or $\{x, y\} \subseteq B_{\sigma(i)} \cup B_{\sigma^3(i)}\}$.
Then θ_i is invariant under f for each $i \in \{1, 2, 3\}$. Thus $\theta_1 \subset \theta_2$ and

$$\theta_1 \wedge \theta_3 = \Delta_A \cup (\bigcup_{k=1}^{4} \{(x, y) | \; x, y \in B_k\}) = \theta_2 \wedge \theta_3.$$

Now, we will show that $\theta_1 \vee \theta_3 = \theta_2 \vee \theta_3$.
It is clearly, $\theta_1 \vee \theta_3 \subseteq \theta_2 \vee \theta_3$.
Let $(a, b) \in \theta_2 \vee \theta_3$. There are $a = q_0, q_1, \dots, q_t = b \in A$ such that $(q_k, q_{k+1}) \in \theta_2 \cup \theta_3$ for all $0 \leq k \leq t - 1$. Without loss of generality, we may assume that $(a, q_1) \in \theta_2$. Since $\{a = q_0, q_1, \dots, q_t = b\}$ is finite, there is the greatest element $q_k \in \{a = q_0, q_1, \dots, q_t = b\}$ such that $(q_{i-1}, q_i) \in \theta_2$ for each $1 \leq i \leq k$ but $(q_k, q_{k+1}) \in \theta_3$, and so, the transitivity of θ_2 implies that $(a, q_k) \in \theta_2$.
If $(q_j, q_{j+1}) \in \theta_3$ for each $k \leq j \leq t-1$, the transitivity of θ_3 implies that $(q_k, b) \in \theta_3$. Since $(a, q_k) \in \theta_2$, we have $\{a, q_k\} \subseteq B_i \cup B_{\sigma(i)}$ or $\{a, q_k\} \subseteq B_{\sigma^2(i)} \cup B_{\sigma^3(i)}$.
If $\{a, q_k\} \subseteq B_i \cup B_{\sigma(i)}$, then $(a, q_k) \in \theta_1$, and since $(q_k, b) \in \theta_3$, we have $(a, b) \in \theta_1 \vee \theta_3$.

Thus, we assume that $\{a, q_k\} \subseteq B_{\sigma^2(i)} \cup B_{\sigma^3(i)}$.
If $\{a, q_k\} \subseteq B_{\sigma^2(i)}$ or $\{a, q_k\} \subseteq B_{\sigma^3(i)}$, then $(a, q_k) \in \theta_3$ and since $(q_k, b) \in \theta_3$, we have $(a, b) \in \theta_3 \subseteq \theta_1 \vee \theta_3$.
Without loss of generality, we may assume that $a \in B_{\sigma^2(i)}$ and $q_k \in B_{\sigma^3(i)}$. Since $(q_k, b) \in \theta_3$ and $q_k \in B_{\sigma^3(i)}$, we have $b \in B_{\sigma(i)}$ or $b \in B_{\sigma^3(i)}$. Since $a \in B_{\sigma^2(i)}$ and by definition of θ_3, we have $(a, k) \in \theta_3$ for all $k \in B_i$. Since $B_i \neq \emptyset$, there is a $x \in B_i$ such that $(a, x) \in \theta_3$. Since $x \in B_i$ and by the definition of θ_1, we have $(x, l) \in \theta_1$ for all $l \in B_{\sigma(i)}$. Since $B_{\sigma(i)} \neq \emptyset$, there is a $s \in B_{\sigma(i)}$ such that $(x, s) \in \theta_1$. Since $s \in B_{\sigma(i)}$ and by the definition of θ_3, we have $(s, m) \in \theta_3$ for all $m \in B_{\sigma^3(i)}$. Since $q_k \in B_{\sigma^3(i)}$, we have $(s, q_k) \in \theta_3$. Thus $a\ \theta_3\ x\ \theta_1\ s\ \theta_3\ q_k\ \theta_3\ b$ which implies that $(a, b) \in \theta_1 \vee \theta_3$. So, $\theta_2 \vee \theta_3 \subseteq \theta_1 \vee \theta_3$.
Next, we assume that $(q_j, q_{j+1}) \notin \theta_3$ for each $k \leq j \leq t-1$. The finitary of $\{a = q_0, q_1, \ldots, q_t = b\}$ implies that there is a greatest element $q_r \in \{a = q_0, q_1, \ldots, q_t = b\}$ such that $(q_{c-1}, q_c) \in \theta_3$ for each $k+1 \leq c \leq r$ but $(q_r, q_{r+1}) \in \theta_2$, and so, the transitivity of θ_3 implies that $(q_k, q_r) \in \theta_3$.
Now, we have $(a, q_k) \in \theta_2$ and $(q_k, q_r) \in \theta_3$. The proof above implies that $(a, q_r) \in \theta_1 \vee \theta_3$. Since $(q_r, q_{r+1}) \in \theta_2$, we can prove by continuing in this process, and so, $\theta_2 \vee \theta_3 \subseteq \theta_1 \vee \theta_3$.
Hence, $\theta_1 \vee \theta_3 = \theta_2 \vee \theta_3$.
So, $\{\theta_1, \theta_2, \theta_3, \theta_1 \wedge \theta_3, \theta_1 \vee \theta_3\}$ is a sublattice of the congruence lattice of $(A; f)$ which is isomorphic to N_5 (see Figure 9). Hence, by $M_3 - N_5$ Theorem, the congruence lattice of $(A; f)$ is not modular.

□

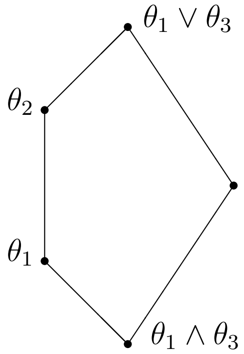


Figure 9. A sublattice of the congruence lattice of $(A; f)$ which is isomorphic to N_5

We note from Proposition 4.7 that the congruence lattice of $(A; f)$ is not modular if the cardinality of A is more than three and f is an identity on A.

We will now prove sufficient conditions for a permutation f on A whose the congruence lattice of $(A; f)$ is modular which is not distributive.

Proposition 4.8. *Let $(A; f)$ be a symmetric algebra with $|A| \geq 4$. If f is a product of three disjoint cycles (can be of length 1) and each pair of them are of relatively prime lengths, then the congruence lattice of $(A; f)$ is modular which is not distributive.*

Proof. Assume that f is a product of three disjoint cycles $\alpha_1\alpha_2\alpha_3$ where one or two of them can be of length 1 and each pair of α_i and α_j with $1 \leq i \neq j \leq 3$ are relatively prime lengths. Let B_i be a subset of A whose elements are in α_i for each $i \in \{1, 2, 3\}$. Then, $f|_{B_i}$ is a cycle on B_i for all $i \in \{1, 2, 3\}$. Proposition 4.5 implies that the congruence lattice of $(B_i; f|_{B_i})$ is a product of chains for each $i \in \{1, 2, 3\}$. Since the lengths of α_i and α_j for $1 \leq i \neq j \leq 3$ are relatively prime, Proposition 4.5 implies that the congruence lattice of $(B_i \cup B_j; f|_{B_i \cup B_j})$ is a linear sum of a product of chains P with a one-element chain $\underline{1}$.

Claim 1: If $\theta \in Con(A; f)\backslash\{A \times A\}$, then θ is one of the following forms:

$$\theta = \cup_{i=1}^{3}\theta_{B_i} \quad \text{or} \quad \theta = \theta_{B_i \cup B_j} \cup \theta_{B_k}.$$

Assume that $\theta \in Con(A; f)\backslash\{A \times A\}$. Then $\theta_{B_i} \subseteq \theta$ for all $i \in \{1, 2, 3\}$. If $\theta = \Delta_A$, then $\theta_{B_i} = \Delta_{B_i}$ for all $i \in \{1, 2, 3\}$. Since $A = B_1 \cup B_2 \cup B_3$, we have $\Delta_A = \cup_{i=1}^{3}\Delta_{B_i} = \cup_{i=1}^{3}\theta_{B_i}$. We will consider $\theta \in Con(A; f)\backslash\{\Delta_A, A \times A\}$ and $\theta \neq \cup_{i=1}^{3}\theta_{B_i}$. Since $\theta_{B_i} \subseteq \theta$ for all $i \in \{1, 2, 3\}$ and $\theta_{B_i \cup B_j} \subseteq \theta$ for all $1 \leq i \neq j \leq 3$, we have $\theta_{B_i \cup B_j} \cup \theta_{B_k} \subseteq \theta$.
Now, let $(x, y) \in \theta$. Since $\theta \neq \cup_{i=1}^{3}\theta_{B_i}$, $\{x, y\} \nsubseteq B_i$ for all $i \in \{1, 2, 3\}$. Since $A = B_1 \cup B_2 \cup B_3$, there are $1 \leq i \neq j \leq 3$ such that $x \in B_i$ and $y \in B_j$. Since $B_i \cap B_j = \emptyset$, we have $(x, y) \in \theta_{B_i \cup B_j} \subseteq \theta_{B_i \cup B_j} \cup \theta_{B_k}$. So, $\theta \subseteq \theta_{B_i \cup B_j} \cup \theta_{B_k}$.
Hence, $\theta = \theta_{B_i \cup B_j} \cup \theta_{B_k}$.

Claim 2: For each $1 \leq i \neq j \leq 3$ and $k \notin \{i, j\}$, $Con(B_i \cup B_j; f|_{B_i \cup B_j}) \times Con(B_k; f|_{B_k})$ can be embedded as a sublattice of $Con(A; f)$.
We define $\beta : Con(B_i \cup B_j; f|_{B_i \cup B_j}) \times Con(B_k; f|_{B_k}) \longrightarrow Con(A; f)$ by
$(\theta, \phi) \longmapsto \bar{\theta} \vee \bar{\phi}$ where $\bar{\theta} = \theta \cup \Delta_{B_k}$ and $\bar{\phi} = \phi \cup \Delta_{B_i \cup B_j}$ for all $\theta \in Con(B_i \cup B_j; f|_{B_i \cup B_j})$ and $\phi \in Con(B_k; f|_{B_k})$.
Let $\theta_t \in Con(B_i \cup B_j; f|_{B_i \cup B_j})$ and $\phi_t \in Con(B_k; f|_{B_k})$ for each $t \in \{1, 2\}$. Since $B_i \cap B_j = \emptyset$ for all $i \in \{1, 2, 3\}$ and $B_1 \cup B_2 \cup B_3 = A$, we have $\bar{\theta}_t \cup \bar{\phi}_t = \bar{\theta}_t \vee \bar{\phi}_t$ for each $t \in \{1, 2\}$. Thus

$$\begin{aligned}
(\theta_1, \phi_1) \subseteq (\theta_2, \phi_2) &\Longleftrightarrow \theta_1 \subseteq \theta_2 \;\; \textit{and} \;\; \phi_1 \subseteq \phi_2 \\
&\Longleftrightarrow \bar{\theta}_1 \subseteq \bar{\theta}_2 \;\; \textit{and} \;\; \bar{\phi}_1 \subseteq \bar{\phi}_2 \\
&\Longleftrightarrow \bar{\theta}_1 \cup \bar{\phi}_1 \subseteq \bar{\theta}_2 \cup \bar{\phi}_2, \\
&\Longleftrightarrow \bar{\theta}_1 \vee \bar{\phi}_1 \subseteq \bar{\theta}_2 \vee \bar{\phi}_2, \\
&\Longleftrightarrow \beta(\theta_1, \phi_1) \subseteq \beta(\theta_2, \phi_2).
\end{aligned}$$

So, β is an order-embedding.

For each $i \in \{1,2,3\}$, let C_i be a sublattice of $Con(A;f)$ which is isomorphic to $Con(B_i \cup B_{\sigma(i)}; f|_{B_i \cup B_{\sigma(i)}}) \times Con(B_{\sigma^2(i)}; f|_{B_{\sigma^2(i)}})$ and let m_i be the greatest element of C_i.

Claim 3: m_1, m_2 and m_3 are the only co-atoms of $Con(A;f)$.
First of all, we will show that $m_i \neq A \times A$ for each $i \in \{1,2,3\}$.
Let $i \in \{1,2,3\}$. Since $|A| \geq 4$ and $\{B_1, B_2, B_3\}$ is a partition of A, there are $x \in B_i$ and $y \in B_{\sigma^2(i)}$. Therefore, $(x,y) \notin m_i$. So, $m_i \neq A \times A$ for each $i \in \{1,2,3\}$.
Next, let $i \in \{1,2,3\}$ and let $\theta \in Con(A;f)$ such that $m_i \subset \theta \subseteq A \times A$. Then there exist $a, b \in A$ such that $(a,b) \in \theta$ but $(a,b) \notin m_i$. Thus $\{a,b\} \nsubseteq B_i \cup B_{\sigma(i)}$ and $\{a,b\} \nsubseteq B_{\sigma^2(i)}$. Since $\{B_1, B_2, B_3\}$ is a partition of A, we may assume that $a \in B_i$ and $b \in B_{\sigma^2(i)}$. Now, let $x, y \in A$. If $\{x,y\} \subseteq B_i \cup B_{\sigma(i)}$ or $\{x,y\} \subseteq B_{\sigma^2(i)}$ then $(x,y) \in m_i$ for some $i \in \{1,2,3\}$. If $\{x,y\} \nsubseteq B_i \cup B_{\sigma(i)}$ and $\{x,y\} \nsubseteq B_{\sigma^2(i)}$, we may assume that $x \in B_i \cup B_{\sigma(i)}$ and $y \in B_{\sigma^2(i)}$. Then $x, a \in B_i \cup B_{\sigma(i)}$; and so, $(x,a) \in m_i \subseteq \theta$ and $(b,y) \in m_i \subseteq \theta$. Since $(a,b) \in \theta$ and by the transitivity of θ, we have $(x,y) \in \theta$. So, $\theta = A \times A$.
Hence, m_i is a co-atom of $Con(A;f)$ for each $i \in \{1,2,3\}$.
Finally, let $\theta \in Con(A;f)$ be such that $\theta \nsubseteq m_i$ for each $i \in \{1,2,3\}$. Then for each $i \in \{1,2,3\}$, there are $a,b,c,d,p,q \in A$ such that $(a,b) \in \theta$, $(c,d) \in \theta$ and $(p,q) \in \theta$ but $(a,b) \notin m_i$, $(c,d) \notin m_{\sigma(i)}$ and $(p,q) \notin m_{\sigma^2(i)}$. Hence, by the definition of m_i, $m_{\sigma(i)}$ and $m_{\sigma^2(i)}$, we have

$$a \in B_i \cup B_{\sigma(i)} \text{ and } b \in B_{\sigma^2(i)},$$
$$c \in B_{\sigma(i)} \cup B_{\sigma^2(i)} \text{ and } d \in B_i,$$
$$p \in B_{\sigma^2(i)} \cup B_i \text{ and } q \in B_{\sigma(i)}.$$

If $a \in B_i$, the cyclically of f and $(a,b) \in \theta$ implies that $(x,y) \in \theta$ for all $x, y \in B_i \cup B_{\sigma^2(i)}$. From $(p,q) \in \theta$, we have either $(s,t) \in \theta$ for all $s,t \in B_{\sigma(i)} \cup B_{\sigma^2(i)}$ or $(s,t) \in \theta$ for all $B_i \cup B_{\sigma(i)}$.
In any cases, the transitivity of θ implies that $(s,t) \in \theta$ for all $s,t \in A$. Hence, $\theta = A \times A$.
We can also prove similarly for the case $a \in B_{\sigma(i)}$ that $\theta = A \times A$.
Therefore, m_1, m_2 and m_3 are the only co-atoms of $Con(A;f)$.
It is clearly, $m_i \vee m_{\sigma(i)} = A \times A$, for each $i \in \{1,2,3\}$.
Let m be the greatest element of the sublattice $C := \bigcap_{i=1}^{3} C_i$ of $Con(A;f)$.

Claim 4: $m = m_i \wedge m_{\sigma(i)}$, for each $i \in \{1,2,3\}$.
Let $i \in \{1,2,3\}$. It is clearly, m is a lower bound of $\{m_1, m_2, m_3\}$. So, $m \subseteq m_i \wedge m_{\sigma(i)}$.
Let θ is a lower bound of $\{m_i, m_{\sigma(i)}\}$. Then $\theta \subseteq m_i$ and $\theta \subseteq m_{\sigma(i)}$. Thus $\theta \in C_i$ and $\theta \in C_{\sigma(i)}$. So, $\theta \in C_i \cap C_{\sigma(i)}$ which implies that $\theta \subseteq m$.
Therefore, $m = m_i \wedge m_{\sigma(i)}$ for each $i \in \{1,2,3\}$.
From Claim 3 and Claim 4, we have that $\{m, m_1, m_2, m_3, A \times A\}$ is a sublattice of

$Con(A;f)$ which is isomorphic to M_3. Therefore, $M_3 - N_5$ Theorem implies that $Con(A;f)$ is not distributive.

Now, we will show that $Con(A;f)$ has no sublattice which is isomorphic to N_5. Note that: if $\theta, \phi \in Con(A;f)$ such that $\phi \subseteq \theta$ then $\theta, \phi \in C_i$ for some $i \in \{1,2,3\}$. Let $\theta, \phi, \varphi \in Con(A;f)$ such that $\phi \subset \theta$, $\varphi \,||\, \theta$ and $\varphi \,||\, \phi$. Then there exists a $1 \leq i \leq 3$ such that $\theta, \phi \in C_i$. If $\varphi \in C_i$ then $\theta, \phi, \varphi \in C_i$ and so, the distributivity of C_i imply that $\phi \wedge \varphi \neq \theta \wedge \varphi$ and $\phi \vee \varphi \neq \theta \vee \varphi$. We consider the case $\varphi \in C_j$ for some $1 \leq j \neq i \leq 3$. If $\varphi \in C$ then the distributivity of C_i imply that $\phi \wedge \varphi \neq \theta \wedge \varphi$ and $\phi \vee \varphi \neq \theta \vee \varphi$. We consider the case $\varphi \in C_j \backslash C$.
If $\theta \in C_i \backslash C$ and $\phi \in C$, then $\theta \vee \varphi = A \times A$ and $\phi \vee \varphi = m_j$. Thus $\phi \vee \varphi \subset \theta \vee \varphi$.
If $\theta, \phi \in C_i \backslash C$, by claim 1, $\theta = \theta_{B_i \cup B_{\sigma(i)}} \cup \theta_{B_{\sigma^2(i)}}$ and $\varphi = \varphi_{B_j \cup B_{\sigma(j)}} \cup \varphi_{B_{\sigma^2(j)}}$. Thus

$$\begin{aligned}
\theta \wedge \varphi &= (\theta_{B_i \cup B_{\sigma(i)}} \cup \theta_{B_{\sigma^2(i)}}) \cap (\varphi_{B_j \cup B_{\sigma(j)}} \cup \varphi_{B_{\sigma^2(j)}}) \\
&\supset (\phi_{B_i \cup B_{\sigma(i)}} \cup \phi_{B_{\sigma^2(i)}}) \cap (\varphi_{B_j \cup B_{\sigma(j)}} \cup \varphi_{B_{\sigma^2(j)}}) \\
&= \phi \wedge \varphi.
\end{aligned}$$

Therefore, there are no sublattices of $Con(A;f)$ which are isomorphic to N_5. Hence, $Con(A;f)$ is modular.

□

Corollary 4.9. *If $(A;f)$ is a symmetric algebra with $|A| \geq 4$ then there exist co-atoms m_1, m_2 and m_3 of $Con(A;f)$ which satisfy the following conditions:*
(i) *for each $i \in \{1,2,3\}$, $\downarrow m_i$ is a lattice of one of the following forms:*

$$P \quad or \quad P \oplus \underline{1} \quad or \quad (P \oplus \underline{1}) \times Q$$

where P and Q are product of chains.
(ii) *The set $\{m, m_1, m_2, m_3, A \times A\}$ is a sublattice of $Con(A;f)$ which is isomorphic to M_3 where m is the greatest element of a sublattice $\bigcap_{i=1}^{3} \downarrow m_i$ of $Con(A,f)$.*

The proof of Corollary 4.9 is followed by Proposition 4.7 and Proposition 4.8.

Definition 4.10. *Let L be a lattice with the greatest element* 1*. We say that L is a M_3-***head lattice** *if L satisfies the following conditions:*
(i) *L contains exactly three co-atoms m_1, m_2 and m_3 which $\downarrow m_i$ satisfy the Condition* (i) *of Corollary 4.9 for each $i \in \{1,2,3\}$, and*
(ii) *The set $\{m, m_1, m_2, m_3, 1\}$ forms a sublattice of L which is isomorphic to M_3 where m is the greatest element of $\bigcap_{i=1}^{3} \downarrow m_i$.*

Proposition 4.11. *M_3-head lattice is a modular which is not distributive.*

We can prove Proposition 4.11 similarly of the proof of Proposition 4.8.

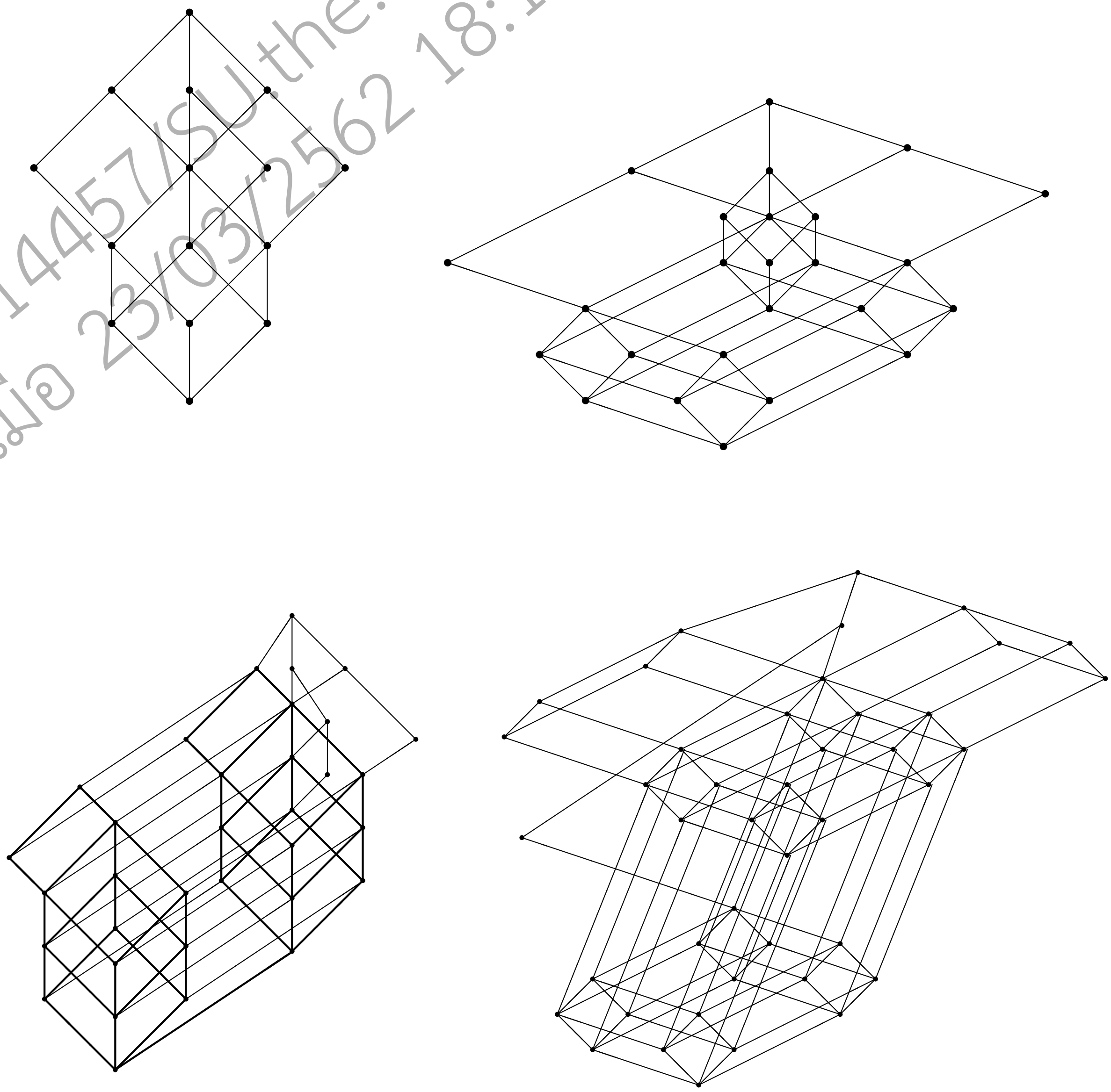


Figure 10. The congruence lattices of some symmetric algebras whose the permutation is a product of three disjoint cycles whose lengths are relatively prime; and, one or two of them can be of length 1.

Theorem 4.12 shows a characterization of a permutation f on a finite set A whose $(A; f)$ is congruence-modular and the proof of the theorem is followed directly by Proposition 4.7, Proposition 4.8, Corollary 4.9 and Proposition 4.11.

Theorem 4.12. *Let* $\bar{A} := (A; f)$ *be a symmetric algebra. Then the followings are equivalent:*
(i) $\bar{A}$ *is a congruence-modular,*
(ii) *Conditions* (i), (ii) *or* (iii) *of Proposition 4.7 are satisfied,*
(iii) $Con(\bar{A})$ *is either a product of chains or a linear sum of a product of chains with one-element chain or a* M_3*-head lattice.*

Chapter 5

All Congruence-modular Near-symmetric Algebras

In chapter 4, we characterize all unary operations f on a finite set A with $\lambda(f) = 0$ whose algebra is congruence-distributive or congruence-modular. In this chapter, we will study in a similar way for characterizations of all unary operations f on a finite set A with $\lambda(f) = 1$ whose algebra is congruence-distributive or congruence-modular.

Let A be a finite set and let f be a unary operation on A with $\lambda(f) = 1$. Then we call $(A; f)$ a **near-symmetric algebra**.
Recall that $\lambda(f) = 1$ if and only if $Imf = Imf^2$.

The following proposition proves a characterization of a unary operation f on a finite set A with $\lambda(f) = 1$.

Proposition 5.1. *Let A be a finite set with $|A| \geq 2$ and let f be a unary operation on A. Then the followings are equivalent:*
1. $\lambda(f) = 1$,
2. *there is a $\emptyset \neq B \subset A$ such that $B \cap Imf = \emptyset$ and $f|_{A\backslash B}$ is a permutation,*
3. *$Imf \subset A$ and $f|_{Imf}$ is a permutation, and*
4. *$Imf \subset A$ and $B \cap Imf$ is a one-element set for all $B \in A_{/_{kerf}}$.*

Proof. (1) $\Rightarrow$ (2) Assume that $\lambda(f) = 1$. Then $Imf \subset A$. Therefore, there is a $\emptyset \neq B \subset A$ such that $A = B\dot{\cup}Imf$ is a disjoint union and $f|_{Imf^{\lambda(f)}}$ is a permutation. Since $\lambda(f) = 1$ and $Imf = A - B$, we have $f|_{A\backslash B}$ is a permutation.

(2) $\Rightarrow$ (3) Assume that there is a $\emptyset \neq B \subset A$ such that $B \cap Imf = \emptyset$ and $f|_{A\backslash B}$ is a permutation. Then, clearly, $Imf \subset A$. Now, we will show that $A\backslash B = Imf$. Clearly, $Imf \subseteq A\backslash B$. Let $x \in A\backslash B$. Since $f|_{A\backslash B}$ is a permutation, $x \in Imf|_{A\backslash B}$, and so, $x \in Imf$, that is $A\backslash B \subseteq Imf$. So, $A\backslash B = Imf$. Hence, $f|_{Imf}$ is a permutation.

(3) $\Rightarrow$ (4) Assume that $Imf \subset A$ and $f|_{Imf}$ is a permutation. Let $B \in A_{/kerf}$. Then for each $b \in B$, there is a $c \in A$ such that $f(b) = c$, that is $f(B) = \{c\}$. Since $f|_{Imf}$ is a permutation, $B \cap Imf$ is singleton.

(4) $\Rightarrow$ (1) From (4), we have $f|_{Imf}$ is a permutation; and together with $Imf \subset A$, we have $\lambda(f) = 1$.

$\square$

Note that: the congruence lattice of any two-element algebra $(A; f)$ is the two-element chain $\{\Delta_A, \nabla_A\}$. We will consider the case that the cardinality of A is more than two.

The following proposition provides some necessary conditions of a near-symmetric algebra which is congruence-distributive and congruence-modular.

Proposition 5.2. *Let $(A\,; f)$ be a near-symmetric algebra with $|A| = n \geq 3$.*
1. *If $(A\,; f)$ is congruence-modular, then $A/_{kerf}$ contains only one block whose cardinality more than one.*
2. *If $(A\,; f)$ is congruence-distributive, then $|Imf| = n - 1$.*

Proof. (1) Assume that $(A\,; f)$ is congruence-modular. Since $\lambda(f) = 1$, we have $A/_{kerf} = \{B_1, B_2, \ldots, B_t\}$ for some integers $t \geq 1$. By Proposition 5.1, we may assume that there are $1 \leq s \leq t$ such that $B_1, B_2, \ldots, B_s$ are the blocks which have more than one-element and $B_i \cap Imf$ is a one-element set for all $1 \leq i \leq t$ and $f|_{Imf}$ is a permutation. Let $f|_{Imf} := \alpha_1\alpha_2\ldots\alpha_r$ for some $r \geq 2$ where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are disjoint cycles.
Suppose that $s \geq 2$. Then $|B_1| > 1$ and $|B_2| > 1$. Let $f(B_1) = \{b_1\}$ and $f(B_2) = \{b_2\}$. Then $b_1 \neq b_2$. Since $B_i \cap Imf$ is singleton for all $1 \leq i \leq t$ and $|B_1| > 1$ and $|B_2| > 1$, there are $u \in B_1$ and $v \in B_2$ such that $u, v \notin Imf$ and there are $a_1 \neq a_2$ such that $a_i \in B_i \cap Imf$ for all $i \in \{1, 2\}$. So, a_i and b_i are in the same cycle α_j for each $i \in \{1, 2\}$ and for some $1 \leq j \leq r$.
Let C be the union of cycles containing b_1 and b_2 and define $\theta_1 := \Delta_A \cup \{(x, y) | x, y \in C\}$ and $\theta_2 := \theta_1 \cup \{(u, v), (v, u)\}$. Then θ_1 and θ_2 are invariant under f and $\Delta_A \subset \theta_1 \subset \theta_2$. Since $(u, v) \notin kerf$ and $B_i \cap Imf$ is a one-element set for each $i \in \{1, 2\}$, we have $\theta_1 \cap kerf = \Delta_A = \theta_2 \cap kerf$. Since $u\ kerf\ a_1\ \theta_1\ b_1\ \theta_1\ b_2\ \theta_1\ a_2\ kerf\ v$, we have $(u, v) \in \theta_1 \vee kerf$. So, $\theta_1 \vee kerf = \theta_2 \vee kerf$. Therefore, $\{\Delta_A, \theta_1, \theta_2, kerf, \theta_1 \vee kerf\}$ is a sublattice of the congruence lattice of $(A; f)$ which is isomorphic to N_5; a contradiction. So, $s = 1$.

(2) Assume that $(A\,; f)$ is congruence-distributive. Then, it is congruence-modular. By part (1), $A/_{kerf}$ contain exactly one block B such that $|B| \geq 2$.
Now, we want to show that $|B| = 2$. Suppose that $|B| > 2$. Then there are $x \neq y$ such that $x, y \in B$ and there exists only one $z \in B \cap Imf$.
Now, we define
$\theta_1 = \Delta_A \cup \{(x, y), (y, x)\}$,

$\theta_2 = \Delta_A \cup \{(y,z),(z,y)\}$,
and $\theta_3 = \Delta_A \cup \{(x,z),(z,x)\}$.
Since x,y,z are in the same block B of $A/_{kerf}$, all θ_1, θ_2 and θ_3 are invariant under f. It is clear from the definitions of θ_1, θ_2 and θ_3 that $\theta_1 \cap \theta_2 = \theta_1 \cap \theta_3 = \theta_2 \cap \theta_3 = \Delta_A$. Now, $\theta_1 \vee \theta_2$, $\theta_1 \vee \theta_3$ and $\theta_2 \vee \theta_3$ are the least equivalence relations on A containing $\{(x,y),(y,x),(y,z),(z,y),(z,x),(x,z)\}$; they are the same relations. Hence, $\{\Delta_A, \theta_1, \theta_2, \theta_3, \theta_1 \vee \theta_3\}$ is a sublattice of the congruence lattice of $(A;f)$ which is isomorphic to M_3. Therefore, the congruence lattice of $(A;f)$ is not distributive; a contradiction. So, $|B| = 2$. Hence, $|Imf| = n-1$.

□

The next proposition shows the forms of the congruence lattice of a near-symmetric algebra $(A;f)$ with $|Imf| = n-1$.

Proposition 5.3. *Let $(A;f)$ be a near-symmetric algebra with $|A| = n \geq 4$ and $|Imf| = n-1$. Then $Con(A;f)$ is isomorphic to $\underline{2} \times Con(Imf;f)$.*

Proof. Let B be the only one block of $A_{/_{kerf}}$ with $|B| = 2$.
Let $u \in B - Imf$ and $b \in B \cap Imf$. Then $f(u) = f(b)$.
Assume that $\theta \in Con(Imf;f)$. It is clear that $\theta \cup \{(u,u)\} \in Con(A;f)$. Now, we define $\bar{\theta} := \theta \cup \{(x,y) | x,y \in [b]_\theta \cup \{u\}\}$ and let $(x,y) \in \bar{\theta}$ with $x \neq y$. If $(x,y) \in \theta$, then $(f(x),f(y)) \in \theta \subseteq \bar{\theta}$. We may assume that $(x,y) = (u,c)$ for some $c \in [b]_\theta$.

Case 1: $f(b) = b$. Then $(f(x),f(y)) = (f(u),f(c)) = (f(b),f(c)) = (b,f(c))$; so, $b, f(c) \in [b]_\theta$ which implies that $(b,f(c)) \in \bar{\theta}$.

Case 2: $f(b) \neq b$. Then $b,c \in [b]_\theta$ implies that $(b,c) \in \theta$; so, $(f(b),f(c)) \in \theta$. Since $(f(u),f(c)) = (f(b),f(c))$, we have $(f(x),f(y)) = (f(u),f(c)) = (f(b),f(c)) \in \theta \subseteq \bar{\theta}$.

In either cases, $\bar{\theta}$ is invariant under f.
We define $g : \underline{2} \times Con(Imf;f) \longrightarrow Con(A;f)$ for each $\theta \in Con(Imf;f)$ by $g((0,\theta)) = \theta \cup \{(u,u)\}$ and $g((1,\theta)) = \theta \cup \{(x,y) | x,y \in [b]_\theta \cup \{u\}\}$. Then, clearly, g is an order-embedding. Now, let $\bar{\theta} \in Con(A;f)$. If $[u]_{\bar{\theta}}$ is singleton, then $\theta = \bar{\theta} - \{(u,u)\} \in Con(Imf;f)$ with $g((0,\theta)) = \bar{\theta}$. But, if $[u]_{\bar{\theta}}$ is not singleton, then $f(u)$ and b are in the block $[u]_{\bar{\theta}}$ since $f(u) = f(b)$. Let $B := [u]_{\bar{\theta}} - \{u\}$. Then $B \neq \emptyset$ and $\mathcal{P} := (A_{/_{\bar{\theta}}} - \{[u]_{\bar{\theta}}\}) \cup \{B\}$ is a partition of Imf. Let θ be the corresponding equivalence relation on Imf to $\mathcal{P}$. Then, clearly, θ is invariant under f and $g((1,\theta)) = \bar{\theta}$. Therefore, g is an order-isomorphism.

□

The following corollary is a consequent of Proposition 5.3.

Corollary 5.4. *Let $(A;f)$ be a near-symmetric algebra with $|A| = n \geq 4$ and $|Imf| = n-1$. Then $Con(Imf;f)$ can be embedded as a sublattice of $Con(A;f)$.*

Lemma 5.5. *Let $(A; f)$ be a near-symmetric algebra with $|A| = n \geq 4$ and $|Imf| = n-1$. If $f|_{Imf}$ is an identity function, the congruence lattice of $(A; f)$ is not distributive.*

Proof. Since $|Imf| = n-1$, we have $|Imf| \geq 3$. Remark 4.2 implies that the congruence lattice of $(Imf; f)$ is not distributive. So, by Corollary 5.4, the congruence lattice of $(A; f)$ is not distributive.

□

The following theorem shows some characterizations of a congruence-distributive near-symmetric algebra.

Theorem 5.6. *Let $(A; f)$ be a near-symmetric algebra with $|A| = n \geq 4$. Then the followings are equivalent:*
1. *$(A; f)$ is congruence-distributive,*
2. *$|Imf| = n-1$ and $(Imf; f)$ is congruence-distributive,*
3. *$|Imf| = n-1$ and $f|_{Imf}$ is one of (i) or (ii) of Proposition 4.1,*
4. *the congruence lattice of $(A; f)$ is one of the followings:*

$$\underline{2} \times P \quad \text{or} \quad \underline{2} \times (P \oplus \underline{1})$$

where P is a product of chains.

Proof. (1) $\Rightarrow$ (2) Assume that $(A; f)$ is congruence-distributive. Then, by part (2) of Proposition 5.2, $|Imf| = n-1$. Hence, Proposition 2.50 and Corollary 5.4 imply that $(Imf; f)$ is congruence-distributive.

(2) $\Rightarrow$ (3) Assume that $|Imf| = n-1$ and $(Imf; f)$ is congruence-distributive. By Lemma 5.5, $f|_{Imf}$ is not an identity function; so, Proposition 4.1 implies the conclusion.

(3) $\Rightarrow$ (4) Assume that $|Imf| = n-1$ and $f|_{Imf}$ is one of conditions (i) or (ii) of Proposition 4.1. If $f|_{Imf}$ is a cycle having no fixed point, Proposition 4.5 and Proposition 5.3 imply that $Con(A; f)$ is of the form $\underline{2} \times P$ where P is a product of chains. If $f|_{Imf}$ is a cycle with one fixed point or $f|_{Imf}$ satisfies (ii) of Proposition 4.1 then Proposition 4.5 and Proposition 5.3 imply that $Con(A; f)$ is of the form $\underline{2} \times (P \oplus \underline{1})$ where P is a product of chains.

(4) $\Rightarrow$ (1) Lemma 2.48 and Proposition 2.50 imply that the lattice of the forms $\underline{2} \times P$ and $\underline{2} \times (P \oplus \underline{1})$ where P is a product of chains are distributive.

□

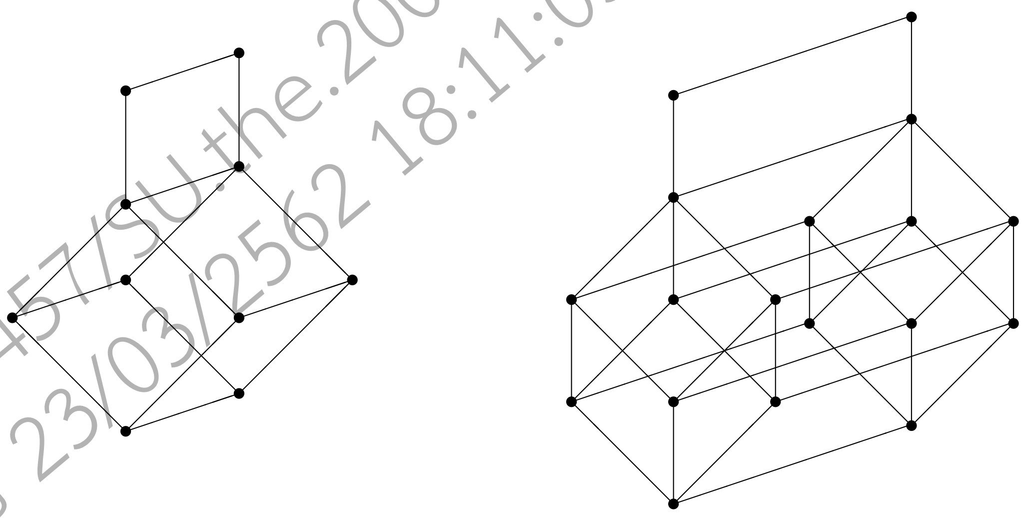


Figure 11. The congruence lattices of some congruence-distributive near-symmetric algebras.

In the following proposition, we prove a necessary condition of a congruence-modular near-symmetric algebra.

Proposition 5.7. *Let $(A; f)$ be a near-symmetric algebra with $|A| = n \geq 4$. If $(A; f)$ is congruence-modular, then $|Imf| = n - 1$ or $|Imf| = n - 2$.*

Proof. Assume that $(A; f)$ is congruence-modular and $|Imf| \leq n - 3$. By Proposition 5.2(1), there are $a, b, c, d \in A$ such that $f(a) = f(b) = f(c) = f(d)$. Then for each $i \in \{1, 2, 3\}$, we define $\theta_i \subseteq A \times A$ as the follows:
$\theta_1 = \Delta_A \cup \{(a, b), (b, a)\}$,
$\theta_2 = \theta_1 \cup \{(c, d), (d, c)\}$,
and $\theta_3 = \Delta_A \cup \{(a, c), (c, a), (b, d), (d, b)\}$.
Since $f(a) = f(b) = f(c) = f(d)$, we have that θ_i is invariant under f for each $i \in \{1, 2, 3\}$. Then $\theta_1 \subseteq \theta_2, \theta_1 \cap \theta_3 = \Delta_A = \theta_2 \cap \theta_3$ and $\theta_1 \vee \theta_3 = \Delta_A \cup \{(x, y) | x, y \in \{a, b, c, d\}\} = \theta_2 \vee \theta_3$. So, $\{\theta_1, \theta_2, \theta_3, \Delta_A, \theta_1 \vee \theta_3\}$ is a sublattice of the congruence lattice of $(A; f)$ which is isomorphic to N_5. Hence, $M_3 - N_5$ Theorem implies that the congruence lattice of $(A; f)$ is not modular, a contradiction. So, $|Imf| \geq n - 2$. But, $|Imf| \leq |A| - 1 = n - 1$ implies that $|Imf| = n - 1$ or $|Imf| = n - 2$. □

The next proposition shows the forms of the congruence lattice of a congruence-modular algebra.

Proposition 5.8. *Let $(A; f)$ be a congruence-modular near-symmetric algebra with $|A| = n \geq 4$.*
(i) *If $|Imf| = n - 1$, then $Con(A; f)$ is isomorphic to $\underline{2} \times Con(Imf; f)$,*
(ii) *If $|Imf| = n - 2$, then $Con(A; f)$ is isomorphic to $M_3 \times Con(Imf; f)$.*

Proof. (i) follows from Proposition 5.3.

(ii) Suppose that $|Imf| = n-2$. Since $Con(A;f)$ is modular, Proposition 5.2 implies that $A/_{kerf}$ contains only one block whose cardinality is more than one.

Let B be the only one block of $A/_{kerf}$ whose cardinality is more than one; that is, $|B| \geq 2$. If $|B| = 2$, then $|Imf| = n-1$, a contradiction. Therefore, $|B| \geq 3$. We will show that $|B| \leq 3$. Suppose that $|B| \geq 4$. Then there are distinct elements $x, y, u, v \in A$ such that $f(x) = f(y) = f(u) = f(v)$. We define

$\theta_1 = \Delta_A \cup \{(x,y),(y,x)\}$,

$\theta_2 = \theta_1 \cup \{(u,v),(v,u)\}$,

and $\theta_3 = \Delta_A \cup \{(x,u),(u,x),(y,v),(v,y)\}$.

It is clearly, θ_i is invariant under f for each $i \in \{1,2,3\}$. Then $\theta_1 \subset \theta_2, \theta_1 \cap \theta_3 = \Delta_A = \theta_2 \cap \theta_3$ and $\theta_1 \vee \theta_3 = \Delta_A \cup \{(a,b) | a,b \in \{x,y,u,v\}\} = \theta_2 \vee \theta_3$. So, $\{\theta_1, \theta_2, \theta_3, \Delta_A, \theta_1 \vee \theta_3\}$ is a sublattice of $Con(A;f)$ which is isomorphic to N_5. By $M_3 - N_5$ Theorem, $Con(A;f)$ is not modular, a contradiction. Thus $|B| \leq 3$. Hence, $|B| = 3$.

Let $B = \{a,b,c\}$. Then $f(a) = f(b) = f(c)$. By Proposition 5.1(4), we have $|B \cap Imf| = 1$. Without loss of generality, we may assume that $c \in B \cap Imf$. Let define $\phi_1, \phi_2, \phi_3 \subseteq B \times B$ by:

$\phi_1 = \Delta_B \cup \{(a,b),(b,a)\}$,

$\phi_2 = \Delta_B \cup \{(a,c),(c,a)\}$,

and $\phi_3 = \Delta_B \cup \{(b,c),(c,b)\}$.

Then, clearly, ϕ_1, ϕ_2 and ϕ_3 are congruence relations on B such that $\phi_1 \cap \phi_2 = \Delta_B = \phi_2 \cap \phi_3 = \phi_1 \cap \phi_3$ and $\phi_1 \vee \phi_2 = \Delta_B \cup \{(x,y) | x,y \in B\} = \phi_2 \vee \phi_3 = \phi_1 \vee \phi_3$. So, $\{\phi_1, \phi_2, \phi_3, \Delta_B, \phi_1 \vee \phi_2\}$ form M_3.

Let denote $\{\phi_1, \phi_2, \phi_3, \Delta_B, \phi_1 \vee \phi_2\}$ by $\bar{M}_3$.

We are going to prove that $Con(A;f)$ is isomorphic to $\bar{M}_3 \times Con(Imf;f)$. Let $\phi \in Con(B; f|_B)$ and $\theta \in Con(Imf; f|_{Imf})$.

Define $\bar{\phi} = \phi \cup \{(x,x) | x \in Imf\}$ and $\bar{\theta} = \theta \cup \{(x,x) | x \in B\}$. Then $\bar{\phi}$ and $\bar{\theta}$ are in $Con(A;f)$.

Now, we define

$\alpha : \bar{M}_3 \times Con(Imf;f) \longrightarrow Con(A;f)$ by $\alpha(\phi,\theta) = \bar{\phi} \vee \bar{\theta}$ for all $(\phi,\theta) \in \bar{M}_3 \times Con(Imf;f)$.

and define

$\beta : Con(A;f) \longrightarrow \bar{M}_3 \times Con(Imf;f)$ by $\beta(\theta) = (\theta|_B, \theta|_{Imf})$ for all $\theta \in Con(A;f)$.

We claim that $\alpha \circ \beta = id_{Con(A;f)}$ and $\beta \circ \alpha = id_{\bar{M}_3 \times Con(Imf;f)}$.

Let $\theta \in Con(A;f)$. Then $\alpha(\beta(\theta)) = \alpha((\theta|_B, \theta|_{Imf})) = \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$.

Now, we want to show that $\theta = \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$.

Since $\bar{\theta}|_B \subseteq \theta$ and $\bar{\theta}|_{Imf} \subseteq \theta$, we have $\bar{\theta}|_B \cup \bar{\theta}|_{Imf} \subseteq \theta$. Thus $\bar{\theta}|_B \vee \bar{\theta}|_{Imf} \subseteq \theta$.

On the other hand, let $(x,y) \in \theta$. Then $x, y \in A = B \dot{\cup} Imf$. If $x, y \in B$, then $(x,y) \in \bar{\theta}|_B \subseteq \bar{\theta}|_B \cup \bar{\theta}|_{Imf}$ and if $x, y \in Imf$, then $(x,y) \in \bar{\theta}|_{Imf} \subseteq \bar{\theta}|_B \cup \bar{\theta}|_{Imf}$. Without loss of generality, we may assume that $x \in B$ and $y \in Imf$. If $x = y$, then $x = c$ and $y = c$. Thus $(x,y) \in \bar{\theta}|_B \cup \bar{\theta}|_{Imf}$. So, we assume that $x \neq y$. Then we consider the following cases:

Case1: $x = c$ and $y \neq c$, then $(x, y) \in \bar{\theta}|_{Imf} \subseteq \bar{\theta}|_B \cup \bar{\theta}|_{Imf}$.

Case2: $x \neq c$ and $y = c$, then $(x, y) \in \bar{\theta}|_B \subseteq \bar{\theta}|_B \cup \bar{\theta}|_{Imf}$.

Case3: $x \neq c$ and $y \neq c$, then $x \in \{a, b\}$ and $y \in Imf\backslash\{c\}$.

Since $(x, y) \in \theta$, we have $(x, c) \in \theta|_B$ and $(x, c) \in \theta|_{Imf}$, that is $(x, c), (c, y) \in \theta|_B \cup \theta|_{Imf}$. Thus $(x, y) \in \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$.
In either cases, we conclude that $(x, y) \in \bar{\theta}|_B \cup \bar{\theta}|_{Imf} \subseteq \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$. Thus $\theta \subseteq \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$. Hence, $\theta = \bar{\theta}|_B \vee \bar{\theta}|_{Imf}$, which implies that $\alpha \circ \beta = id_{Con(A;f)}$.
Next, we will show that $\beta \circ \alpha = id_{\bar{M}_3 \times Con(Imf;f)}$.
Let $\phi \in \bar{M}_3$ and $\theta \in Con(Imf; f)$.
Then $\beta(\alpha((\phi, \theta))) = \beta(\bar{\phi} \vee \bar{\theta}) = ((\bar{\phi} \vee \bar{\theta})|_B, (\bar{\phi} \vee \bar{\theta})|_{Imf})$.
Now, we want to show that $\phi = (\bar{\phi} \vee \bar{\theta})|_B$ and $\theta = (\bar{\phi} \vee \bar{\theta})|_{Imf}$.
Since $\phi \in \bar{M}_3$ and $\theta \in Con(Imf; f)$, we have $\phi \subseteq (\phi \cup \theta)|_B \subseteq (\bar{\phi} \cup \bar{\theta})|_B \subseteq (\bar{\phi} \vee \bar{\theta})|_B$ and $\theta \subseteq (\phi \cup \theta)|_{Imf} \subseteq (\bar{\phi} \cup \bar{\theta})|_{Imf} \subseteq (\bar{\phi} \vee \bar{\theta})|_{Imf}$. Thus $\phi \subseteq (\bar{\phi} \vee \bar{\theta})|_B$ and $\theta \subseteq (\bar{\phi} \vee \bar{\theta})|_{Imf}$.
Let $(x, y) \in (\bar{\phi} \vee \bar{\theta})|_B$. Then $x, y \in B$ and there are $q_0 = x, q_1, q_2, \ldots, q_n = y \in A$ such that $(q_i, q_{i+1})) \in \bar{\phi} \cup \bar{\theta}$ for all $0 \leq i \leq n - 1$. But, $x \in B$. So, we consider only two cases: $x \in \{a, b\}$ or $x = c$.

Case 1: $x \in \{a, b\}$.

Since $\{q_0 = x, q_1, q_2, \ldots, q_n = y\}$ is finite, there is the greatest element, q_k, in $\{q_0 = x, q_1, q_2, \ldots, q_n = y\}$ such that $(q_{j-1}, q_j) \in \phi$ for all $1 \leq j \leq k$ but $(q_k, q_{k+1}) \notin \phi$, and so, the transitivity of ϕ implies that $(x, q_k) \in \phi$. Since $(q_{k-1}, q_k) \in \phi$ and $(q_k, q_{k+1}) \notin \phi$, we have $q_k = c$ and $q_{k+1} \in Imf\backslash\{c\}$. So, $(c, q_{k+1}) \in \theta$. If $q_{k+1} = y$, then $y = c$, by the transitivity of θ, we have $(c, c) \in \theta$, and so, $(c, c) \in \phi$. Thus $(x, y) \in \phi$. Now, assume that $q_{k+1} \neq y$. Then there is an integer $l > k$ such that $(q_{t-1}, q_t) \in \theta$ for all $k \leq t \leq l$ but $(q_l, q_{l+1}) \notin \theta$. By transitivity of θ, we have $(q_k, q_l) \in \theta$ and so, $q_l = c$ and $q_{l+1} \in \{a, b\}$. Thus $(c, c) \in \theta$ and so, $(c, c) \in \phi$. Continuing in this process, we have $(x, y) \in \phi$.

Case 2: $x = c$.

If $q_1 \in \{a, b\}$, then $(x, q_1) \in \phi$, and by case 1, we have $(q_1, y) \in \phi$. So, the transitivity of ϕ implies that $(x, y) \in \phi$. We assume that $q_1 \in Imf\backslash\{c\}$. Then $(x, q_1) \in \theta$. Since $\{q_0 = x, q_1, q_2, \ldots, q_n = y\}$ is finite, there is the greatest element, q_s, in $\{q_0 = x, q_1, q_2, \ldots, q_n = y\}$ such that $(q_{r-1}, q_r) \in \theta$ for all $1 \leq r \leq s$ and $(q_s, q_{s+1}) \notin \theta$. So, by transitivity of θ, we have $(x, q_s) \in \theta$, and so, $q_s = c$ and $q_{s+1} \in \{a, b\}$. Since $x = c$ and $q_s = c$, we have $(x, q_s) \in \phi$. Since $q_{s+1} \in \{a, b\}$ and by case 1, we have $(q_{s+1}, y) \in \phi$. By the transitivity of ϕ, we have $(x, y) \in \phi$.
Hence, $(\bar{\phi} \vee \bar{\theta})|_B \subseteq \phi$
Similarly, $(\bar{\phi} \vee \bar{\theta})|_{Imf} \subseteq \theta$. Thus $(\bar{\phi} \vee \bar{\theta})|_B = \phi$ and $(\bar{\phi} \vee \bar{\theta})|_{Imf} = \theta$.
Hence α and β are bijections.
It remain to show that α is a homomorphism.
Let $(\varphi_i, \psi_i) \in \bar{M}_3 \times Con(Imf; f)$ for each $i \in \{1, 2\}$. Then $\alpha((\varphi_1, \psi_1) \vee (\varphi_2, \psi_2)) = \alpha(\varphi_1 \vee \varphi_2, \psi_1 \vee \psi_2) = \overline{\varphi_1 \vee \varphi_2} \vee \overline{\psi_1 \vee \psi_2} = (\bar{\varphi_1} \vee \bar{\varphi_2}) \vee (\bar{\psi_1} \vee \bar{\psi_2}) = (\bar{\varphi_1} \vee \bar{\psi_1}) \vee (\bar{\varphi_2} \vee \bar{\psi_2}) = \alpha(\varphi_1, \psi_1) \vee \alpha(\varphi_2, \psi_2)$ and $\alpha((\varphi_1, \psi_1) \wedge (\varphi_2, \psi_2)) = \alpha(\varphi_1 \wedge \varphi_2, \psi_1 \wedge \psi_2) = \overline{\varphi_1 \wedge \varphi_2} \vee$

$\overline{\psi_1 \wedge \psi_2} = (\bar{\varphi_1} \wedge \bar{\varphi_2}) \vee (\bar{\psi_1} \wedge \bar{\psi_2}) = (\bar{\varphi_1} \wedge \bar{\psi_1}) \wedge (\bar{\varphi_2} \wedge \bar{\psi_2}) = \alpha(\varphi_1, \psi_1) \wedge \alpha(\varphi_2, \psi_2).$
□

Lemma 5.9. *Let $(A; f)$ be a near-symmetric algebra with $|A| = n \geq 6$ such that $|Imf| = n - 1$ or $|Imf| = n - 2$. If $f|_{Imf}$ is an identity function, $Con(A; f)$ is not modular.*

Proof. Since $|Imf| = n - 1$ or $|Imf| = n - 2$, we have $|Imf| \geq 5$ or $|Imf| \geq 4$. Remark 4.2 implies that $Con(Imf; f)$ is not modular. So, by Proposition 5.8, $Con(A; f)$ is not modular.

□

The next theorem shows characterizations of a congruence-modular near-symmetric algebra.

Theorem 5.10. *Let $(A; f)$ be a near-symmetric algebra with $|A| = n \geq 4$. Then the followings are equivalent:*
1. *$(A; f)$ is congruence-modular,*
2. *$(Imf; f)$ is congruence-modular and either $|Imf| = n - 1$ or $|Imf| = n - 2$,*
3. *$f|_{Imf}$ is one of (i) or (ii) or (iii) of Proposition 4.7 and either $|Imf| = n - 1$ or $|Imf| = n - 2$,*
4. *$Con(A; f)$ is one of the following lattices*

$$\underline{2} \times P \quad or \quad \underline{2} \times (P \oplus \underline{1}) \quad or \quad \underline{2} \times L$$

or

$$M_3 \times P \quad or \quad M_3 \times (P \oplus \underline{1}) \quad or \quad M_3 \times L$$

where P is a product of chains and L is a M_3-head lattice.

Proof. (1) ⇒ (2) Assume that $(A; f)$ is congruence-modular. Then, by Proposition 5.7, $|Imf| = n - 1$ or $|Imf| = n - 2$ which implies by Proposition 5.8 that $Con(Imf; f)$ is modular.

(2) ⇒ (3) Assume that $|Imf| = n - 1$ or $|Imf| = n - 2$ and $(Imf; f)$ is congruence-modular. Lemma 5.5 implies that $f|_{Imf}$ is not an identity function; so, $f|_{Imf}$ is one of (i) or (ii) or (iii) of Proposition 4.7.

(3) ⇒ (4) Assume that $|Imf| = n - 1$ or $|Imf| = n - 2$ and $f|_{Imf}$ is one of (i) or (ii) or (iii) of Proposition 4.7. We consider the following cases:

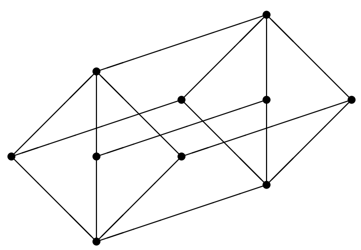
Case1: $|Imf| = n - 1$ and $f|_{Imf}$ is one of (i) or (ii) or (iii) of Proposition 4.7.
If $f|_{Imf}$ is a cycle having no fixed point, Proposition 4.5 and Proposition 5.8(i) imply that $Con(A; f)$ is of the form $\underline{2} \times P$ where P is a product of chains.
If $f|_{Imf}$ is a cycle with one fixed point or α satisfies (ii) of Proposition 4.1 then Proposition 4.5 and Proposition 5.8(i) imply that $Con(A; f)$ is of the form

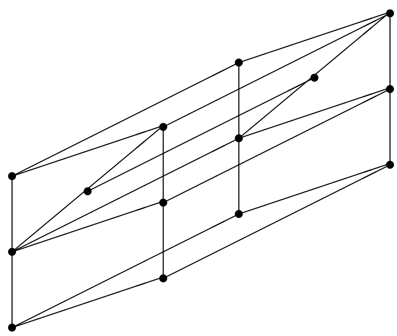
$\underline{2} \times (P \oplus \underline{1})$ where P is a product of chains.
If $f|_{Imf}$ satisfies the condition of Proposition 4.8 then Proposition 5.8(i) implies that $Con(A; f)$ is of the form $\underline{2} \times L$ where L is a M_3-head lattice.

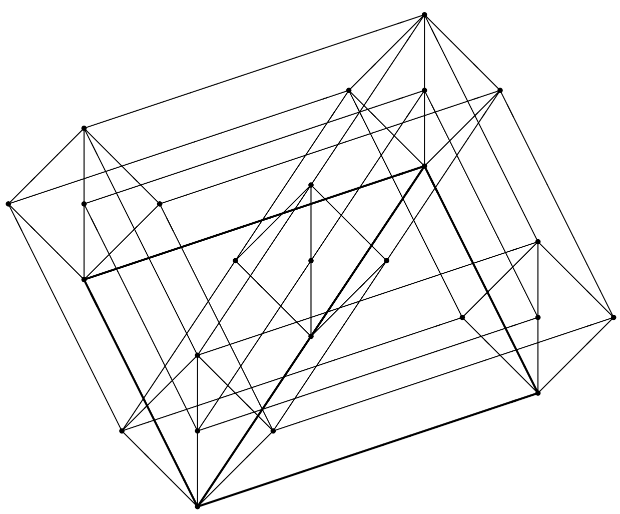
Case2: $|Imf| = n - 2$ and $f|_{Imf}$ is one of (i) or (ii) or (iii) of Proposition 4.7.
If $f|_{Imf}$ is a cycle having no fixed point, then Proposition 4.5 and Proposition 5.8(ii) imply that $Con(A; f)$ is of the form $M_3 \times P$ where P is a product of chains.
If $f|_{Imf}$ is a cycle with one fixed point or f satisfies (ii) of Proposition 4.1, Proposition 4.5 and Proposition 5.8(ii) imply that $Con(A; f)$ is of the form $M_3 \times (P \oplus 1)$ where P is a product of chains.
If $f|_{Imf}$ satisfies the condition of Proposition 4.8, then Proposition 5.8(ii) implies that $Con(A; f)$ is of the form $M_3 \times L$ where L is a M_3-head lattice.

(4) $\Rightarrow$ (1) If the congruence lattice of a near-symmetric algebra $(A; f)$ is one of the form in (4), then Lemma 2.48 and Proposition 2.50 imply that $(A; f)$ is a congruence-modular.

□







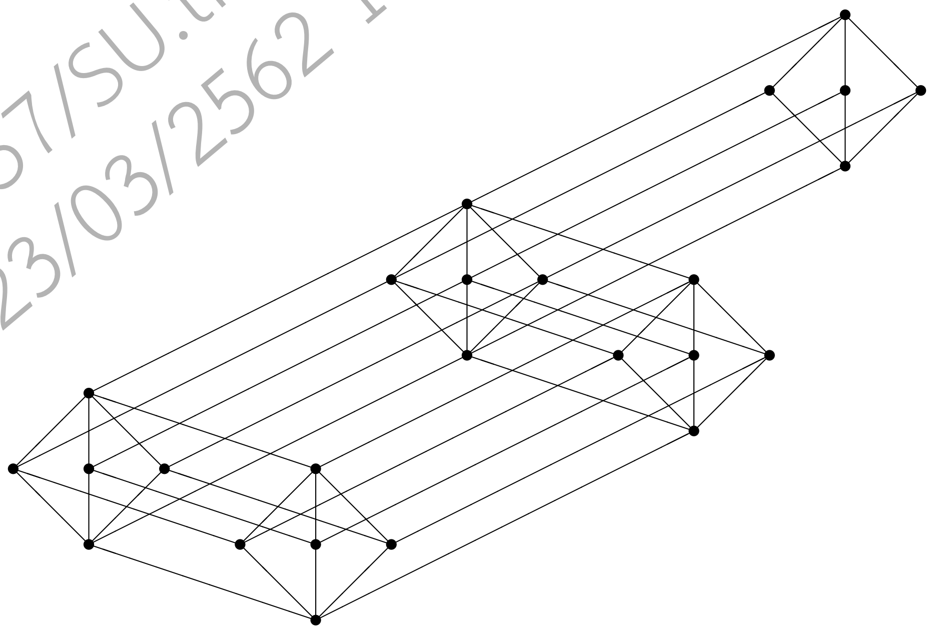


Figure 12. The congruence lattices of some congruence-modular near-symmetric algebras.

References

[1] J.Berman, On the congruence lattices of unary algebras, Proceedings of the American Mathematical Society, vol.36, 34-38, November, 2007.

[2] B.A.Davey and H.A.Priestley, Introduction to Lattices and Order, Cambridge Mathematical Textbooks, New York, 1990.

[3] K.Denecke and S.L.Wismath, Universal Algebra and Applications in Theoretical Computer Science, Chapman & Hall, CRC Press, Boca Raton, London, New York, Washington DC, 2002.

[4] W.Edwin Clark, Elementary Number Theory, Department of Mathematics University of South Florida, 2002.

[5] G.Gratzer, Universal Algebra, D.Van Nostrand Company, INC, 1968.

[6] D.Jakubikova and Kosice, On congruence relations of monounary algebras I, Czechoslovak Mathematical Journal, 32(107), 437-459, 1982.

[7] D.Jakubikova and Kosice, On congruence relations of monounary algebras II, Czechoslovak Mathematical Journal, 33(108), 448-466, 1983.

[8] R.McKenzie and D.Hobby, The structure of finite algebras, Contemporary Mathematics, vol.76, Providence, Rhode Island, 1988.

[9] C.Ratanaprasert, K.Denecke, Unary operations with long pre-periods, Discrete Mathematics, 308, 4998-5005, 2008.

APPENDIX

List of Symbols

$Con(A;f)$	set of all congruence relations on an algebra $(A;f)$
$P \oplus \underline{1}$	a linear sum of a product of chains with one-element chain $\underline{1}$
$\lambda(f)$	pre-period of a unary operation f
$\downarrow n$	a lattice of a non-negative integer n

Biography

NAME	Miss Supharat Thiranantanakorn
ADDRESS	15/25 Moo 3 Tambol Srisatong, Amphur Nakhon Chaisri, Nakhon Pathom, 73120
INSTITUTION ATTENDED	
2005	Bachelor of Science (Mathematics), Silpakorn University
2009	Master of Science (Mathematics), Silpakorn University