On Codes based on $BCK$-algebras

A. Borumand Saeid, H. Fatemidokht, C. Flaut and M. Kuchaki Rafsanjani

Abstract. In this paper, we present some new connections between $BCK$-algebras and binary block codes.

Keywords: $BCI/BCK$-algebras; Binary block codes; Partially ordered set.

AMS Classification. 06F35, 94B60.

1 Introduction

$BCI/BCK$-algebras were first introduced in mathematics in 1966 by Y. Imai and K. Iseki, through the paper [Im, Is; 66], as a generalization of the concept of set-theoretic difference and propositional calculi. One of the recent applications of $BCK$-algebras was given in the Coding Theory (see [Fl; 14], [Ju, So; 11]).

2 Preliminaries

Definition 2.1. An algebra $(X, *, \theta)$ of type $(2,0)$ is called a $BCI$-algebra if the following conditions are fulfilled:

- $BCI-1$ $(x * y) * (x * z)) * (z * y) = \theta$
- $BCI-2$ $(x * (x * y)) * y = \theta$
- $BCI-3$ $x * x = \theta$
- $BCI-4$ $x * y = \theta$ and $y * x = \theta$ imply $x = y$
If a BCI-algebra $X$ satisfies the following identity:

- **BCK-5** $\theta \ast x = \theta$

then $X$ is called a BCK-algebra [Me, Ju; 94].

The partial order relation on a $BCI/BCK$-algebra is defined such that $x \leq y$ if and only if $x \ast y = \theta$.

A $BCI/BCK$-algebra $X$ is called commutative if $x \ast (x \ast y) = y \ast (y \ast x)$, for all $x, y \in X$ and implicative if $x \ast (y \ast x) = x$, for all $x, y \in X$.

If $(X, \ast, \theta)$ and $(Y, \circ, \theta)$ are two $BCI/BCK$-algebras, a map $f : X \to Y$ with the property $f(x \ast y) = f(x) \circ f(y)$, for all $x, y \in X$, is called a $BCI/BCK$-algebras morphism. If $f$ is a bijective map, then $f$ is an isomorphism of $BCI/BCK$-algebras [Me, Ju; 94].

Hereafter in this paper, $X$ always denotes a finite $BCI/BCK$-algebra.

**Definition 2.2.** A mapping $\tilde{A} : A \to X$ is called a BCK-function on $A$, which $A$ and $X$ is a nonempty set and a BCK-algebra, respectively.

**Definition 2.3.** A cut function of $\tilde{A}$, for $q \in X$, is defined to be a mapping $\tilde{A}_q : A \to \{0, 1\}$ such that $(\forall x \in A)(\tilde{A}_q(x) = 1 \iff q \ast \tilde{A}(x) = \theta)$

**Definition 2.4.** Let $A = \{1, 2, \ldots, n\}$ and let $X$ be a $BCK$-algebra. In [Ju, So; 11], to each $BCK$-function $\tilde{A} : A \to X$ can be associated a binary block-code of length $n$. A codeword in a binary block-code $V$ is $v_x = x_1x_2\ldots x_n$ such that $x_i = x_j \Leftrightarrow A_x(i) = j$ for $i \in A$ and $j \in \{0, 1\}$.

Let $v_x = x_1x_2\ldots x_n$ and $v_y = y_1y_2\ldots y_n$ be two codewords belonging to a binary block-code $V$. Define an order relation $\leq_c$ on the set of codewords belonging to a binary block-code $V$ as follows [Ju, So; 11]:

$v_x \leq_c v_y \Leftrightarrow y_i \leq x_i$ for $i = 1, 2, \ldots, n$. 

2
3 Main results

Definition 3.1. Let \((S, \leq)\) be a partially ordered set. For \(q \in S\), we define a mapping
\[
S_q : S \rightarrow \{0, 1\}
\]
such that
\[
(\forall b \in S)(S_q(b) = 1 \iff q \leq b).
\]
A codeword \(v_x = x_1x_2\cdots x_n\) of a binary block-code \(V\) is determined as follow:
\[
x_i = x_j \iff S_x(i) = j, \text{ for } i \in S \text{ and } j \in \{0, 1\}.
\]

Example 3.2. Let \(S = \{0, 1, 2, 3, 4\}\) be a set with a partial order over \(S\) showed in the Figure 1(a).

![Figure 1](image_url)

\((S, \leq)\)
\((V, \leq_c)\)

Figure 1: a) partial ordering. b) order relation \(\leq_c\)
then

| \( S_x \) | 0 | 1 | 2 | 3 | 4 |
|----------|---|---|---|---|---|
| \( S_0 \) | 1 | 1 | 1 | 1 | 1 |
| \( S_1 \) | 0 | 1 | 1 | 1 | 1 |
| \( S_2 \) | 0 | 0 | 1 | 0 | 1 |
| \( S_3 \) | 0 | 0 | 0 | 1 | 1 |
| \( S_4 \) | 0 | 0 | 0 | 0 | 1 |

and thus \( V_1 - P = \{11111, 01111, 00101, 00011, 00001\} \).

**Example 3.3.** Let \( S = \{0, 1, 2, 3, 4\} \) be a set with a partial order over \( S \) showed in the figure 2(a).

![Figure 2](image)

Figure 2: a) partial ordering. b) order relation \( \leq_c \)
then

| \( S_\sigma \) | 0 | 1 | 2 | 3 | 4 |
|----------------|---|---|---|---|---|
| \( S_0 \)     | 1 | 1 | 1 | 1 | 1 |
| \( S_1 \)     | 0 | 1 | 0 | 1 | 0 |
| \( S_2 \)     | 0 | 0 | 1 | 0 | 1 |
| \( S_3 \)     | 0 | 0 | 0 | 1 | 0 |
| \( S_4 \)     | 0 | 0 | 0 | 0 | 1 |

and thus \( V_2 - P = \{11111, 01010, 00101, 00010, 00001\} \).

**Example 3.4.** Let \( S = \{A, B, C, D\} \) be a set with a partial order over \( S \) as in the Figure 3(a).

In the following, we will compute binary block-code based on Definition 2.4. for \( BCK \)-algebras. We will show that there is a correspondence between the ordered relation on \( BCK \)-algebra and partial ordered set.

![Figure 3: a)partial ordering. b)order relation \( \leq_c \)](image)
Example 3.5. Let \( X = \{0, 1, 2, 3, 4\} \) be a BCK-algebra with the following Cayley table:

\[
\begin{array}{c|cccc}
* & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 \\
2 & 2 & 1 & 0 & 1 \\
3 & 3 & 3 & 3 & 0 \\
4 & 4 & 4 & 4 & 0 \\
\end{array}
\]

![Figure 4: a) ordered relation. b) order relation \( \leq_c \)](image)

The above figure is the ordered relation on \( X \).

Let \( \tilde{A} : X \rightarrow X \) be a BCK-function on \( X \) given by

\[
\tilde{A} = \begin{pmatrix}
0 & 1 & 2 & 3 & 4 \\
0 & 1 & 2 & 3 & 4 \\
\end{pmatrix}
\]

then

\[
\begin{array}{c|cccc}
\tilde{A}_x & 0 & 1 & 2 & 3 \\
\hline
\tilde{A}_0 & 1 & 1 & 1 & 1 \\
\tilde{A}_1 & 0 & 1 & 1 & 1 \\
\tilde{A}_2 & 0 & 0 & 1 & 0 \\
\tilde{A}_3 & 0 & 0 & 0 & 1 \\
\tilde{A}_4 & 0 & 0 & 0 & 0 \\
\end{array}
\]
thus $V_1 - B = \{11111, 01111, 00101, 00011, 00001\}$.

**Example 3.6.** Let $X = \{0, 1, 2, 3, 4\}$ be a BCK-algebra with the following Cayley table:

| $*$ | 0 | 1 | 2 | 3 | 4 |
|-----|---|---|---|---|---|
| 0   | 0 | 0 | 0 | 0 | 0 |
| 1   | 1 | 0 | 1 | 0 | 1 |
| 2   | 2 | 0 | 2 | 0 | 0 |
| 3   | 3 | 1 | 3 | 0 | 3 |
| 4   | 4 | 2 | 4 | 0 | 0 |

Figure 5: a) ordered relation. b) order relation $\leq_c$

The above figure is the ordered relation on $X$.

Let $\tilde{A} : X \to X$ be a BCK-function on $X$ given by

$$\tilde{A} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

then
\[\begin{array}{cccccc}
\hat{A}_x & 0 & 1 & 2 & 3 & 4 \\
\hat{A}_0 & 1 & 1 & 1 & 1 & 1 \\
\hat{A}_1 & 0 & 1 & 0 & 1 & 0 \\
\hat{A}_2 & 0 & 0 & 1 & 0 & 1 \\
\hat{A}_3 & 0 & 0 & 0 & 1 & 0 \\
\hat{A}_4 & 0 & 0 & 0 & 0 & 1 \\
\end{array}\]

thus \(V_2 - B = \{11111, 01010, 00101, 00010, 00001\}\).

**Remark 3.7.** On a partial ordered set with a minimum element \(\theta\) we can define a \(BCK\)-algebra structure (see [Fl; 14], (2.1)) From the obtained block-codes by the aforesaid methods, it is obvious that \(V_1 - P = V_1 - B\) and \(V_2 - P = V_2 - B\). We think that the problem occurred because we use only the order of \(BCK\)-algebra, not its algebraic properties. From above examples, it is obvious that the method presented in paper [Ju, So; 11] does not depend on algebraic properties of \(BCK\)-algebra. Also the obtained codes are not good codes, since their Hamming distance is not good. According to the figures 1 to 5, there is a one-to-one correspondence between the ordering relation \(\leq\) and order relation \(\leq_c\).

Let \(X\) be a \(BCK\)-algebra and \(V\) be a linear binary block-code with \(n\) codewords of length \(n\). We consider the matrix \(M_V = (m_{i,j})_{i,j \in \{1,2,\ldots,n\}} \in \mathcal{M}_n(\{0,1\})\) with the rows consisting of the codewords of \(V\). This matrix is called the *matrix associated to the code* \(V\). We consider the codewords in \(V\) lexicographic ordered in the ascending sense. With this remark, for \(V = \{w_1, \ldots, w_n\}\), we denote lines in \(M_V\) with \(L_{w_1}, \ldots, L_{w_n}\). Obviously, \(w_1 = \underbrace{00\ldots0}_{n\text{-time}}\). On \(V\), we define the following multiplication "\(*\)"

\[w_i \ast w_j = w_k \text{ if and only if } L_{w_i} + L_{w_j} = L_{w_k}.\]  

(2.1.)

**Proposition 3.8.** With this multiplication, \((V, \ast, \theta)\), where \(\theta = w_1\), becomes an abelian group. \(\square\)

**Remark 3.9.** The above group is a \(BCI\)-algebra.
Example 3.10. We consider the binary linear code $C = \{0000, 0001, 0010, 0011\} = \{\theta, A, B, C\}$. The associated $BCI$-algebra (group) is $X = \{\theta, A, B, C\}$ with zero element $\theta$ and multiplication given in the following table:

|  *  | $\theta$ | A   | B   | C   |
|-----|---------|-----|-----|-----|
| $\theta$ | $\theta$ | A   | B   | C   |
| A   | A       | $\theta$ | C   | B   |
| B   | B       | C   | $\theta$ | A   |
| C   | C       | B   | A   | $\theta$ |

Definition 3.11. Let $(X, *, \theta)$ be a $BCI/BCK$-algebra, and $I \subseteq X$. We say that $I$ is a right-ideal if $\theta \in I$ and $x \in I, y \in X$ imply $x * y \in I$. An ideal $I$ of a $BCI/BCK$-algebra $X$ is called a closed ideal if it is also a subalgebra of $X$ (i.e. $\theta \in I$ and if $x, y \in I$ it results that $x * y \in I$).

Let $C$ be a binary block code. In Theorem 2.9, from [Fl; 14], we find a $BCK$-algebra $X$ such that the obtained binary block-code $V_X$ contains the binary block-code $C$ as a subset.

Let $C$ be a binary block code with $m$ codewords of length $q$. With the above notations, let $X$ be the associated $BCK$-algebra and $W = \{\theta, w_1, ..., w_{m+q}\}$ the associated binary block code which include the code $C$. We consider the codewords $\theta, w_1, w_2, ..., w_{m+q}$ lexicographic ordered, $\theta \geq_{\text{lex}} w_1 \geq_{\text{lex}} w_2 \geq_{\text{lex}} ... \geq_{\text{lex}} w_{m+q}$. Let $M \in M_{m+q+1}(\{0, 1\})$ be the associated matrix with the rows $\theta, w_1, ..., w_{m+q}$, in this order. We denote with $L_{w_i}$ and $C_{w_j}$ the lines and columns in the matrix $M$. The sub-matrix $M'$ of the matrix $M$ with the rows $L_{w_1}, ..., L_{w_m}$ and the columns $C_{w_{m+1}}, ..., C_{w_{m+q}}$ is the matrix associated to the code $C$.

Proposition 3.12. With the above notations, we have that $\{\theta, w_{m+1}, ..., w_{m+q}\}$ determines a closed right ideal in the algebra $X$.

Proof. Let $Y = \{\theta, w_{m+1}, ..., w_{m+q}\}$. Due to the multiplications and the order relation $\leq$ given by the relations (2.1) and (1.1) from [Fl; 14], we can have only the following two possibilities: $w_i * w_j = \theta$ or $w_i * w_j = w_i$. Therefore $Y$ is a
right-ideal in $X$. The multiplication (2.1.) is:

$$\begin{align*}
\theta \ast x &= \theta \quad \text{and} \quad x \ast x = \theta, \forall x \in X; \\
x \ast y &= \theta, \text{ if } x \leq y, \quad x, y \in X; \\
x \ast y &= x, \text{ otherwise.}
\end{align*}$$

\[\Box\]

**Remark 3.13.** From Proposition 3.12, we obtain that to each binary block code we can associate a $BCK$-algebra in which this code determines a right ideal.

Let $A$ be a nonempty set and $X$ be a $BCK$-algebra.

**Proposition 3.14.** Let $C$ be a binary block code with $m$ codewords of length $q$ and let $X$ be the associated $BCK$-algebra, as the above. Therefore, there are the sets $A$ and $B \subseteq X$, the $BCK$-function $f : A \to X$ and a cut function $f_r$ such that

$$C = \{f_r : A \to \{0, 1\} / f_r(x) = 1, \text{ if and only if } r \ast f(x) = \theta, \forall x \in A, r \in B\}.$$

\[\Box\]

**Remark 3.15.**

i) Let $S = \{1, 2, ..., n\}$ be the set with $n$ elements. We know that $(\mathcal{P}(S), \Delta, \cap)$ is a Boolean ring, where $\mathcal{P}(S)$ is the power set of the set $S$, $\Delta$ is symmetric difference of the sets and $\cap$ is the intersection of two sets. Let $\mathcal{F} = \{f : S \to \{0, 1\} / f \text{ function}\}$. To each $f \in \mathcal{F}$ corresponds a binary block codeword. To each binary block codeword $c_1$ corresponds an element from $\mathcal{P}(S)$. Indeed, to each binary codeword $c = (i_1, ..., i_n)$ we will associate the set $I_c = \{j_1, j_2, ..., j_k\} \in \mathcal{P}(S)$ such that $i_{j_1} = i_{j_2} = ... = i_{j_k} = 1$.

ii) Using the above established correspondence, if $C = \{c_1, c_2, ..., c_m\}$ is a linear binary block code and $Q = \{I_{c_1}, I_{c_2}, ..., I_{c_m}\} \subseteq \mathcal{P}(S)$, where $I_{c_i}$ is the associated subset for the codeword $c_i$, then $Q$ is a sub-ring in the Boolean ring $(\mathcal{P}(S), \Delta, \cap)$. It results a bijective map between the sub-rings of the Boolean ring $(\mathcal{P}(S), \Delta, \cap)$ and linear binary block codes with codewords of length $n$.

**Example 3.16.**

i) Let $C = \{0000, 0001, 0010, 0011\} = \{w_6, w_7, w_8, w_9\}$ be a linear binary block code and let $X = \{\theta, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9\}$ be the...
obtained BCK-algebra as in Theorem 2.9 from [Fl; 14]. The multiplication of
this algebra is given in the below table

| * | θ | w_2 | w_3 | w_4 | w_5 | w_6 | w_7 | w_8 | w_9 |
|---|---|---|---|---|---|---|---|---|---|
| θ | θ | θ | θ | θ | θ | θ | θ | θ | θ |
| w_2 | w_2 | θ | w_2 | w_2 | w_2 | w_2 | θ | θ | θ |
| w_3 | w_3 | θ | w_3 | w_3 | w_3 | w_3 | θ | w_3 | θ |
| w_4 | w_4 | w_4 | θ | w_4 | w_4 | w_4 | w_4 | θ | w_4 |
| w_5 | w_5 | w_5 | w_5 | θ | w_5 | w_5 | w_5 | w_5 | θ |
| w_6 | w_6 | w_6 | w_6 | w_6 | θ | w_6 | w_6 | w_6 | θ |
| w_7 | w_7 | w_7 | w_7 | w_7 | w_7 | θ | w_7 | w_7 | θ |
| w_8 | w_8 | w_8 | w_8 | w_8 | w_8 | θ | w_8 | w_8 | θ |
| w_9 | w_9 | w_9 | w_9 | w_9 | w_9 | w_9 | w_9 | w_9 | θ |

From Proposition 3.12, we remark that \{θ, w_6, w_7, w_8, w_9\} is a right ideal
in the BCK-algebra X. From Proposition 3.14, for \(A = \{w_6, w_7, w_8, w_9\}\)
and \(B = \{w_2, w_3, w_4, w_5\}\), we recover the initial code \(C\).

**Example 3.17.** For the same linear binary block code \(C = \{0000, 0001, 0010, 0011\}\),
let \(Q = \{∅, \{4\}, \{3\}, \{3, 4\}\}\) as in Remark 3.15 ii). It is clear that \(Q\) is a sub-
ing the Boolean ring \((\mathcal{P}(\{1, 2, 3, 4\}), \Delta, \cap)\) and \(C\) can be considered as a
sub-ring of this Boolean ring.

**Remark 3.18.** In [Fl; 14], Theorem 2.2, the studied binary block codes have
Hamming distance equal with 1. In the same paper, Theorem 2.9, to an arbitrary
binary block code \(C\) we associate a BCK algebra \(X\) and the code associated to
this algebra includes the code \(C\). Proposition 3.14 improved this theorem since
we can even obtain the code \(C\) and from Proposition 3.12 we have that the code
\(C\) generate a right ideal in the algebra \(X\).

**Remark 3.19.** The obtained results of above remarks and propositions can
be illustrated by partially ordered sets. Let \(C\) be a binary block code with \(m\)
codewords of length \(q\). According to Proposition 2.8 and Theorem 2.9 in [Fl;
14], we can find the matrix \(M \in \mathcal{M}_{m+q+1}(\{0, 1\})\) that is the matrix associated
to the code \(C\). Let \(S\) be the associated partially ordered set. Therefore, there
are the sets \(A\) and \(B \subseteq S\) and the function \(f : A \to S\), such that we can define
the bellow set:

\[C = \{f_r : A \to \{0, 1\} / f_r(b) = 1, \text{if and only if } r \leq b, \forall b \in A, r \in B\}.\]
Here, \( A = \{m+2, \cdots, m+q+1\} \) and \( B = \{2, \cdots, m+1\} \).

**Example 3.20.** Let \( C = \{0000, 0001, 0010, 0011\} \) be a linear binary block code and let \( S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \). In this example \( m = q = 4 \). The matrix associated to the code \( C \) is:

\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
\]

Figure 6: partial ordering.

The above figure is partial ordering over \( S \). From above Proposition, \( A = \{6, 7, 8, 9\} \) and \( B = \{2, 3, 4, 5\} \) that from \( A \) and \( B \), we can recover the initial code \( C \).
Conclusions. Even if, from the above examples, appears that the associated binary block codes depend only from the order relation defined on a $BCK$-algebra, will be very interesting to study in a further paper how and if the properties of $BCK$-algebras can influence the properties of the associated binary block codes.

References

[Im, Is; 66] Y. Imai, K. Iseki, *On axiom systems of propositional calculi*, Proc. Japan Academic, **42**(1966), 19-22.

[Fl; 14] C. Flaut, *$BCK$-algebras arising from block codes*, arxiv.

[Ju, So; 11] Y. B. Jun, S. Z. Song, *Codes based on $BCK$-algebras*, Inform. Sciences., **181**(2011), 5102-5109.

[Me, Ju; 94] J. Meng and Y.B. Jun, *$BCK$-algebras*, Kyung Moon Sa Co. Seoul, Korea, 1994.

Arsham Borumand Saeid
Dept. of Math. Shahid Bahonar University of Kerman, Kerman, Iran
e-mail: arsham@uk.ac.ir

Cristina Flaut
Faculty of Mathematics and Computer Science, Ovidius University, Bd. Mamaia 124, 900527, Constanta, ROMANIA
e-mail: cristina_flaut@yahoo.com

H. Fatemidokht and Marjan Kuchaki Rafsanjani
Dept. of Computer Science Shahid Bahonar University of Kerman, Kerman, Iran
e-mail: kuchaki@uk.ac.ir.