A Weight on Boolean Algebras for Cryptography and Error Correcting Codes

Yong-Ho Yon' An-Na Kang

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

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.
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 section 3, 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 \((B; \lor, \land, \neg, 0, 1)\) such that
1. \((B; \lor, \land)\) is a distributive lattice,
2. \(x \lor 0 = x\) and \(x \land 1 = x\) for all \(x \in B\),
3. \(x \lor x' = 1\) and \(x \land x' = 0\) 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. \((x \lor y)' = x' \land y'\) and \((x \land y)' = x' \lor y'\),
4. \(x \land y' = 0\) 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 \(x \in B\),
\[x = \lor \{a \in A_B | a \leq x\}\].

**Lemma 2.3.** [14] Let \(B\) be a finite Boolean algebra. Then the map \(\eta : B \to P(A_B)\) given by
\[\eta(x) = \{a \in A_B | a \leq x\}\] for each \(x \in B\)
is an isomorphism with the inverse \(\eta^{-1}\) of \(\eta\) given by \(\eta^{-1}(S) = \lor S\) 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
\[\{a \in A_B | a \leq x\}\]
of \(B\). Then from Lemma 2.2 and 2.3, we have
\[A(x) = \eta(x) = \lor x \cap A_B,\]
\[x = \eta^{-1}(\eta(x)) = \lor A(x)\]
for all \(x \in B\), where \(\lor x = \{z \in B | z \leq x\}\).

**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 \(\lor x \subseteq \lor y\), and hence
\[A(x) = \lor x \cap A_B \subseteq \lor y \cap A_B = A(y)\].
Conversely, if \(A(x) \subseteq A(y)\), then \(x = \lor A(x) \leq \lor A(y) = y\). It is clear that \(x = y\) if and only if \(A(x) = A(y)\). \(\square\)

**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. \(\lor x \cap \lor y = \{0\}\);
3. \(x \land y = 0\).

**Proof.** ((1)\(\Rightarrow\)(2)) Let \(A(x) \cap A(y) = \phi\). It is