

The algebraic-function congruences on distributive lattices

Wei Ji*

College of Science, Guilin University of Technology, Guilin 541004, Guangxi, China

Original research papers

Received: XX December 20XX

Accepted: XX December 20XX

Online Ready: XX December 20XX

Abstract

We propose the Chinese Remainder Theorem in distributive lattices and apply the results to investigate the congruences induced by algebraic functions on distributive lattices. It is shown that the congruence induced by an algebraic function preserves abutment relationships in distributive lattices.

Keywords: distributive lattice; algebraic function; congruence; Chinese remainder theorem; lattice polynomial function

2010 Mathematics Subject Classification: 03G10;06B05

1 Introduction

In lattice theory, lattice polynomials have been defined as well-formed expressions involving variables linked by the lattice operation \wedge and \vee in an arbitrary combination of parentheses; see for instance in [2, 8]. Lattice polynomials has been widely used in the fuzzy set theory, such as aggregation functions [4, 11, 12], Sugeno integral [5, 7, 9, 10], etc.

The concept of lattice polynomial function can be straightforwardly generalized by fixing some variables as parameters. Such parameterized polynomial functions are called algebraic functions. The algebraic functions on a lattice have been extensively studied in many books and papers, such as [6, 13, 14, 15]. Unary algebraic functions play the most important role in lattice theory.

Let L be a lattice. The meet or join of two unary algebraic functions on L is a unary algebraic function. It follows that all unary algebraic functions on L form a lattice. We call this lattice the unary algebraic-function lattice of L and denote it by $A_1(L)$. The meet and join in $A_1(L)$ are denoted by \wedge_1 and \vee_1 respectively. The order relation in $A_1(L)$ is denoted by \leq_1 . It is clear that if $f(x), g(x) \in A_1(L)$, then $f(x) \leq_1 g(x)$ if and only if $f(x) \leq g(x)$ for any $x \in L$.

Let $\text{Con}(L)$ denote the set of all congruence relations on L ordered by set inclusion. It is known that $\text{Con}(L)$ is a boolean lattice if L is a finite distributive lattice. The top element and the bottom element of $\text{Con}(L)$ are denoted by ι and ω respectively. If $f(x)$ is a homomorphism on L then the kernel of $f(x)$ is the congruence relation $\ker f$ defined by $(a, b) \in \ker f(x) \iff f(a) = f(b)$ on L .

*Corresponding author: E-mail: javeey@163.com

In distributive lattices, if $f(x)$ is a unary algebraic function then $\ker f$ is a congruence relation, called an algebraic-function congruence.

Let L be a distributive lattice and $a, b \in L$. The smallest congruence that identifies a and b , is called a principal congruence and denoted by $\vartheta(a, b)$. The intersection of two principal congruences is a principal congruence. If $b \leq a$ and $d \leq c$ then $\vartheta(a, b) \wedge \vartheta(c, d) = \vartheta(a \wedge c, a \wedge c \wedge (b \vee d))$ [3, Theorem 8.11].

In the remainder of this paper, unless otherwise specified, L denotes a distributive lattice. We denote f, g the unary functions with a variable x . Other lowercase letters a, b, \dots denote the elements in L . The covering relations in L and $A_1(L)$ are denoted by \prec and \prec_1 respectively.

2 The congruences induced by $x \wedge a$ and $x \vee a$

Every unary algebraic function on a distributive lattice L can be represented by one of the following forms: $x, x \wedge a, x \vee a$ and $(x \wedge a) \vee b$ with $b \leq a$. In this section, we discuss the congruences induced by $x \wedge a$ and $x \vee a$, which are denoted by $\Gamma(a)$ and $\Psi(a)$ respectively. It is known that $\vartheta(a, b) = \Gamma(a \wedge b) \wedge \Psi(a \vee b)$ [3, Theorem 8.10].

Proposition 2.1. *The following statements are equivalent:*

1. $a \leq b$.
2. $\Gamma(b) \leq \Gamma(a)$.
3. $\Psi(a) \leq \Psi(b)$.

Proof. $1 \Rightarrow 2$: Let $a, b \in L$ with $a \leq b$. If $(y, z) \in \Gamma(b)$, then $y \wedge b = z \wedge b$. It follows that $y \wedge a = z \wedge a$ and hence $(y, z) \in \Gamma(a)$.

$2 \Rightarrow 1$: Suppose $\Gamma(b) \leq \Gamma(a)$ holds. Since $(a \wedge b, a) \in \Gamma(b)$, we have $(a \wedge b, a) \in \Gamma(a)$ and thus $a \wedge b = a$.

$1 \Leftrightarrow 3$: This is established similarly. □

To compute the $\Gamma(a) \wedge \Gamma(b)$, we need the following Chinese Remainder theorem. A Chinese Remainder Theorem in distributive lattices was proposed by Balachandran in [1]. Now we give a different version which is more similar to the Chinese Remainder Theorem in elementary number theory. The innovative point of our theorem is that it gives the solutions of a system as well as the condition under which it has a solution.

Lemma 2.1. *In a lattice, if $a \wedge x \leq y$ and $a \wedge y \leq x$, then $a \wedge x = a \wedge y$.*

Proof. It is clear that $(a \wedge x) \wedge (a \wedge y) \leq y \wedge (a \wedge y) = a \wedge y$, and therefore, $a \wedge y \leq a \wedge x$. Similarly, we have $a \wedge x \leq a \wedge y$ and thus $a \wedge x = a \wedge y$. □

Theorem 2.2 (Chinese Remainder Theorem). *Let L be a distributive lattice and $a, b, c, d \in L$.*

1. *The system of equations*

$$\begin{cases} x \equiv c \ (\Gamma(a)), \\ x \equiv d \ (\Gamma(b)) \end{cases} \quad (2.1)$$

has a solution if and only if $c \equiv d \ (\Gamma(a \wedge b))$.

2. *If System 2.1 has a solution, then y is a solution if and only if*

$$y \equiv (c \wedge a) \vee (d \wedge b) \ (\Gamma(a \vee b)).$$

Proof. Let y be a solution of System 2.1. It follows that $y \wedge a = c \wedge a$ and $y \wedge b = d \wedge b$. Therefore,

$$\begin{aligned} y \wedge (a \vee b) &= (y \wedge a) \vee (y \wedge b) \\ &= (c \wedge a) \vee (d \wedge b) \\ &= ((c \wedge a) \vee (d \wedge b)) \wedge (a \vee b). \end{aligned}$$

Hence $y \equiv (c \wedge a) \vee (d \wedge b) \ (\Gamma(a \vee b))$. Moreover,

$$\begin{aligned} y \wedge a &= y \wedge (a \vee b) \wedge a \\ &= ((c \wedge a) \vee (d \wedge b)) \wedge a \\ &= (c \wedge a) \vee (d \wedge b \wedge a). \end{aligned}$$

From $y \wedge a = c \wedge a$ we obtain $c \wedge a = (c \wedge a) \vee (d \wedge b \wedge a)$ and hence that $(a \wedge b) \wedge d \leq c \wedge a \leq c$. Similarly, we have $(a \wedge b) \wedge c \leq d$. It follows from Lemma 2.1 that $(a \wedge b) \wedge c = (a \wedge b) \wedge d$. Hence $c \equiv d \ (\Gamma(a \wedge b))$.

Conversely, suppose $c \equiv d \ (\Gamma(a \wedge b))$. It follows that $c \wedge (a \wedge b) = d \wedge (a \wedge b)$. Let $y \in L$ such that $y \equiv (c \wedge a) \vee (d \wedge b) \ (\Gamma(a \vee b))$. Then we have

$$\begin{aligned} y \wedge a &= y \wedge (a \vee b) \wedge a \\ &= ((c \wedge a) \vee (d \wedge b)) \wedge (a \vee b) \wedge a \\ &= ((c \wedge a) \vee (d \wedge b)) \wedge a \\ &= ((c \wedge a) \vee (d \wedge b \wedge a)) \\ &= (c \wedge a) \vee (c \wedge b \wedge a) \\ &= c \wedge a. \end{aligned}$$

Hence $y \equiv c \ (\Gamma(a))$. Similarly, we have $y \equiv d \ (\Gamma(b))$. So y is a solution of System 2.1. \square

Proposition 2.2. $\Gamma(a) \wedge \Gamma(b) = \Gamma(a \vee b)$, $\Psi(a) \wedge \Psi(b) = \Psi(a \wedge b)$

Proof. From Proposition 2.1, we have $\Gamma(a \vee b) \leq \Gamma(a) \wedge \Gamma(b)$. Conversely, let $(y, z) \in \Gamma(a) \wedge \Gamma(b)$. Since $y \equiv y \ (\Gamma(a \vee b))$, the system

$$\begin{cases} x \equiv y \ (\Gamma(a)), \\ x \equiv y \ (\Gamma(b)) \end{cases}$$

has a solution. In fact, it follows from Theorem 2.2 that c is a solution if and only if $c \equiv y \wedge (a \vee b) \ (\Gamma(a \vee b))$. Since $y \equiv z \ (\Gamma(a))$ and $y \equiv z \ (\Gamma(b))$, c is also a solution of the system

$$\begin{cases} x \equiv z \ (\Gamma(a)), \\ x \equiv z \ (\Gamma(b)). \end{cases}$$

Hence $c \equiv z \wedge (a \vee b) \ (\Gamma(a \vee b))$. It follows that $y \wedge (a \vee b) \equiv z \wedge (a \vee b) \ (\Gamma(a \vee b))$. So we have $y \wedge (a \vee b) = z \wedge (a \vee b)$ and hence $(y, z) \in \Gamma(a \vee b)$. It follows that $\Gamma(a) \wedge \Gamma(b) \leq \Gamma(a \vee b)$. Therefore, $\Gamma(a) \wedge \Gamma(b) = \Gamma(a \vee b)$. Similarly, we have $\Psi(a) \wedge \Psi(b) = \Psi(a \wedge b)$. \square

To compute $\Gamma(a) \vee \Gamma(b)$, we need the following generalized Chinese Remainder Theorem.

Theorem 2.3 (Generalized Chinese Remainder Theorem). *Let Θ, Φ be congruences on a lattice L . The system of equations*

$$\begin{cases} x \equiv a \ (\Theta), \\ x \equiv b \ (\Phi) \end{cases} \quad (2.2)$$

has a solution if and only if $(a, b) \in \Theta \circ \Phi$. In fact, y is a solution if and only if $y \equiv c \ (\Theta \wedge \Phi)$, where c is an element such that $(a, c) \in \Theta$ and $(c, b) \in \Phi$.

Proof. Suppose System 2.2 has a solution and let y be a solution. It follows that $(a, y) \in \Theta$ and $(y, b) \in \Phi$. Hence $(a, b) \in \Theta \circ \Phi$. Let c be an element such that $(a, c) \in \Theta$ and $(c, b) \in \Phi$. It is clear that $y \equiv c \ (\Theta \wedge \Phi)$. Conversely, if $(a, b) \in \Theta \circ \Phi$, then there exists $c \in L$, such that $(a, c) \in \Theta$ and $(c, b) \in \Phi$. If $y \equiv c \ (\Theta \wedge \Phi)$, then $y \equiv c \ (\Theta)$ and $y \equiv c \ (\Phi)$. It follows that $y \equiv a \ (\Theta)$ and $y \equiv b \ (\Phi)$. Hence y is a solution of System 2.2. \square

Proposition 2.3. $\Gamma(a) \vee \Gamma(b) = \Gamma(a \wedge b)$, $\Psi(a) \vee \Psi(b) = \Psi(a \vee b)$.

Proof. From Proposition 2.1, we have $\Gamma(a) \leq \Gamma(a \wedge b)$ and $\Gamma(b) \leq \Gamma(a \wedge b)$ and hence $\Gamma(a) \vee \Gamma(b) \leq \Gamma(a \wedge b)$. Conversely, from Theorem 2.2 and 2.3, System 2.1 has a solution if and only if $(a, b) \in \Gamma(a \wedge b)$, if and only if $(a, b) \in \Gamma(a) \circ \Gamma(b)$. Thus $\Gamma(a \wedge b) = \Gamma(a) \circ \Gamma(b)$. Since $\Gamma(a) \circ \Gamma(b) \subseteq \Gamma(a) \vee \Gamma(b)$, we have $\Gamma(a \wedge b) \subseteq \Gamma(a) \vee \Gamma(b)$. It follows that $\Gamma(a) \vee \Gamma(b) = \Gamma(a \wedge b)$. Similarly, we have $\Psi(a) \vee \Psi(b) = \Psi(a \vee b)$. \square

The sets $\{\Gamma(x) | x \in L\}$ and $\{\Psi(x) | x \in L\}$, which are denoted by $\Gamma(L)$ and $\Psi(L)$ respectively, are sublattices of $\text{Con}(L)$. Moreover, the mapping $\Gamma : L \rightarrow \Gamma(L)$ is a dual-isomorphism and the mapping $\Psi : L \rightarrow \Psi(L)$ is an isomorphism.

Theorem 2.4. The complement of $\Gamma(a)$ in $\text{Con}(L)$ is $\Psi(a)$.

Proof. In a distributive lattice, if $a \wedge x = a \wedge y$ and $a \vee x = a \vee y$, then $x = y$. It follows that $\Gamma(a) \wedge \Psi(a) = \omega$. It remains to show that $\Gamma(a) \vee \Psi(a) = \iota$. For any $x, y \in L$, since $(x \wedge y \wedge a, a) \in \Psi(a)$ and $(a, x \vee y \vee a) \in \Gamma(a)$, we have $(x \wedge y \wedge a, x \vee y \vee a) \in \Gamma(a) \vee \Psi(a)$. Since x, y are in the interval $[x \wedge y \wedge a, x \vee y \vee a]$, we have $(x, y) \in \Gamma(a) \vee \Psi(a)$ and thus $\Gamma(a) \vee \Psi(a) = \iota$. \square

3 The congruence induced by $(x \wedge a) \vee b$

If L is bounded, then for any $f(x) \in A_1(L)$, there exist $a, b \in L$ with $b \leq a$ such that $f(x) = (x \wedge a) \vee b$. Now we discuss the congruences determined by $(x \wedge a) \vee b$ and $(x \vee a) \wedge b$, which are denoted by $\Gamma(a, b)$ and $\Psi(a, b)$ respectively.

Proposition 3.1. Let L be a distributive lattice and $a, b \in L$. Then

$$\Gamma(a, b) = \Gamma(a, a \wedge b) = \Gamma(a \vee b, b) = \Psi(b, a \vee b) = \Psi(a \wedge b, a) = \Psi(b, a)$$

Proof. If $(x, y) \in \Gamma(a, b)$, then $(x \wedge a) \vee b = (y \wedge a) \vee b$. It follows that $(x \vee b) \wedge (a \vee b) = (y \vee b) \wedge (a \vee b)$ and hence $(x, y) \in \Psi(b, a \vee b)$. Since $a \leq a \vee b$, we have $(x \vee b) \wedge a = (y \vee b) \wedge a$ and thus $(x, y) \in \Psi(b, a)$. Therefore, $\Gamma(a, b) \leq \Psi(b, a \vee b) \leq \Psi(b, a)$. Similarly, we have $\Psi(b, a) \leq \Gamma(a, a \wedge b) \leq \Gamma(a, b)$ and hence $\Gamma(a, b) = \Gamma(a, a \wedge b) = \Psi(b, a \vee b) = \Psi(b, a)$. From $\Gamma(a, b) = \Psi(b, a)$ we obtain $\Gamma(a, a \wedge b) = \Psi(a \wedge b, a)$. Since $(x \wedge a) \vee b = (x \wedge (a \vee b)) \vee b$, we have $\Gamma(a \vee b, b) = \Gamma(a, b)$. \square

Theorem 3.1. $\Gamma(a, b) = \Gamma(a) \vee \Psi(b)$, $\Psi(a, b) = \Psi(a) \vee \Gamma(b)$.

Proof. Since $\Gamma(a) \leq \Gamma(a, b)$ and $\Psi(b) \leq \Gamma(a, b)$, we have $\Gamma(a) \vee \Psi(b) \leq \Gamma(a, b)$. To obtain the reverse inequality, let $(x, y) \in \Gamma(a, b) \wedge \Psi(a) \wedge \Gamma(b)$. It follows that

$$\begin{cases} (x \wedge a) \vee b = (y \wedge a) \vee b, \\ x \vee a = y \vee a, \\ x \wedge b = y \wedge b \end{cases}$$

and therefore

$$\begin{aligned}
 x \wedge a &= (x \wedge a) \wedge ((x \wedge a) \vee b) \\
 &= (x \wedge a) \wedge ((y \wedge a) \vee b) \\
 &= ((x \wedge a) \wedge (y \wedge a)) \vee ((x \wedge a) \wedge b) \\
 &= ((x \wedge a) \wedge (y \wedge a)) \vee ((y \wedge a) \wedge b) \\
 &= (y \wedge a) \wedge ((x \wedge a) \vee b) \\
 &= (y \wedge a) \wedge ((y \wedge a) \vee b) \\
 &= y \wedge a.
 \end{aligned}$$

But since $x \vee a = y \vee a$, we have $x = y$ by Theorem 2.4 and hence $\Gamma(a, b) \wedge \Psi(a) \wedge \Gamma(b) = \omega$. Since $\Gamma(a) \vee \Psi(b)$ and $\Psi(a) \wedge \Gamma(b)$ are complementary, we have

$$\begin{aligned}
 \Gamma(a, b) &= \Gamma(a, b) \wedge \iota \\
 &= \Gamma(a, b) \wedge ((\Gamma(a) \vee \Psi(b)) \vee (\Psi(a) \wedge \Gamma(b))) \\
 &= (\Gamma(a, b) \wedge (\Gamma(a) \vee \Psi(b))) \vee (\Gamma(a, b) \wedge (\Psi(a) \wedge \Gamma(b))) \\
 &= \Gamma(a, b) \wedge (\Gamma(a) \vee \Psi(b)).
 \end{aligned}$$

Therefore $\Gamma(a, b) \leq \Gamma(a) \vee \Psi(b)$ and hence $\Gamma(a, b) = \Gamma(a) \vee \Psi(b)$. It follows from Proposition 3.1 that $\Psi(a, b) = \Gamma(b, a) = \Psi(a) \vee \Gamma(b)$. \square

Let $f(x)$ and $g(x)$ be lattice endomorphisms on L . Then $\ker f \circ g$ and $\ker g \circ f$ are congruence relations on L . In general $\ker f \circ g$ is not equal to $\ker g \circ f$. But when $f(x) = x \wedge a$ and $g(x) = x \vee b$, we have $\ker f \circ g = \ker g \circ f = \ker f \vee \ker g$ from Theorem 3.1.

Let $a, b \in L$ with $b \leq a$. Then $\vartheta(a, b) = \Gamma(b) \wedge \Psi(a)$. It follows that the complement of $\vartheta(a, b)$ is $\Psi(b) \vee \Gamma(a)$, which is equal to $\Gamma(a, b)$.

Theorem 3.2. *The join of two algebraic-function congruences is an algebraic-function congruence. More precisely, if $b \leq a$ and $d \leq c$ then $\Gamma(a, b) \vee \Gamma(c, d) = \Gamma(a \wedge c, a \wedge c \wedge (b \vee d))$.*

Proof. If $b \leq a$ and $d \leq c$, then complement of $\Gamma(a, b) \vee \Gamma(c, d)$ is $\vartheta(a, b) \wedge \vartheta(c, d)$, which is equal to the complement of $\Gamma(a \wedge c, a \wedge c \wedge (b \vee d))$. Since every element has at most one complement in distributive lattices, it follows that $\Gamma(a, b) \vee \Gamma(c, d) = \Gamma(a \wedge c, a \wedge c \wedge (b \vee d))$. \square

Theorem 3.3. *The mapping $\ker : A_1(L) \rightarrow \text{Con}(L)$ preserves abutment relationships, in the sense that, if $f(x) \prec_1 g(x)$ in $A_1(L)$, then $\ker f \prec \ker g$ or $\ker g \prec \ker f$ in $\text{Con}(L)$.*

Proof. Suppose $f(x) = (x \wedge a) \vee b$ and $g(x) = (x \wedge c) \vee d$ with $b \leq a$ and $d \leq c$. If $f(x) \prec_1 g(x)$, then $a \prec c$ and $b = d$, or $a = c$ and $b \prec d$. Indeed, if $a \neq c$, then $a \prec c$ and $b = d$. To see this, suppose there exists $p \in L$ such that $a < p < c$. It follows that $(x \wedge a) \vee b <_1 (x \wedge p) \vee b <_1 (x \wedge c) \vee b \leq_1 (x \wedge c) \vee d$, a contradiction to $f(x) \prec_1 g(x)$. Thus we have $a \prec c$ and therefore $b = d$. Similarly, if $b \neq d$, then $a = c$ and $b \prec d$.

If $a \prec c$ and $b = d$, then $\Gamma(c) \prec \Gamma(a)$ and $\Psi(b) = \Psi(d)$. It follows from Theorem 3.1 that $\Gamma(c) \vee \Psi(d) = \Gamma(c, d)$ and $\Gamma(a) \vee \Psi(d) = \Gamma(a) \vee \Psi(b) = \Gamma(a, b)$. Thus the intervals $[\Gamma(c), \Gamma(a)]$ and $[\Gamma(c, d), \Gamma(a, b)]$ are isomorphic and hence $\Gamma(c, d) \prec \Gamma(a, b)$. If $a = c$ and $b \prec d$, we have $\Gamma(a, b) \prec \Gamma(c, d)$ in a similar way. Thus the mapping $\ker : A_1(L) \rightarrow \text{Con}(L)$ preserves abutment relationships. \square

Example 3.4. *Figure 1 shows an example of how the mapping $\ker : A_1(L) \rightarrow \text{Con}(L)$ acts. The second diagram in Figure 1 is the diagram of $A_1(L)$ in which $P_{u,v}$ represents the algebraic function $(x \wedge u) \vee v$, while the third one is the diagram of $\text{Con}(L)$ in which $P_{u,v}$ represents $\ker((x \wedge u) \vee v)$. Fold the diagram of $A_1(L)$ and turn it over, we obtain $\text{Con}(L)$.*

In general, the map $\ker : A_1(L) \rightarrow \text{Con}(L)$ is not surjective. Thus we can not always get a whole diagram of $\text{Con}(L)$ by folding $A_1(L)$.

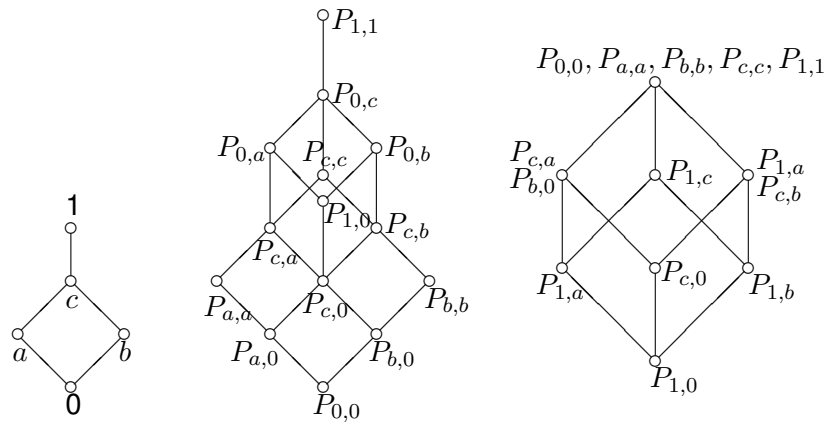


Figure 1: Diagrams of L , $A_1(L)$ and $\text{Con}(L)$

4 Conclusion

The Chinese remainder theorem in number theory is a useful tool to solve problems in computing, coding and cryptography. In this paper, we studied the Chinese remainder theorem in distributive lattices. Subsequently, the congruences induced by algebraic functions on distributive lattices are discussed. It is shown that the congruence induced by an algebraic function preserves abutment relationships.

Competing Interests

Author has declared that no competing interests exist.

References

- [1] Balachandran VK. The Chinese remainder theorem for the distributive lattice. J. Indian Math. Soc. 1949;13:76-80.
- [2] Birkhoff G. Lattice Theory, American Mathematical Society Colloquium Publications, Rhode Island; 1967.
- [3] Blyth TS. Lattices and Ordered Algebraic Structures, Springer Verlag, London; 2005.
- [4] Çaylı GD. On a new class of t-norms and t-conorms on bounded lattices. Fuzzy Sets Syst. 2018;332:129-143.
- [5] Couceiro M, J. Marichal. Characterizations of discrete Sugeno integrals as polynomial functions over distributive lattices. Fuzzy Sets Syst. 2010;161:694-707.
- [6] Couceiro M, Marichal JL. Representations and characterizations of polynomial functions on chains. J. Mult.-Valued Log. S. 2010;16:65-86.

- [7] Couceiro M, Marichal JL. Associative polynomial functions over bounded distributive lattices. *Order*. 2011;28:1-8.
- [8] Grätzer G. *General Lattice Theory*, second ed, Birkhäuser Verlag, Basel; 1998.
- [9] Halaš R, Pócs J. On lattices with a smallest set of aggregation functions. *Inform. Sci.* 2015;325:316-323.
- [10] Halaš R, Mesiar R, Pócs J. Congruences and the discrete Sugeno integrals on bounded distributive lattices. 2016; 367-368:443-448.
- [11] Halaš R, Pócs J. On the clone of aggregation functions on bounded lattices. *Inform. Sci.* 2016;329:381-389.
- [12] Karaçal F, Mesiar R. Aggregation functions on bounded lattices. *Int. J. Gen. Syst.* 2017;46:37-51.
- [13] Marichal JL. Weighted lattice polynomials of independent random variables. *Discrete Appl. Math.* 2008;156:685-694.
- [14] Marichal JL. Weighted lattice polynomials. *Discrete Mathe.* 2009;309:814-820.
- [15] Rudeanu S. *Lattice Functions and Equations*, Springer Verlag, London; 2001.