ISSN 2234-4438
융합정보논문지 제7권 제3호 pp. 65-71, 2017 DOI : https://doi.org/10.22156/CS4SMB.2017.7.3.065

A Homomorphism on Orthoimplication Algebras for Quantum Logic

Yong-Ho Yon*
Division of Information and Communication Convergence Engineering, Mokwon University

양자논리를 위한 직교함의 대수에서의 준동형사상

연용호*
목원대학교 정보통신융합공학부

Abstract The quantum logic was introduced by G. Birkhoff and J. von Neumann in order to study projections of a Hilbert space for a formulation of quantum mechanics, and Husimi proposed orthomodular law and orthomodular lattices to complement the quantum logic. Abott introduced orthoimplication algebras and its properties to investigate an implication of orthomodular lattice. The commuting relation is an important property on orthomodular lattice which is related with the distributive law and the modular law, etc. In this paper, we define a binary operation on orthoimplication algebra and the greatest lower bound by using this operation and research some properties of this operation. Also we define a homomorphism and characterize the commuting relation of orthoimplication algebra by the homomorphism.

Key Words : Logical Implication, Quantum Logic, Ortholattices, Orthomodular Lattices, Orthoimplication Algebras, Commuting Relation

요 약 양자논리는 양자역학을 위한 수학적 구조인 힐버트 공간에서의 사영을 다루기 위해 Birkhoff와 von Neumann에 의해 소개되었고. Husimi는 이 양자논리를 보완하기 위해 직교모듈라의 성질과 직교모듈라 격자를 제안하였다. Abbott은 직교모듈라 격자에서의 함의를 연구하기 위해 직교함의 대수와 그 성질을 소개하였다. 직교모듈라 격자에서 가환관계는 분배법칙과 모듈라 성질 등과 관련된 중요한 성질이다. 본 논문에서는 직교함의 대수에서의 한 이항연산과 이를 이용한 최대하계를 정의하고 그 이항연산의 성질을 밝힌다. 또한 준동형사상을 정의하고 이를 이용하여 직교함의 대수에서의 가환관계를 특성화한다.

키워드 : 논리적 함의, 양자논리, 직교격자, 직교모듈로 격자, 직교함의 대수, 가환관계

1. Introduction

The quantum logic was introduced by G. Birkhoff and J. von Neumann in order to study projections of a Hilbert space for a formulation of quantum mechanics, and Husimi proposed orthomodular law and orthomodular lattices to complement the quantum logic[1,2].

An *ortholattice* is a bounded lattice L with an orthocomplement $'$ which satisfies the following[3] : for every $a, b \in L$,

(1) $a \le b$ implies $b' \le a'$,

(2) $a'' = a$,

(3) $a \vee a' = 1$ and $a \wedge a' = 0$.

An *orthomodular lattice* is an ortholattice L satisfying the *orthomodular law*:[3]

Received 2017-05-11 Revised 2017-05-15 Accepted 2017-06-20 Published 2017-06-30
*Corresponding author : Yong-Ho Yon (yhyon@mokwon.ac.kr)

$$a \le b \text{ implies } a \vee (a' \wedge b) = b$$

Finch introduced logical conjunctions and implications that are defined on an orthomodular lattice[4,5]. Abbott and Chajda et al. proposed orthoimplication algebras and orthomodular implication algebras, respectively, as another types of quantum logic[6-8], and some operations and logical structures were considered to describe the quantum logic[3,9-13].

Lattice theory is a mathematical basis for role-based security[14]. Quantum computing technology is used in many fields such as cryptography, security and algorithm, etc.. and the need for quantum logic is increasing due to the development of quantum computers[15-17].

The commuting relation is an important property on orthomodular lattice which is related with the distributive law and the modular law, etc. In this paper, we define a binary operation on orthoimplication algebra and research some properties of this operation. Then we define an anti $\wedge$-homomorphism by the binary operation and characterize the commuting relation by this homomorphism.

2. A Binary Operation on Orthoimplication Algebras

An *orthoimplication algebra* is an algebraic system $(A, \cdot)$ of type 2 satisfying the following axioms[6]: for every $a, b, c \in A$,

(IA1) $(ab)a = a$,

(IA2) $(ab)b = (ba)a$,

(IA3) $a((ba)c) = ac$.

Lemma 2.1. ([6]) Let $(A, \cdot)$ be an orthoimplication algebra. Then A contains an element 1 and satisfies the following properties:

(1) $aa = 1$,

(2) $1a = a$,

(3) $a1 = 1$,

(4) $ab = ba \Rightarrow a = b$,

(5) $a(ba) = 1$,

(6) $a(ab) = ab$,

(7) $ab = 1 \Rightarrow a(bc) = ac$,

(8) $ab = 1 \Rightarrow (bc)(ac) = 1$.

An orthoimplication algebra A is a poset with a partial order $\le$ defined by

$$a \le b \Leftrightarrow ab = 1$$

for any $a, b \in A$, and A is a $\vee$-semilattice with

$$a \vee b = (ab)b$$

for every $a, b \in A$[6].

Lemma 2.2. Let $(A, \cdot)$ be an orthoimplication algebra. Then A satisfies the following properties:

(1) $a \le ba$,

(2) $a \le b \Rightarrow a(bc) = ac$,

(3) $a \le b \Rightarrow bc \le ac$.

Proof. It is clear from Lemma 2.1. □

Lemma 2.3. ([6]) Let $(A, \cdot)$ be an orthoimplication algebra. If $u \le a \le b$ for any $u, a, b \in A$, then $b = (bu)a$.

Every principal order filter $[a, 1] = \{x \in A \mid a \le x\}$ in orthoimplication algebra A is an orthomodular lattice with an orthocomplimentation $\perp_a$ defined by $x^{\perp_a} = xa$ for every $x \in [a, 1]$, and conversely every semi-orthomodular lattice A, i.e., a join semilattice with greatest element in which every principal filter is an orthomodular lattice and satisfies the compatibility condition: $u \le a \le b \Rightarrow b^{\perp_a} = b^{\perp_u} \vee a$, is an orthoimplication algebra with a binary operation $\cdot$ defined by $ab = (a \vee b)^{\perp_b}$ for every $a, b \in A$[6].

Theorem 2.4. If A is an orthomodular lattice, then $(A, \cdot)$ is an orthoimplication algebra with

$$ab = (a' \wedge b') \vee b$$

for every $a, b \in A$.

Proof. Let $a, b \in A$. Then we have

$$\begin{aligned}(ab)a &= (((a' \wedge b') \vee b)' \wedge a') \vee a \\ &= (((a' \wedge b')' \wedge b') \wedge a') \vee a \\ &= ((a' \wedge b')' \wedge (b' \wedge a')) \vee a \\ &= 0 \vee a \\ &= a.\end{aligned}$$

Hence $(A, \cdot)$ satisfies the axiom (IA1). Also,

$$\begin{aligned}(ab)b &= (((a' \wedge b') \vee b)' \wedge b') \vee b \\ &= (((a' \wedge b')' \wedge b') \wedge b') \vee b \\ &= ((a \vee b) \wedge (b' \wedge b')) \vee b \\ &= ((a \vee b) \wedge b') \vee b \\ &= a \vee b\end{aligned}$$

by the orthomodular law since $b \leq a \vee b$. Similarly, we can show $(ba)a = b \vee a$. Hence

$$(ab)b = a \vee b = b \vee a = (ba)a.$$

To show that $(A, \cdot)$ satisfies the axiom (OIA3), let $a, b, c \in A$ and $x = (ba)' \wedge c'$. Then

$$(ba)c = ((ba)' \wedge c') \vee c = x \vee c.$$

Since $a \leq (b' \wedge a') \vee a = ba$, $(ba)' \leq a'$,

$$x = (ba)' \wedge c' \leq a' \wedge c'.$$

This follows that

$$\begin{aligned}a((ba)c) &= a(x \vee c) \\ &= (a' \wedge (x \vee c)') \vee (x \vee c) \\ &= (a' \wedge (x' \wedge c')) \vee (x \vee c) \\ &= (((a' \wedge c') \wedge x') \vee x) \vee c \\ &= (a' \wedge c') \vee c \quad \text{(by orthomodular law)} \\ &= ac.\end{aligned}$$

Hence $(A, \cdot)$ is an orthoimplication algebra. □

Theorem 2.5. A is an orthomodular lattice if and only if A is an orthoimplication algebra with the smallest element 0.

Proof. $(\Rightarrow)$ It is clear from Lemma 2.4.
$(\Leftarrow)$ Let A be an orthoimplication algebra with the smallest element 0. Then by Theorem 4 of [6], the principal filter $A = [0,1]$ is an orthomodular lattice with an orthocomplementation $'$ given by $a' = a0$ for every $a \in A$. □

Let $(A, \cdot)$ be an orthoimplication algera with the smallest element 0. Then we can define a binary operation $*$ on A by

$$a^*b = (b'a')'$$

for every $a, b \in A$, where $x' = x0$ for every $x \in A$.

From now on, we will consider all orthoimplication algebras have the smallest element 0.

Lemma 2.6. Let A be an orthoimplication algebra. Then the binary operation $*$ satisfies the following:

(1) $a \leq b \Leftrightarrow a^*b = 0$,
(2) $a^*0 = a$ and $0^*a = 0$,
(3) $1^*a = a'$,
(4) $a^*b \leq a$, i.e., $(a^*b)^*a = 0$,
(5) $a \leq b \Rightarrow c^*b \leq c^*a$,

Proof. It is clear from the definition of the binary operation $*$ on A. □

Theorem 2.7. Let A be an orthoimplication algebra. Then A is a $\wedge$-semilattice with

$$a \wedge b = a^*(a^*b) = b^*(b^*a)$$

for every $a, b \in A$.

Proof. Let $a, b \in A$. Then

$$\begin{aligned}a^*(a^*b) &= ((a^*b)'a')' = ((b'a')a')' \\ &= ((a'b')b')' = ((b^*a)'b')' = b^*(b^*a)\end{aligned}$$

by (IA2). Also $a^*(a^*b) \leq a$ and

$$a^*(a^*b) = b^*(b^*a) \leq b$$

by Lemma 2.6(4). That is, $a^*(a^*b)$ is a lower bound of a and b. Suppose that $c \leq a$ and $c \leq b$. Then $a' \leq c'$ and $b' \leq c'$. Since A is a $\vee$-semilattice with $a' \vee b' = (b'a')a'$, $(b'a')a' \leq c'$. This implies

$$c \leq ((b'a')a')' = a^*(a^*b).$$

Hence $a^*(a^*b)$ is the greatest lower bound of a and b, and $a \wedge b = a^*(a^*b)$. □

Lemma 2.8. Let A be an orthoimplication algebra. Then A satisfies the following:

(1) $a^*b \leq c \Leftrightarrow a^*c \leq b$,
(2) $b \leq c \Rightarrow (a^*b)^*c = a^*c$,
(3) $a \leq b \Rightarrow a'^*b = b'$,

(4) $a \wedge a' = 0$

Proof. (1) Let $a * b \leq c$. Then

$$a * c \leq a * (a * b) = a \wedge b \leq b$$

by Lemma 2.6(5) and Theorem 2.7.

(2) Let $b \leq c$. Then $c' \leq b'$, and

$$(a * b) * c = (c'(b'a'))' = (c'a')' = a * c$$

by Lemma 2.2(2).

(3) Let $a \leq b$. Then

$$a' * b = (1 * a) * b = 1 * b = b'.$$

by Lemma 2.6(3) and (2) of this lemma,

(4) Let $a \in A$. Then

$$a \wedge a' = a' * (a' * a) = a' * a' = 0$$

by Theorem 2.7 and (3) of this lemma. □

3. A Homomorphism of Orthoimplication Algebras

Let A be an orthoimplication algebra. Then for each $u \in A$, we define a map $\varphi_u : A \to A$ by

$$\varphi_u(a) = u * a$$

for every $a \in A$

Lemma 3.1. Let A be an orthoimplication algebra and $u, a, b \in A$. Then the map φ_u satisfies the following:

(1) $a \leq b \Rightarrow \varphi_u(b) \leq \varphi_u(a)$,

(2) φ_1 is a bijective map and $\varphi_1(a) = a'$

(3) $u \leq a \Leftrightarrow \varphi_u(a) = 0$,

(4) $\varphi_u(a) \leq b \Rightarrow \varphi_u(b) \leq a$

Proof. (1) Let $a \leq b$. Then by Lemma 2.6(5),

$$\varphi_u(b) = u * b \leq u * a = \varphi_u(a).$$

(2) For every $a \in A$, $\varphi_1(a) = 1 * a = a'$ by Lemma 2.6(3) and definition of the map φ_u.

Let $\varphi_1(a) = \varphi_1(b)$. Then $a' = b'$ implies

$$a = a'' = b'' = b.$$

Hence φ_1 is injective. Let $a \in A$. Then there is an element $a' \in A$ such that $\varphi_1(a') = a'' = a$. This implies φ_1 is surjective. Hence φ_1 is bijective.

(3) It is clear from Lemma 2.6(1).

(4) Let $\varphi_u(a) \leq b$. Then $u * a \leq b$ implies $u * b \leq a$ by Lemma 2.8(1). Hence $\varphi_u(b) \leq a$. □

Theorem 3.2. Let A be an orthoimplication algebra and $u \in A$. Then the map $\varphi_u : A \to A$ is an anti $\wedge$-homomorphism of A. That is,

$$\varphi_u(a \wedge b) = \varphi_u(a) \vee \varphi_u(b)$$

for every $a, b \in A$.

Proof. Let $a, b \in A$. Then $a \wedge b \leq a$ and $a \wedge b \leq b$. By Lemma 3.1(1),

$$\varphi_u(a) \leq \varphi_u(a \wedge b) \text{ and } \varphi_u(b) \leq \varphi_u(a \wedge b).$$

This implies that $\varphi_u(a \wedge b)$ is an upper bound of $\varphi_u(a)$ and $\varphi_u(b)$.

Suppose that c is an upper bound of $\varphi_u(a)$ and $\varphi_u(b)$. Then $\varphi_u(a) \leq c$ and $\varphi_u(b) \leq c$. This implies $\varphi_u(c) \leq a$ and $\varphi_u(c) \leq b$ by Lemma 3.1(4), so $\varphi_u(c) \leq a \wedge b$, and $\varphi_u(a \wedge b) \leq c$ by Lemma 3.1(4). Hence $\varphi_u(a \wedge b)$ is the least upper bound of $\varphi_u(a)$ and $\varphi_u(b)$, and $\varphi_u(a \wedge b) = \varphi_u(a) \vee \varphi_u(b)$. □

The anti $\wedge$-homomorphism φ_u is not an anti $\vee$-homomorphism in general as the following example shows.

Example 3.3. Let $A = \{0, x, y, z, w, 1\}$. If we define a binary operation · on A by the following table:

·	1	x	y	z	w	0
1	1	x	y	z	w	0
x	1	1	y	z	w	y
y	1	x	1	z	w	x
z	1	x	y	1	w	w
w	1	x	y	z	1	z
0	1	1	1	1	1	1

then $(A, \cdot)$ is an orthoimplication algebra with Hasse diagram of Fig. 1. The binary operation $*$ on A is defined by the following table:

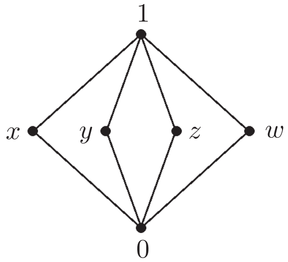

Fig. 1. Hasse diagram of $(A, \cdot)$

*	1	x	y	z	w	0
1	0	y	x	w	z	1
x	0	0	x	x	x	x
y	0	y	0	y	y	y
z	0	z	z	0	z	z
w	0	w	w	w	0	w
0	0	0	0	0	0	0

For $x, y, z \in A$, $\varphi_x(y \vee z) = \varphi_x(1) = x^*1 = 0$ and $\varphi_x(y) \wedge \varphi_x(z) = (x^*y) \wedge (x^*z) = x \wedge x = x$. That is, $\varphi_x(y \vee z) \neq \varphi_x(y) \wedge \varphi_x(z)$, and φ_x is not anti $\vee$-homomorphism of A.

For each element u in an orthoimplication algebra A, the map $\varphi_u : A \to A$ is antitone and

$$\varphi_u(a) \in [0, u] := \{x \in A \mid 0 \le x \le u\}$$

since $\varphi_u(a) = u^*a \le u$. Also, for every $a \in [0, u]$, there is an element $\varphi_u(a) \in [0, u]$ such that

$$\varphi_u(\varphi_u(a)) = u^*(u^*a) = u \wedge a = a,$$

hence the co-restriction $\varphi_u^\circ : A \to [0, u]$ of φ_u is surjective. If we define

$$Ker\varphi_u := \{x \in A \mid \varphi_u(x) = 0\},$$

then $Ker\varphi_u = [u, 1]$ by Lemma 2.6(1) and it is a principal filter of A.

Lemma 3.4. Let A be an orthoimplication algebra and $u \in A$. Then the map φ_u satisfies the following:

(1) $\varphi_u(1) = 0$ and $\varphi_u(0) = u$,

(2) $a \le b \Rightarrow \varphi_u(a)^*b = \varphi_u(b)$,

(3) $\varphi_u(a) \wedge a = 0$,

(4) $\varphi_u(a') = a$ for every $a \in [0, u]$,

(5) $\varphi_u(a) = \varphi_u(b) \Leftrightarrow a = b$ for every $a, b \in [0, u]$.

Proof. (1) $\varphi_u(1) = u^*1 = 0$ since $u \le 1$. Also, $\varphi_u(0) = u^*0 = u$ by Lemma 2.6(2).

(2) Let $a \le b$. Then by Lemma 2.8(2),

$$\varphi_u(a)^*b = (u^*a)^*b = u^*b = \varphi_u(b).$$

(3) Let $a \in A$. Then by (2) of this lemma,

$$\varphi_u(a) \wedge a = \varphi_u(a)^*(\varphi_u(a)^*a) = \varphi_u(a)^*\varphi_u(a) = 0.$$

(4) Let $a \le u$. Then $u' \le a'$, and by Lemma 2.8(3),

$$\varphi_u(a') = u^*a' = u''^*a' = a'' = a.$$

(5) Let $a, b \in [0, u]$ and $\varphi_u(a) = \varphi_u(b)$. Since $a \le u$ and $b \le u$, we have

$$a = u \wedge a = \varphi_u(\varphi_u(a)) = \varphi_u(\varphi_u(b)) = u \wedge b = b.$$

The converse direction is trivial. □

Let A be an orthoimplication algebra and $a, b \in A$. Then we say that a *commutes* with b, denoted by aCb, if $a = (a \wedge b) \vee (a \wedge b')$.

Let $\varphi_a^2 = \varphi_a \circ \varphi_a$. Then for every $b \in A$,

$$\varphi_a^2(b) = \varphi_a(\varphi_a(b)) = a^*(a^*b) = a \wedge b,$$

hence we can define the commuting relation aCb by

$$a = \varphi_a^2(b) \vee \varphi_a^2(b').$$

Theorem 3.5. Let A be an orthoimplication algebra and $a, b \in A$. Then aCb if and only if

$$\varphi_a(b) \wedge \varphi_a(b') = 0.$$

Proof. Let aCb. Then we have

$$a = \varphi_a^2(b) \vee \varphi_a^2(b') = \varphi_a(\varphi_a(b) \wedge \varphi_a(b'))$$

since φ_a is anti $\wedge$-homomorphism. Also since $\varphi_a(0) = a$, $\varphi_a(0) = \varphi_a(\varphi_a(b) \wedge \varphi_a(b'))$. Hence

$$0 = \varphi_a(b) \wedge \varphi_a(b')$$

by Lemma 3.4(5) since $0, \varphi_a(b) \wedge \varphi_a(b') \in [0, a]$.

Conversely, suppose that $0 = \varphi_a(b) \wedge \varphi_a(b')$. Then since φ_a is anti $\wedge$-homomorphism,

$$\begin{aligned}\varphi_a(0) &= \varphi_a(\varphi_a(b) \wedge \varphi_a(b')) \\ &= \varphi_a(\varphi_a(b)) \vee \varphi_a(\varphi_a(b')) \\ &= \varphi_a^2(b) \vee \varphi_a^2(b'),\end{aligned}$$

and $\varphi_a(0) = a$. This implies $a = \varphi_a^2(b) \vee \varphi_a^2(b')$.

Hence aCb. □

4. Conclusions

The orthoimplication algebra is an algebraic structure with implication defined on orthomodular lattice. Orthomodular lattices do not satisfy the distributive law in general. Because the commuting relation C is closely related with the distributive law in orthomodular lattices, the commuting relation was studied by some literature. In this paper we define a anti $\wedge$-homomorphism and the commuting relation on orthoimplication algebras and research the properties of the anti $\wedge$-homomorphism. In particular, the commuting relation is characterized by the anti $\wedge$-homomorphism of orthoimplication algebras.

REFERENCES

[1] G. Birkhoff and J. von Neumann, "The logic of quantum mechanics," *Annals of Mathematics,* Vol. 37, No. 4, pp. 822-843, Oct. 1936.
DOI : 10.2307/1968621

[2] K. Husimi, "Studies on the foundations of quantum mechanics I," *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series,* Vol. 19, pp. 766-789, 1937.
DOI : 10.11429/ppmsj1919.19.0_766

[3] G. Kalmbach, *Orthomodular lattices*, Academic Press, New York, 1983.

[4] P. D. Finch, "On the lattice structure of quantum logic," *The Journal of Symbolic Logic,* Vol. 34, No. 2, pp. 275-282, Jun. 1969.
DOI : 10.2307/2271104

[5] P. D. Finch, "Quantum logic as an implication algebra," *Bulletin of the Australian Mathematical Society,* Vol. 2, No. 1, pp. 101-106, Feb. 1970.
DOI : 10.1017/S0004972700041642

[6] J. C. Abbott, "Orthoimplication algebras," *Studia Logica,* Vol. 35, pp. 173-177, Jun. 1976.
DOI : 10.1007/BF02120879

[7] I. Chajda, R. Halaš and H. Länger, "Orthomodular implication algebras," *International Journal of Theoretical Physics,* Vol. 40, No. 11, pp. 1875-1884, Nov. 2001.
DOI : 10.1023/A:1011933018776

[8] N. D. Megill and M. Pavičić, "Quantum implication algebras," *International Journal of Theoretical Physics,* Vol. 42, No. 12, pp. 2807-2822, Oct. 2003.
DOI : 10.1023/B:IJTP.0000006007.58191.da

[9] G. M. Hardegree, "Quasi-implication algebras, Part I: Elementary theory," *Algebra Universalis,* Vol. 12, No. 1, pp. 30-47, Dec. 1981.
DOI : 10.1007/BF02483861

[10] G. M. Hardegree, "Quasi-implication algebras, Part II: Structure theory," *Algebra Universalis,* Vol. 12, No. 1, pp. 48-65, Dec. 1981.
DOI : 10.1007/BF02483862

[11] G. M. Hardegree, "Material implication in orthomodular (and Boolean) lattices," *Notre Dame J. Form. Log.,* Vol. 22, No. 2, pp. 163-182, Apr. 1981.
DOI : 10.1305/ndjfl/1093883401

[12] J. J. M. Gabiëls and M. Navara, "Associativity of operations in orthomodular lattices," *Math. Slovaca,* Vol. 62, No. 6, pp. 1069-1078, Dec. 2012.
DOI : 10.2478/s12175-012-0065-2

[13] I. Chajda and S. Radeleczki, "An approach to orthomodular lattices via lattices with an antitone involution," *Math. Slovaca,* Vol. 66, No. 4, pp. 773-780, Aug. 2016.
DOI : 10.1515/ms-2015-0179

[14] H. J. Lee, O. C. Na, S. Y. Sung and H. B. Chang, "A Design on Security Governance Framework for Industry Convergence Environment," *Journal of the Korea* Convergence Society, Vol. 6, No. 4, pp. 33-40, Aug. 2015.
DOI : 10.15207/JKCS.2015.6.4.033

[15] N. Y. Heo and Y. J. Ko, "The Status of Research of Quantum dot Using 4P Analysis-Focusing on the application and convergence field of quantum technology," *Journal of the Korea Convergence Society,* Vol. 6, No. 2, pp. 49-55, 2015.
DOI : 10.15207/ JKCS.2015.6.2.049

[16] Y. S. Park, K. R. Park and D. H. Kim, "A Study of Distribute Computing Performance Using a Convergence of Xeon-Phi Processor and Quantum ESPRESSO," *Journal of the Korea Convergence Society,* Vol. 7, No. 5, pp. 15-21, Oct. 2016.
DOI : 10.15207/JKCS.2016.7.5.015

[17] S. H. Yun, "The Biometric Authentication Scheme Capable of Multilevel Security Control," *Journal of the*

Korea Convergence Society, Vol. 8, No. 2, pp. 9-14, Feb. 2017.
DOI : 10.15207/JKCS.2017.8.2.009

저 자 소 개

연 용 호(Yong-Ho Yon) [정회원]

- 1988년 2월 : 충북대학교 수학과 학사
- 1990년 2월 : 충북대학교 수학과 석사
- 1997년 8월 : 충북대학교 수학과 박사
- 2011년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 교수

<관심분야> : 격자론, 격자암호, 양자논리