암호학 및 오류 수정 코드를 위한 부울 대수 가중치 연구

A Weight on Boolean Algebras for Cryptography and Error Correcting Codes

연용호*, 강안나*

Yong-Ho Yon*, An-Na Kang*

요 약

Sphere-packing problem은 주어진 공간에 가능한 한 많은 구(sphere)를 채울 수 있는 배열을 찾는 문제이고 covering problem은 이에 쌍대적인 최적화의 문제로 코딩이론에 적용된다. 본 논문에서는 이진 코드이론에서의 가중치(weight)와 해밍거리(Hamming distance)에 대한 개념을 부울 대수(Boolean algebra)의 개념으로 일반화한다. 부울 대수에서의 가중치와 이를 이용하여 거리함수를 정의하고, 이들의 기본적인 성질들을 밝힌다. 또한, 부울 대수에서의 sphere-packing bound와 Gilbert-Varshamov bound의 정리를 증명한다.

Abstract

A sphere-packing problem is to find an arrangement of the spheres to fill as large area of the given space as possible, and covering problems are optimization problems which are dual problems to the packing problems. We generalize the concepts of the weight and the Hamming distance for a binary code to those of Boolean algebra. In this paper, we define a weight and a distance on a Boolean algebra and research some properties of the weight and the distance. Also, we prove the notions of the sphere-packing bound and the Gilbert-Varshamov bound on Boolean algebra.

Key words : Boolean algebra, weight, distance, sphere-packing bound, Gilbert-Varshamov bound
부울 대수, 가중치, 거리

Ⅰ. INTRODUCTION

Coding theory has been studied for the effective use of the data, such as data compression, error correction, cryptography and network transmission, in computer science.

A typical sphere-packing problem is to find an arrangement of the spheres to fill as large area of the given space as possible, and covering problems are optimization problems which are dual problems to the packing problems. Sphere-packing bounds are closely related to error-correcting code.

In coding theory, packing problems have investigated in order to find maximal codes with given minimum distance [1]-[3], and covering problems were examined in order to find codes with given covering radius. It is the aim to determine the minimal cardinality of such a covering code

* 목원대학교 공학교육혁신센터(Innovation Center for Engineering Education, Mokwon University)
· 제1저자 (First Author) : 연용호 (Yong-Ho Yon) · 교신저자 (Corresponding Author) : 강안나 (An-Na Kang)
· 투고일자 : 2011년 10월 5일
· 심사(수정)일자 : 2011년 10월 5일 (수정일자 : 2011년 10월 25일)
· 게재일자 : 2011년 10월 30일

[4]-[7]. Improved sphere-packing bounds for binary code were introduced in [8],[9], and a improving Gilbert-Varshamov bound for q-ary codes was studied in [10]. The general theory of code can be found in [11]-[13].

In section 2, we define a weight function on Boolean algebras and research basic properties of it, and in section3, we define a distance on Boolean algebras using the weight function and research basic properties of the distance, and prove the similar notions with the sphere-packing bound and the Gilbert-Varshamov bound in coding theory.

Ⅱ. A WEIGHT FUNCTION ON BOOLEAN ALGEBRAS

Let $(P; \leq)$ be a poset and let $x, y \in P$. We say y *covers* x, written by $x \prec y$ or $y \succ x$, if $x < y$ and $x \leq z < y$ implies $z = x$.

Let L be a lattice with the bottom element 0. Then an element a in L is called an *atom* if $0 \prec a$. If L is a finite lattice, then for all $x \in L$ with $x \neq 0$, there is an atom a such that $0 \prec a \leq x$.

A *Boolean algebra* is an algebraic structure $(B; \vee, \wedge, ', 0, 1)$ such that

(1) $(B; \vee, \wedge)$ is a distributive lattice,

(2) $x \vee 0 = x$ and $x \wedge 1 = x$ for all $x \in B$,

(3) $x \vee x' = 1$ and $x \wedge x' = 0$ for all $x \in B$.

Lemma 2.1. [14] *Let B be a Boolean algebra and $x, y \in B$. Then*

(1) $0' = 1$and $1' = 0$

(2) $x'' = x$,

(3) $(x \vee y)' = x' \wedge y'$ and $(x \wedge y)' = x' \vee y'$,

(4) $x \wedge y' = 0$ if and only if $x \leq y$,

(5) $x \leq y$ if and only if $x' \geq y'$.

If B is a finite Boolean algebra, then B has atoms and we will write A_B to denote the set of all atoms in B.

Lemma 2.2. [14] *Let B be a finite Boolean algebra. Then for each $x \in B$,*

$$x = \vee \{a \in A_B \mid a \leq x\}.$$

Lemma 2.3. [14] Let B be a finite Boolean algebra. Then the map $\eta : B \rightarrow P(A_B)$ given by

$$\eta(x) = \{a \in A_B \mid a \leq x\} \text{ for each } x \in B$$

is an isomorphism with the inverse η^{-1} of η given by $\eta^{-1}(S) = \vee S$ for each $S \in P(A_B)$, where $P(A_B)$ is the power set of A_B.

Further discussion of the fundamentals of Boolean algebra can be found in [14],[15].

Let B be a finite Boolean algebra and $x \in B$. We will write $A(x)$ to denote the subset

$$\{a \in A_B \mid a \leq x\}$$

of B. Then from Lemma 2.2 and 2.3, we have

$$A(x) = \eta(x) = \downarrow x \cap A_B,$$

$$x = \eta^{-1}(\eta(x)) = \vee A(x)$$

for all $x \in B$, where $\downarrow x = \{z \in B \mid z \leq x\}$.

Lemma 2.4. *Let B be a finite Boolean algebra. Then for any $x, y \in B$, $x \leq y$ if and only if $A(x) \subseteq A(y)$. In particular, $x = y$ if and only if $A(x) = A(y)$.*

Proof. Let $x \leq y$. Then $\downarrow x \subseteq \downarrow y$, and hence

$$A(x) = \downarrow x \cap A_B \subseteq \downarrow y \cap A_B = A(y).$$

Conversely, if $A(x) \subseteq A(y)$, then $x = \vee A(x) \leq \vee A(y) = y$. It is clear that $x = y$ if and only if $A(x) = A(y)$. □

Lemma 2.5. *Let B be a finite Boolean algebra and $x, y \in B$. Then the following are equivalent :*

(1) $A(x) \cap A(y) = \phi$;

(2) $\downarrow x \cap \downarrow y = \{0\}$;

(3) $x \wedge y = 0$.

Proof. ((1)⇒(2)) Let $A(x) \cap A(y) = \phi$. It is clear that $0\in \downarrow x \cap \downarrow y$. Suppose that there exists $z\in \downarrow x \cap \downarrow y$ such that $z \neq 0$. Then there is an atom a such that $0 \prec a \leq z$, that is $a \in A(z) \neq \phi$. Since $z \leq x$and $z \leq y$, we have

$$A(z) \subseteq A(x) \text{ and } A(z) \subseteq A(y)$$

from Lemma 2.4, and hence

$$\phi \neq A(z) \subseteq A(x) \cap A(y).$$

It is a contradiction. Hence $\downarrow x \cap \downarrow y = \{0\}$.

((2)⇒(3)) Let $\downarrow x \cap \downarrow y = \{0\}$. Since $x \wedge y \leq$ $\leq x$ and $x \wedge y \leq y$, we have

$$x \wedge y \in \downarrow x \cap \downarrow y = \{0\}.$$

Hence $x \wedge y = 0$.

((3)⇒(1)) Let $x \wedge y = 0$. Suppose that $A(x) \cap A(y) \neq \phi$. Then there is an atom z such that $z \leq x$ and $z \leq y$, that is, $0 < z \leq x \wedge y$, and it is a contradiction. Hence $A(x) \cap A(y) = \phi$. □

Definition 2.6. Let B be a finite Boolean algebra. Then for any $x, y \in B$, x and y are said to be *disjoint* if $x \wedge y = 0$.

Definition 2.7. Let B be a finite boolean algebra. Then the *weight* w on B is a map $w: B \to \mathbb{Z}$ given by

$$w(x) = |A(x)|$$

for each $x \in B$, where $|X|$ is the cardinality of a set X.

Lemma 2.8. *Let B be a finite boolean algebra. Then*

(1) $w(x) \geq 0$ *for all* $x \in B$,
in particular, $w(x) = 0 \Leftrightarrow x = 0$,

(2) $w(a) = 1$ for all $a \in A_B$,

(3) $x \leq y \Rightarrow w(x) \leq w(y)$ *for any* $x, y \in B$.

Proof. It is clear from the definition of weight. □

Proposition 2.9. Let B be a finite Boolean algebra *and* $x,y \in B$. *Then*

(1) $A(x \vee y) = A(x) \cap A(y)$

(2) $A(x \wedge y) = A(x) \cap A(y)$,

(3) $A(x) \cup A(x') = A_B$

(4) $A(x) \cap A(x') = \phi$

Proof. (1) Let $x, y \in B$. Since $x \leq x \vee y$ an $y \leq x \vee y$, we have

$$A(x) \subseteq A(x \vee y) \text{ and } A(y) \subseteq A(x \vee y).$$

by Lemma 2.4, Hence $A(x) \cup A(y) \subseteq A(x \vee y)$. Conversely, let $a \in A(x \vee y)$. Then a is an atom with $a \leq x \vee y$, and

$$0 \leq a \wedge x \leq a \text{ and } 0 \leq a \wedge y \leq a.$$

If $a \wedge x = 0$ and $a \wedge y = 0$, then

$$a = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y) = 0.$$

It is a contradiction. This implies that

$$a \wedge x \neq 0 \text{ or } a \wedge y \neq 0.$$

Since a is an atom, $a \wedge x = a$ or $a \wedge y = a$, that is, $a \leq x$ or $a \leq y$. Hence $a \in A(x) \cup A(y)$.

(2) Let $x, y \in B$. Then it is clear that $A(x \wedge y)$ $A(x) \cap A(y)$ since $x \wedge y \leq x$ and $x \wedge y \leq y$. Conversely, suppose that $a \in A(x) \cap A(y)$. Then $a \leq x$ and $a \leq y$. It follows that $a \leq x \wedge y$. Hence $a \in A(x \wedge y)$.

(3) Let $x \in B$. Then it is clear that

$$A(x) \cup A(x') \subseteq A_{B.}$$

To prove $A_B \subseteq A(x) \cup A(x')$, suppose that $a \in A_B$ and $a \not\in A(x)$. Then $a \wedge x < a$. Since a is an atom, $a \wedge x'' = a \wedge x = 0$. From Lemma 2.1(4), $a \leq x'$, that is, $a \in A(x')$. Hence

$$A_B \subseteq A(x) \cup A(x').$$

(4) Let $x \in B$. Then $x \wedge x' = 0$. Hence

$$A(x) \cap A(x') = \phi$$

from Lemma 2.5. □

Proposition 2.10. *Let B be a finite Boolean algebra, w the weight on B and $x,y \in B$. Then*

(1) $w(x \vee y) = w(x) + w(y) - w(x \wedge y)$,

(2) *if x and y are disjoint in B, then*
$w(x \vee y) = w(x) + w(y)$,

(3) $w(x \wedge y') = w(x) - w(x \wedge y)$.

Proof. (1) and (2) are trivial from Definition 2.7 and

Proposition 2.9.

(3) Let x, $y \in B$. Then

$$x = x \wedge (y \vee y') = (x \wedge y) \vee (x \wedge y'),$$

$(x \wedge y) \wedge (x \wedge y') = x \wedge (y \wedge y') = x \wedge 0 = 0$.

From (2) of this proposition, we have

$$\begin{aligned} w(x) &= w((x \wedge y) \vee (x \wedge y')) \\ &= w(x \wedge y) + w(x \wedge y'). \end{aligned}$$

Hence $w(x \wedge y') = w(x) - w(x \wedge y)$. □

Theorem 2.11. *Let B be a finite Boolean algebra and $x, y \in B$. Then*

(1) *if $a \in A_B$ and $a \not\in A(x)$ then $x \prec x \vee a$,*

(2) *if $x \prec y$, then there is a unique $a \in A_B$ such that $a \not\in A(x)$ and $y = x \vee a$.*

Proof. (1) Let $a \in A_B$ and $a \not\in A(x)$. Then

$$\begin{aligned} A(x \vee a) &= A(x) \cup A(a) = A(x) \cup \{a\} \\ &\neq A(x) \end{aligned}$$

and $x \vee a \neq x$ by Lemma 2.4, hence $x < x \vee a$. If $x \leq z < x \vee a$, then

$$A(x) \subseteq A(z) \subseteq A(x \vee a) = A(x) \cup \{a\}$$

by Lemma 2.4. Since $A(z) \neq A(x \vee a)$,

$$A(x) = A(z).$$

Hence $x = z$. It follows that $x \prec x \vee a$.

(2) Let $x \prec y$. Then $0 = x \wedge x' \leq y \wedge x'$. We will show that $y \wedge x'$ is an atom. If $y \wedge x' = 0$, then we have

$$y = y \wedge (x' \vee x) = (y \wedge x') \vee x = 0 \vee x = x,$$

and it is impossible, hence $y \wedge x' \neq 0$, that is, $0 < y \wedge x'$. Suppose that $0 \leq z < y \wedge x'$ for some $z \in B$. Then

$$\begin{aligned} x \leq z \vee x &\leq (y \wedge x') \vee x = y \wedge (x' \vee x) \\ &= y \wedge 1 = y. \end{aligned}$$

Since $x \prec y$, $z \vee x = x$ or $z \vee x = y$. If $z \vee x = y$, then we have

$$\begin{aligned} y \wedge x' &= (y \wedge x') \wedge y = (y \wedge x') \wedge (z \vee x) \\ &= z \vee ((y \wedge x') \wedge x) = z \vee 0 = z. \end{aligned}$$

It is impossible, hence $z \vee x = x$. Since $z < y \wedge x' \leq x'$ and $z \leq z \vee x = x$, $z \leq x \wedge x' = 0$. It follows that $z = 0$. Hence $y \wedge x'$ is an atom with $y \wedge x' \leq y$.

Set $a = y \wedge x'$. Then $a \not\in A(x)$ since $a \wedge x = (y \wedge x') \wedge x = 0$ and $x \vee a = x \vee (y \wedge x') = y$. To show that this atom a is unique, suppose that $a, b \in A_B$ and $x \vee a = y = x \vee b$. Then

$a \wedge x' = (x \vee a) \wedge x' = (x \vee b) \wedge x' = b \wedge x'$.

If $a \wedge x' = 0$, then we have

$$y = a \vee x = (a \wedge x') \vee x = 0 \vee x = x,$$

and it is impossible, hence $a \wedge x' \neq 0$. In the similar way, $b \wedge x' \neq 0$. Since a and b are atoms and since $a \wedge x' \leq a$ and $b \wedge x' \leq b$,

$$a \wedge x' = a \text{ and } b \wedge x' = b.$$

This imply that $a = a \wedge x' = b \wedge x' = b$. □

In Theorem 2.11(2), if $x \prec y$, then the unique atom a satisfying $y = x \vee a$ is $y \wedge x'$, and $a = y \wedge x' \in A(x')$.

Corollary 2.12. *Let B be a finite Boolean algebra and w the weight on B. Then for any $x, y \in B$,*

$$x \prec y \Rightarrow w(y) = w(x) + 1.$$

Proof. From Theorem 2.11(2), there is $a \in A_B$ such that $a \not\in A(x)$ and $y = x \vee a$, it follows that $A(y) = A(x) \cup A(a) = A(x) \cup \{a\}$, hence we have $w(y) = w(x) + 1$. □

Ⅲ. A DISTANCE ON BOOLEAN ALGEBRA

Lemma 3.1. *Let B be a boolean algebra. If we define a map $d : B \times B \to \mathbb{R}$ by*

$$d(x,y) = w((x \wedge y') \vee (x' \wedge y))$$

for every x, $y \in B$, then d satisfies the following :

(1) $d(x,y) \geq 0$,

(2) $d(x,y) = 0$ *if and only if* $x = y$,

(3) $d(x,y) = d(y,x)$,

(4) $d(x,y) \leq d(x,z) + d(z,y)$.

Proof. The proof of (1) and (3) is trivial. We need prove (2) and (4).

(2) It is trivial that $x = y$ implies $d(x,y) = 0$, because $x \wedge y' = x' \wedge y = x \wedge x' = 0$. Conversely, suppose that $d(x,y) = 0$. Then

$$0 = d(x,y) = w(x \wedge y') + w(x' \wedge y)$$

since $x \wedge y'$ and $x' \wedge y$ are disjoint. Hence we have

$$w(x \wedge y') = 0 \text{ and } w(x' \wedge y) = 0.$$

This implies that $x \wedge y' = 0$ and $x' \wedge y = 0$ from Lemma 2.8(1), and $x \le y$ and $y \le x$ from Lemma 2.1(4). It follows that $x = y$.

(4) Let $x, y, z \in B$. Since $x \wedge y' \le y'$ and $x \wedge y' \le x$, we have

$$\begin{aligned} x \wedge y' &= (x \wedge y') \wedge 1 \\ &= (x \wedge y') \wedge (z \vee z') \\ &= [(x \wedge y') \wedge z] \vee [(x \wedge y') \wedge z'] \\ &\le (y' \wedge z) \vee (x \wedge z'). \end{aligned}$$

In the similar way, we have

$$x' \wedge y \le (x' \wedge z) \vee (y \wedge z').$$

This implies that

$$\begin{aligned} &(x \wedge y') \vee (x' \wedge y) \\ &\quad \le (x \wedge z') \vee (x' \wedge z) \vee (y \wedge z') \vee (y' \wedge z) \end{aligned}$$

Hence we have

$$\begin{aligned} d(x,y) &= w((x \wedge y') \vee (x' \wedge y)) \\ &\le w((x \wedge z') \vee (x' \wedge z) \\ &\qquad \vee (y \wedge z') \vee (y' \wedge z)) \\ &\le w((x \wedge z') \vee (x' \wedge z)) \\ &\qquad + w((y \wedge z') \vee (y' \wedge z)) \\ &= d(x,z) + d(z,y) \end{aligned}$$

by Lemma 2.8(3) and Proposition 2.10. □

From Lemma 3.1, the map d is a metric on B, and d has the following property :

$$d(x,y) = w(x \wedge y') + w(x' \wedge y)$$

since $(x \wedge y') \wedge (x' \wedge y) = (x \wedge x') \wedge (y \wedge y') = 0$. Let B be a finite Boolean algebra. If $|A_b| = n$, then B contains 2^n elements, and if L_k is the set of all elements with weight k for each $k = 0, 1, 2, \ldots, n$, that is, $L_k = \{x \in B | w(x) = k\}$, then the set $\wp = \{L_k \mid k = 0, 1, 2, \ldots, n\}$ is a partition of B.

Proposition 3.2. *Let B be a finite Boolean algebra. Then for all x, $y \in B$,*

$$d(x,y) = w(x) + w(y) - 2w(x \wedge y).$$

Proof. It is clear from Proposition 2.10(3). □

Corollary 3.3. *Let B be a finite Boolean algebra with $|A_B| = n$, and let $x \in L_{m_1}$ and $y \in L_{m_2}$ with $0 \le m_{1,} m_2 \le n$. Then*

(1) *if $m_1 + m_2$ is even, then $d(x,y)$ is even,*

(2) *if $m_1 + m_2$ is odd, then $d(x,y)$ is odd,*

(3) *if $x, y \in L_m$ for any non-negative integer m with $m \le n$, then $d(x,y)$ is even.*

Proof. It follows immediately from the preceding Pro-position. □

Let B be a finite Boolean algebra. If δ is a non-negative integer and $x \in B$, then $B(x;\delta)$ is the set of all elements that has the distance δ from x, that is, $B(x;\delta) = \{y \in B \mid d(x,y) = \delta\}$.

The *sphere centered at x with radius δ* is defined by $S(x;\delta) = \{y \in B \mid d(x,y) \le \delta\}$. Form the definition of sphere, we have $S(x;\delta) = \bigcup_{i=0}^{\delta} B(x;i)$.

Proposition 3.4. *Let B be a finite Boolean algebra and δ a positive integer and $x \in B$. then $B(x;\delta)$ is the set of all elements of the form :*

$$y_1 \vee y_2,$$

where $y_1, y_2 \in B$ such that $y_1 \le x$, $y_2 \le x'$ and $w(y_1) - w(y_2) = w(x) - \delta$.

Proof. Suppose that $y \in B(x;\delta)$. Then

$$y = y \wedge (x \vee x') = (y \wedge x) \vee (y \wedge x').$$

Let $y_1 = y \wedge x$ and $y_2 = y \wedge x'$. Then $y_1 \le x$ and $y_2 \le x'$, and we have

$$\begin{aligned} \delta = d(x,y) &= w(x) + w(y) - 2w(x \wedge y) \\ &= w(x) + w(y) - 2w(y_1). \end{aligned}$$

by Proposition 3.2. Since $w(y)=w(y_1)+w(y_2)$,

$$\delta=w(x)+w(y_1)+w(y_2)-2w(y_1).$$

This implies that $w(x)-\delta=w(y_1)-w(y_2)$.

Conversely, suppose that $y_{1,}\, y_2 \in B$ such that $y_1 \le x$, $y_2 \le x'$ and $w(y_1)-w(y_2)=w(x)-\delta$. Then we have

$$\begin{aligned} x\wedge(y_1\vee y_2)' &= x\wedge {y_1}'\wedge {y_2}' \\ &= x''\wedge {y_2}'\wedge {y_1}' \\ &= (x'\vee y_2)'\wedge {y_1}' \\ &= x''\wedge {y_1}' \\ &= x\wedge {y_1}', \end{aligned}$$

and since $y_1\wedge x'=0$ by Lemma 2.1(4),

$$\begin{aligned} (y_1\vee y_2)\wedge x' &= (y_1\wedge x')\vee(y_2\wedge x') \\ &= 0\vee y_2 = y_2. \end{aligned}$$

Hence from Proposition 2.10(3), we have

$$\begin{aligned} & d(y_1\vee y_2, x) \\ &= w((y_1\vee y_2)\wedge x')+w((y_1\vee y_2)'\wedge x) \\ &= w(y_2)+w(x\wedge {y_1}') \\ &= w(y_2)+w(x)-w(x\wedge y_1) \\ &= w(y_2)+w(x)-w(y_1) \\ &= w(x)-(w(y_1)-w(y_2)) \\ &= w(x)-w(x)+\delta \\ &= \delta, \end{aligned}$$

and it follows that $y_1\vee y_2 \in B(x;\delta)$. □

Proposition 3.5. *Let B be a finite Boolean algebra and δ a positive integer. Then for any $x\in B$, the following are equivalent :*

(1) $y\in B(x;\delta)$,

(2) *there are δ atoms $a_1, a_2, \ldots, a_\delta$ such that $y=(x\wedge({a_1}'\wedge\cdots\wedge {a_m}'))\vee(a_{m+1}\vee\cdots\vee a_\delta)$ where $a_1,\ldots,a_m\in A(x)$ and $a_{m+1},\ldots,a_\delta \in A(x')$ for some $m\in\{0,1,2,\ldots,\delta\}$.*

Proof. ((1)⇒(2)) Let $y\in B(x;\delta)$. Then from Proposition 3.4, there are $y_{1,}\, y_2\in B$ such that $y=y_1\vee y_2$, and $y_1 \le x$, $y_2 \le x'$and

$$w(y_1)-w(y_2)=w(x)-\delta.$$

From Lemma 2.2 and 2.4,

$$y_1=c_1\vee\cdots\vee c_l$$

with $A(y_1)=\{c_1,\cdots,c_l\}\subseteq A(x)$, and

$$y_2=d_1\vee\cdots\vee d_r$$

with $A(y_2)=\{d_1,\cdots,d_r\}\subseteq A(x')$. If $\{a_1,\cdots,a_m\}=A(x)-\{c_1,\cdots,c_l\}$, then $A(x)=\{a_1,\cdots,a_m,c_1,\cdots,c_l\}$ and $m+l=w(x)$.

Let $\alpha={a_1}'\wedge\cdots\wedge {a_m}'$. Then we have

$$x=a_1\vee\cdots\vee a_m\vee c_1\vee\cdots\vee c_l=\alpha'\vee y_1.$$

Since c_i and a_j are atoms, $c_i\wedge {a_j}''=c_i\wedge a_j=0$, and by Lemma 2.1(4), $c_i \le {a_j}'$ for each $i=1,2,\cdots,l$ and $j=1,2,\cdots,m$. This implies that

$$y_1=c_1\vee\cdots\vee c_l \le {a_j}'$$

for each $j=1,2,\cdots,m$, and hence

$$y_1 \le {a_1}'\wedge\cdots\wedge {a_m}'=\alpha.$$

It follows that

$$x\wedge\alpha=(\alpha'\vee y_1)\wedge\alpha=y_1\wedge\alpha=y_1,$$

hence $y=y_1\vee y_2=(x\wedge\alpha)\vee y_2$. Since $w(y_1)-w(y_2)=w(x)-\delta$, that is, $l-r=l+m-\delta$ and $m+r=\delta$.

Set $d_i=a_{m+i}$ for each $i=1,2,\cdots,r$. Then $y_2=a_{m+1}\vee\cdots\vee a_\delta$ and

$$y=(x\wedge({a_1}'\wedge\cdots\wedge {a_m}'))\vee(a_{m+1}\vee\cdots\vee a_\delta)$$

with $a_1,\ldots,a_m\in A(x)$ *and* $a_{m+1},\ldots,a_\delta\in A(x')$.

((2)⇒(1)) Suppose that there are δ atoms $a_1, a_2, \cdots, a_\delta$ such that

$$y=(x\wedge({a_1}'\wedge\cdots\wedge {a_m}'))\vee(a_{m+1}\vee\cdots\vee a_\delta)$$

with $a_1,\ldots,a_m\in A(x)$ and $a_{m+1},\ldots,a_\delta\in A(x')$ for some $m\in\{0,1,2,\ldots,\delta\}$. Let $\alpha=a_1\vee\cdots\vee a_m$ and $\beta=a_{m+1}\vee\cdots\vee a_\delta$. Then

$$y=(x\wedge\alpha')\vee\beta,$$

where $\alpha\le x$, $\beta\le x'$, $w(\alpha)=m$, $w(\beta)=\delta-m$. Since $(x\wedge\alpha')\wedge\beta\le\alpha'\wedge(x\wedge x')=0$, we have

$$\begin{aligned} w(y) &= w(x\wedge\alpha')+w(\beta) \\ &= w(x)-w(x\wedge\alpha)+w(\beta) \\ &= w(x)-w(\alpha)+w(\beta) \\ &= w(x)+\delta-2m, \end{aligned}$$

and since $x\wedge\beta\le x\wedge x'=0$, that is, $x\wedge\beta=0$,

$$\begin{aligned} x\wedge y &= x\wedge((x\wedge\alpha')\vee\beta) \\ &= x\wedge(x\wedge\alpha') = x\wedge\alpha', \end{aligned}$$

hence we have

$$\begin{aligned} w(x\wedge y) &= w(x\wedge\alpha') \\ &= w(x)-w(x\wedge\alpha) \\ &= w(x)-w(\alpha) \\ &= w(x)-m. \end{aligned}$$

From Proposition 3.2, we have

$$\begin{aligned} & d(x,y) \\ &= w(x)+w(y)-2w(x\wedge y) \\ &= w(x)+(w(x)+\delta-2m)-2(w(x)-m) \\ &= \delta \end{aligned}$$

This implies that $y\in B(x;\delta)$. □

From the Proposition 3.4, the elements in $B(x;\delta)$ is characterized by δ atoms in B.

Corollary 3.6. *Let B be a finite Boolean algebra with $|A_B|=n$, and δ a positive integer. Then for every $x\in B$,*

(1) $|B(x;\delta)|=\binom{n}{\delta}$,

(2) $|S(x;\delta)|=\sum_{k=0}^{\delta}\binom{n}{k}$.

Proof. (1) It follows immediately from Proposition 3.5, that is, we can make an element in $B(x;\delta)$ by joining δ elements of A_B.

(2) It follows immediately from

$$S(x;\delta)=\bigcup_{k=0}^{\delta}B(x;k). \qquad \square$$

Let B be a finite Boolean algebra and $C\subseteq B$. We define the *minimum distance* of C as following:

$$d_m(C)=\min\{d(x,y)\mid x,y\in C \text{ and } x\neq y\}$$

and denote $\wp_\delta$ for the set of all subsets of B with minimum distance δ, that is,

$$\wp_\delta=\{C\subseteq B\mid d_m(C)=\delta\}.$$

Theorem 3.7. *Let B be a finite Boolean algebra with $|A_B|=n$ and δ a positive integer. Then*

$$|C|\le\frac{|B|}{\sum_{k=0}^{e}\binom{n}{k}}$$

for any $C\in\wp_\delta$, where $e=\left\lfloor\frac{\delta-1}{2}\right\rfloor$.

Proof. Let $C\in\wp_\delta$ and $x,y\in C$ with $x\neq y$. If $z\in S(x;e)\cap S(y;e)$, then we have

$$d(x,y)\le d(x,z)+d(z,y)\le e+e\le\delta-1,$$

and it is impossible because the minimum distance of C is δ. Hence $S(x;e)\cap S(y;e)=\phi$. It follows that

$$\sum_{x\in C}|S(x;e)|=|\bigcup_{x\in C}S(x;e)|\le|B|.$$

since $\bigcup_{x\in C}S(x;e)\subset B$. This implies that

$$|C||S(x;e)|\le|B|.$$

Hence $|C|\le\frac{|B|}{\sum_{k=0}^{e}\binom{n}{k}}$ from Corollary 3.6(2). □

Theorem 3.7 gives the optimal number of codewords (elements in C) for error-correcting. In general, C is called a perfect e-error-correcting code in coding theory if C satisfies the equality in Theorem 3.7.

Theorem 3.8. *Let B be a finite Boolean algebra $|A_B|=n$ and δ a positive integer. If $C\in\wp_\delta$ such that $|C|=\max\{|D|\mid D\in\wp_\delta\}$, then*

$$|C|\ge\frac{|B|}{\sum_{k=0}^{\delta-1}\binom{n}{k}}.$$

Proof. We need show that $\{S(x;\delta-1)\mid x\in C\}$ cover B. Suppose that $z\in B$ and $z\notin S(x;\delta-1)$ for all $x\in C$. Then $d(x,z)\ge\delta$ for all $x\in C$. It follows that $d(x,y)\ge\delta$ for all $x,y\in C\cup\{z\}$, hence $d_m(C\cup\{z\})=d_m(C)=\delta$. This is a contradiction to maximality of $|C|$ in $\wp_\delta$. So we have

$$\begin{aligned} |B| &\le|\bigcup_{x\in C}S(x;\delta-1)| \\ &\le\sum_{x\in C}|S(x;\delta-1)| \\ &=|C|\sum_{k=0}^{\delta-1}\binom{n}{k}. \end{aligned}$$

Hence we have $\frac{|B|}{\sum_{k=0}^{\delta-1}\binom{n}{k}}\le|C|$. □

Ⅳ. CONCLUSION

We defined a weight and a distance on Boolean algebras as a generalization of binary code, and represented basic properties of them. Also using the concepts of the weight and the distance, we proved the sphere-packing bound and the sphere-covering bound of Boolean algebra. We are sure that these concepts and notions can be used to the different boolean algebras with the binary codes, especially cryptographic algorithms, error correction codes, and network transmission for enhancing their quality and effectiveness.

REFERENCES

[1] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, 3rd ed., New York, NY : Springer, 1999.

[2] F. J. Mac Williams and N. J. A. Sloane, The Theory of Error-Correcting Code, North-Holland, Amsterdam, New York, Oxford, 1977.

[3] M. Plotkin, Binary codes with specified minimum distance, IRE Trans. Inform. Theory, vol. IT-6, pp. 445-450, Sept. 1960,

[4] G. D. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes, North-Holland, Amsterdam, 1997.

[5] G. D. Cohen, M. G. Karpovsky, H. F. Jr. Mattson and J. R. Schatz, Covering Radius - Survey and Recent Results, IEEE Trans. Inform. Theory, vol. 31, pp. 328-343, 1985.

[6] G. D. Cohen, S. N. Litsyn, A. C. Lobstein and H. F. Jr. Mattson, Covering Radius 1985-1994, Appl. Algebra Eng. Comm. Comp., vol. 8, pp. 173-239, 1997.

[7] R. L. Graham and N. J. A. Sloane, On the Covering Radius of Codes, IEEE Trans. Inform. Theory, vol. 31, pp. 385-401, 1985.

[8] G. Wiechman and I. Sason, An Improved Sphere-Packing Bound for Finite-Length Codes Over Symmetric Memoryless Channels, IEEE Trans. Inform. Theory, vol. 54. no. 5, pp. 1962 – 1990, May 2008.

[9] K. Mahdaviani , S. Shahidi, S. Haddadi, M. Ardakani and C. Tellambura, Improving the Sphere-Packing Bound for Binary Codes over Memoryless Symmetric Channels, 47 Annual Allerton Conference, pp. 553-557, 2009.

[10] V. Vu and L. Wu, Improving the Gilbert-Varshamov bound for q-ary codes, IEEE Trans. Inform. Theory, vol. 51, no. 9, pp. 3200 – 3208, Sept. 2005.

[11] R. Hill, A First Course in Coding Theory, Clarendon Press, Oxford, 1986.

[12] S. Roman, Coding and Information Theory, Springer-Verlag, 1992.

[13] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[14] B. A. Davey and H. A. Priestley, Introduction to lattices and order, Cambridge University Press, Cambridge, 1990.

[15] G. Grätzer, General lattice theory Academic press, inc. New York, 1978.

연 용 호 (延鎔鎬)

1997.8 : Ph. D. degree in Department of Mathematics, Chungbuk National University.

2011.3.1 : Assistant Professor in Innovation Center for Engineering Education, Mokwon University.

Research Interesting : Algebras with Implication, Quantum Logics, 302-729, Korea

강 안 나

1991 : M. Ed. degree in Department of Computer Education, Kyung Hee University.

2008 : Ph. D degree in Department of Electronic Information and Communication Engineering, Mokwon University

2009.3.1.~ : Assistant Professor in Innovation Center for Engineering Education, Mokwon University

Research interests : Multimedia, Engineering education, Creative Problem Solving.