Boolean Differential Operators

Jorge Catumba and Rafael Díaz

Abstract

We consider four combinatorial interpretations for the algebra of Boolean differential operators and construct, for each interpretation, a matrix representation for the algebra of Boolean differential operators.

Keywords: Boolean Algebras, Differential Operators, Directed Graphs.

MSC: 05E15, 05C76, 03G05.

1 Introduction

A Boolean function with $n$-arguments, $n \in \mathbb{N}$, is a map $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, where $\mathbb{Z}_2 = \{0, 1\}$ is the field with two elements. The $\mathbb{Z}_2$-algebra $\text{BF}_n$ of Boolean functions on $n$-arguments, with pointwise sum and multiplication, is isomorphic to the Boolean algebra $\text{PP}[n]$ of sets of subsets of $[n] = \{1, ..., n\}$. Indeed, we identify a vector in $\mathbb{Z}_2^n$ with an element of $\text{P}[n]$ via the characteristic function, and we identify a map $\text{P}[n] \rightarrow \mathbb{Z}_2$ with a subset of $\text{P}[n]$ again with the help of characteristic functions. The sum and product of Boolean functions correspond to the symmetric difference and the intersection of subsets of $\text{P}[n]$, respectively. The canonical isomorphism $\text{BF}_n \simeq \text{PP}[n]$ just described establishes the link between classical propositional logic and set theory [1].

The partial derivative $\partial_i f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, for $i \in [n]$, of a Boolean function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, see [3], is given by

$$\partial_i f(a) = f(a + e_i) + f(a),$$

(1)

where $a \in \mathbb{Z}_2^n$ and $e_i$ is the vector with 1 at the $i$-th position and 0’s at the other positions.
We define the \( \mathbb{Z}_2 \)-algebra \( \text{BDO}_n \) of Boolean differential operators on \( \mathbb{Z}_2^n \) in analogy with the definition of differential operators on the affine space \( k^n \), for a field \( k \) of characteristic zero, i.e. \( \text{BDO}_n \) is the subalgebra of \( \text{End}_{\mathbb{Z}_2}(\text{BF}_n) \) generated by the operators of multiplication by Boolean functions, and the partial derivative operators \( \partial_i \) defined in (1).

It turns out that \( \text{BDO}_n = \text{End}_{\mathbb{Z}_2}(\text{BF}_n) \), see [2], i.e. any \( \mathbb{Z}_2 \)-linear operator from \( \text{BF}_n \) to itself is actually given by a Boolean differential operator. Therefore a Boolean differential operator \( A \in \text{BDO}_n \) is just a map

\[
A : \text{BF}_n \rightarrow \text{BF}_n \quad \text{such that} \quad A(f + g) = A(f) + A(g), \quad \text{for} \quad f, g \in \text{BF}_n.
\]

We are interested in finding a suitable set theoretical interpretation for the algebras \( \text{BDO}_n \) that extends the above mentioned interpretation of \( \text{BF}_n \) as the Boolean algebra \( \text{PP}[n] \), and may shed a light towards a logical understanding of the \( \mathbb{Z}_2 \)-algebras \( \text{BDO}_n \). Indeed, we believe that the \( \mathbb{Z}_2 \)-algebras \( \text{BDO}_n \) may play a semantic role, analogous to that played by truth functions in classical logic, within the context of a "quantum like" operational logic yet to be fully understood. A few steps in that direction are taken in [2].

Our main goal in this work is to find suitable matrix representations for the \( \mathbb{Z}_2 \)-algebras \( \text{BDO}_n \). By dimension counting \( \text{BDO}_n = \text{End}_{\mathbb{Z}_2}(\text{BF}_n) \) is non-canonically isomorphic to the \( \mathbb{Z}_2 \)-algebra \( \text{M}_{2^n \times 2^n}(\mathbb{Z}_2) \) of square matrices of size \( 2^n \) with 0-1 entries. Note that \( \text{M}_{2^n \times 2^n}(\mathbb{Z}_2) \) may be identified, via characteristic functions, with \( \text{P}(\text{P}[n] \times \text{P}[n]) \) the set of subsets of \( \text{P}[n] \times \text{P}[n] \), or equivalently, with the set \( \text{DG}_{\text{P}[n]} \) of simple directed graphs (possibly with loops) with vertex set \( \text{P}[n] \). A matrix \( A \in \text{M}_{2^n \times 2^n}(\mathbb{Z}_2) = \text{P}(\text{P}[n] \times \text{P}[n]) \) is regarded as a directed graph with vertex set \( \text{P}[n] \) by drawing an edge from \( b \in \text{P}[n] \) to \( a \in \text{P}[n] \) if and only if \( (a, b) \in A \). The sum and product of matrices in \( \text{M}_{2^n \times 2^n}(\mathbb{Z}_2) \) induce operations of sum and product of digraphs in \( \text{DG}_{\text{P}[n]} \). The sum on \( \text{DG}_{\text{P}[n]} \) is the symmetric difference. The product \( AB \) of digraphs \( A, B \in \text{DG}_{\text{P}[n]} \) is such that the pair \( (a, b) \in AB \) if and only if there is an odd number of sets \( c \in \text{P}[n] \) such that \( (a, c) \in A \) and \( (c, b) \in B \).

To define an explicit isomorphism \( \text{BDO}_n \cong \text{M}_{2^n \times 2^n}(\mathbb{Z}_2) \) a choice of basis for
must be made. In this work we only consider the basis \( \{ m^a \mid a \in P[n] \} \) for 
\( \text{BF}_n \), where the Boolean function \( m^a : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2 \) is given on \( b \in P[n] \) by:
\[
m^a(b) = \begin{cases} 
1 & \text{if } a = b, \\
0 & \text{otherwise}.
\end{cases}
\]

We let \( [A] \in M_{2^n \times 2^n}(\mathbb{Z}_2) \) be the matrix of the Boolean differential operator 
\( A \in \text{BDO}_n \) in the basis \( \{ m^a \mid a \in P[n] \} \).

We are going to use the following simple algebraic construction. Let \( A \) be a 
\( \mathbb{Z}_2 \)-algebra, \( V \) a \( \mathbb{Z}_2 \)-vector space, and \( l : V \rightarrow A \) be a \( \mathbb{Z}_2 \)-linear bijective map. 
We use \( l \) to pullback the product on \( A \) to a product on \( V \) given for \( v, w \in V \) by
\[
vw = l^{-1}(l(v)l(w)).
\]

With this product on \( V \) the map \( l \) becomes an algebra isomorphism.

As we shall see each of our choices of bases for \( \text{BDO}_n \) induces a \( \mathbb{Z}_2 \)-linear bijective map from \( \text{DG}_{P[n]} \) to \( \text{BDO}_n \). In \cite{2} we use four such bijections to pullback the composition product on \( \text{BDO}_n \) to \( \text{DG}_{P[n]} \), thus we obtain four products on 
\( \text{DG}_{P[n]} \) denoted, respectively, by \( * \), \( \circ \), \( \bullet \), \( * \). Having various presentations for the 
product on \( \text{BDO}_n \) is desirable, just as it is useful to generate truth functions by 
several types of logical connectives.

Our main goal in this work is to explicitly describe matrix representations for 
the products \( * \), \( \circ \), \( \bullet \), \( * \) on \( \text{DG}_{P[n]} \). It turns out that the product \( * \) is the easiest 
to handle, in Section 2 we discuss some of its basic properties and describe an 
explicit isomorphism with \( M_{2^n \times 2^n}(\mathbb{Z}_2) \). In the remaining Sections, we present explicit 
isomorphisms between the products \( \circ \), \( \bullet \), \( * \) and the product on \( M_{2^n \times 2^n}(\mathbb{Z}_2) \), 
the algebra of square matrices of size \( 2^n \) with entries in \( \mathbb{Z}_2 \).

Let us comment on some conventions assumed in this work. In the figures 
we draw a subset of \( P[n] \times P[n] \) as a subset of the real plane, using the bijective correspondence between \( P[n] = \mathbb{Z}_2^n \) and the natural numbers in the interval 
\([0, 2^n - 1]\) resulting of ordering \( P[n] \) by cardinality and lexicographic order within
a given cardinality. For example $P[2]$ and $[0, 3]$ are in correspondence as follows $\emptyset \rightarrow 0$, $\{1\} \rightarrow 1$, $\{2\} \rightarrow 2$, $\{1, 2\} \rightarrow 3$. When drawing a product, the elements of the first factor are drawn as triangles; the elements of the second factor are drawn as circles; and the elements in the product are drawn as stars. We identify matrices in $M_{2^n \times 2^n}(\mathbb{Z}_2)$ with maps $P[n] \times P[n] \rightarrow \mathbb{Z}_2$ using again the cardinality-lexicographic order on $\mathbb{Z}_2^n = P[n]$. We use juxtaposition for the product of matrices, and $\text{rank}(A)$ for the rank of matrix $A$.

2 MS Basis and the $\star$-Product

As mentioned in the introduction we are going to consider four different bases for the $\mathbb{Z}_2$-algebra $\text{BDO}_n$ of Boolean differential operators on $\mathbb{Z}_2^n$. In this section we consider the MS-basis

$$\{ m^c s^d \mid c, d \in P[n] \},$$

where the Boolean functions $m^c$ were described in the introduction, and the shift operators $s^d : \text{BF}_n \rightarrow \text{BF}_n$ are given by

$$s^d = \prod_{i \in d} s_i,$$

where $s_i f(a) = f(a + e_i)$, for $a \in \mathbb{Z}_2^n$, $i \in [n]$, $f \in \text{BF}_n$.

Note that $\partial_i = s_i + 1$ and $s_i = \partial_i + 1$, where 1 stands for the identity operator; thus one can move back and forward from the shift operators $s^d = \prod_{i \in d} s_i$ to the partial derivatives operators $\partial^d = \prod_{i \in d} \partial_i$. Indeed, it is easy to check that

$$\partial^d = \sum_{c \subseteq d} s^c \quad \text{and} \quad s^d = \sum_{c \subseteq d} \partial^c. \quad (3)$$

Consider the identifications

$$\text{DG}_{P[n]} \simeq \text{Map}(P[n] \times P[n], \mathbb{Z}_2) \simeq \text{BDO}_n,$$

where the identification on the left is given by characteristic functions and we use it freely without change of notation; the non-canonical identification on the right is obtained via the bijective $\mathbb{Z}_2$-linear map $l_1 : \text{DG}_{P[n]} \rightarrow \text{BDO}_n$ sending a directed graph $A \in \text{DG}_{P[n]}$ to the Boolean differential operator given by

$$l_1(A) = \sum_{(c, d) \in A} m^c s^d = \sum_{c, d \in P[n]} A(c, d) m^c s^d.$$
The $\star$-product on $\text{DG}_{P[n]}$ is the pullback via the map $l_1$ of the composition product on $\text{BDO}_n$. The $\star$-product, see [2], is given for $A, B \in \text{DG}_{P[n]}$ by the equivalent identities:

$$A \star B = l_1^{-1}(l_1(A)l_1(B));$$

$$A \star B(c, d) = \sum_{e \in P[n]} A(c, e)B(c+e, d+e); \quad (4)$$

$$A \star B = \{ (c, d) \in P[n] \times P[n] \mid O\{e \in P[n] \mid (c, e) \in A, \ (c+e, d+e) \in B\} \},$$

where the notation $OC$ means that the finite set $C$ has odd cardinality.

We proceed to introduce a matrix representation for the algebra $(\text{DG}_{P[n]}, \star)$. Consider the map $M_1 : \text{DG}_{P[n]} \longrightarrow M_{2^n \times 2^n}(\mathbb{Z}_2)$ sending a directed graph $A \in \text{DG}_{P[n]}$ to the matrix of the operator

$$l_1(A) = \sum_{c, d \in P[n]} A(c, d)m^cs^d$$

in the basis $\{m^a \mid a \in P[n]\}$, i.e. we have that

$$M_1(A) = [l_1(A)].$$

Note that $M_1$ is a $\mathbb{Z}_2$-linear map since it is the composition of two $\mathbb{Z}_2$-linear maps.

**Theorem 1.** The map $M_1 : (\text{DG}_{P[n]}, \star) \longrightarrow (M_{2^n \times 2^n}(\mathbb{Z}_2), \cdot)$ is an algebra isomorphism given for $A \in \text{DG}_{P[n]}$ by

$$M_1(A)_{a,b} = A(a, a + b). \quad (5)$$

The inverse map $D_1 : (M_{2^n \times 2^n}(\mathbb{Z}_2), \cdot) \longrightarrow (\text{DG}_{P[n]}, \star)$ sends a matrix $N \in M_{2^n \times 2^n}(\mathbb{Z}_2)$ to the directed graph $D_1(N)$ with characteristic function given by

$$D_1(N)(a, b) = N_{a, a+b}. \quad (6)$$

**Proof.** First note that $m^cs^d(m^b) = \delta(b, c + d)m^c$, where $\delta$ is the Kronecker delta function. Therefore the matrix $[m^cs^d] \in M_{2^n \times 2^n}(\mathbb{Z}_2)$ is such that:

$$[m^cs^d]_{a,b} = \delta(a, c)\delta(b, c + d). \quad (7)$$
Thus for $A \in \text{DG}_{P[\mathbb{Z}_2]}$ we have that:

$$M_1(A)_{a,b} = \left[ \sum_{c,d \in P[n]} A(c,d)m^c s^d \right]_{a,b} = \sum_{c,d \in P[n]} A(c,d)[m^c s^d]_{a,b} = \sum_{c,d \in P[n]} A(c,d)\delta(a,c)\delta(b,c + d) = A(a, a + b).$$

The maps $M_1$ and $D_1$ are inverse of each other, indeed we have that

$$D_1(M_1(A))(a,b) = M_1(A)_{a,a+b} = A(a, a + b) = A(a,b),$$
$$M_1(D_1(N))_{a,b} = D_1(N)(a, a + b) = N(a, a + b) = N(a,b)$$

for $A \in \text{DG}_{P[n]}$ and $N \in M_{2^n \times 2^n}(\mathbb{Z}_2)$.

Next we show that $M_1$ is an algebra morphism. Thus we have that:

$$M_1(A \star B) = [l_1(A \star B)] = [l_1(A)]l_1(B)) = [l_1(A)]l_1(B)) = M_1(A)M_1(B).$$

Explicitly, for $A, B \in \text{DG}_{P[n]}$, we have using (4) and (5) that:

$$M_1(A \star B)_{a_1,a_2} = A \star B(a_1, a_1 + a_2) =$$

$$\sum_{b \in P[n]} A(a_1, b)B(a_1 + b, a_1 + a_2 + b) = \sum_{b \in P[n]} M_1(A)(a_1, a_1 + b)M_1(B)(a_1 + b, a_2) =$$

$$\sum_{b \in P[n]} M_1(A)(a_1, b)M_1(B)(b, a_2) = (M_1(A)M_1(B))_{a_1,a_2}.$$

Corollary 2. $|\text{Ker}(l_1(A))| = 2^r$ and $|\text{Im}(l_1(A))| = 2^{n-r}$, where $r = \text{rank}(M_1(A))$.

Example 3. Consider the Jordan-like matrices $M_{2^n \times 2^n}(\mathbb{Z}_2)$ having ones on the principal diagonal and on the diagonal directly above the principal. The associated Boolean differential operators in the MS-basis, for $n \in [4]$, are given in Table 1.

Example 4. The multiplication table of $(\text{DG}_{P[1]}, \star)$ is given in Table 2.
Proof. Let \((A, B)\) where \(a, b, e\) are defined. Then we have that:

\[
\text{Lemma 5.} \quad \text{Proposition 6.}
\]

Table 1: Associated Boolean differential operators of Jordan-like matrices.

It would be nice to have an intuitive understanding of the \(*\)-product, say in the spirit of Venn diagrams. In order to gain a better understanding of the meaning of the \(*\)-product we consider several examples. The first example is the simple case of the product of graphs with a unique edge.

Lemma 5. Let \(a, b, c, d \in P[n]\), then we have that:

\[
\{(a, b)\} \ast \{(c, d)\} = \begin{cases} 
\{(a, b + d)\} & \text{if } a = b + c, \\
\emptyset & \text{if } a \neq b + c.
\end{cases}
\]

Proof. Let \((a_1, a_2) \in \{(a, b)\} \ast \{(c, d)\}\), then there is an odd number of sets \(e \in P[n]\) such that

\[
(a_1, e) = (a, b) \quad \text{and} \quad (a_1 + e, a_2 + e) = (c, d),
\]

Thus \(a_1 = a, e = b, a = b + c, a_2 = b + d\). So, there is no such \(e\) if \(a \neq b + c\). In the case \(a = b + c\), we have that \((a_1, a_2) = (a, b + d)\).

In the next examples we consider the \(*\)-product on graphs using suitable decompositions of the graphs.

Proposition 6. Let \(A, B \in DG_{P[n]}\) be given by

\[
A = \sum_{b \in P[n]} A_b \times \{b\} \quad \text{and} \quad B = \sum_{c \in P[n]} B_c \times \{c\},
\]

where \(A_b\) is the set endpoints of edges in \(A\) starting at \(b\), and \(B_c\) is similarly defined. Then we have that:

\[
A \ast B = \sum_{b, c \in P[n]} (A_b \cap (B_c + b)) \times \{b + c\}.
\]
Proof. Using the distributive property, recall that $(DG_{P[n]}, \star) \simeq (M_{2^n \times 2^n}(\mathbb{Z}_2), \cdot)$, we get

$$A \star B = \sum_{b,c \in P[n]} (A_b \times \{b\}) \star (B_c \times \{c\}).$$

Suppose $(a_1, a_2) \in (A_b \times \{b\}) \star (B_c \times \{c\})$, then there is an odd number of sets $e \in P[n]$ such that $(a_1, e) \in A_b \times \{b\}$ and $(a_1 + e, a_2 + e) \in B_c \times \{c\}$. Clearly, the only possible set $e$ with those properties is $e = b$, and furthermore $a_1 \in A_b$, $a_2 = b + c$, and $a_1 \in B_c + b$. Therefore, we have that:

$$(A_b \times \{b\}) \star (B_c \times \{c\}) = (A_b \cap (B_c + b)) \times \{b + c\},$$

yielding the desired result. \qed

Remark 7. To contrast the classical intersection $\cap$ with the $\star$-product note that the intersection of graphs $A, B \in DG_{P[n]}$ can be written as

$$A \cap B = \sum_{b \in P[n]} (A_b \cap B_b) \times \{b\} = \sum_{b,c \in P[n]} \delta(b, c) (A_b \cap B_b) \times \{b\}. $$

Example 8. Let $A_{\{1, 2\}} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}\} \in PP[4]$, then

$$(A_{\{1, 2\}} \times \{1, 2\}) \star (A_{\{1, 2\}} \times \{1, 2\}) = \{\{1\}, \{2\}\} \times \emptyset,$$

since $\{1, 2\} + \{1, 2\} = \emptyset$. $\{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}\}$ is equal to

$$\emptyset, \{1\}, \{2\}, \{2, 3\}, \{2, 3\}, \{1, 2, 4\}, \{1, 2, 4\}, \{1, 2, 4\}, \{1, 2, 4\},$$

and $\{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}\} \cap \emptyset = \emptyset$. Figure shows a graphical representation of the product $(A_{\{1, 2\}} \times \{1, 2\}) \star (A_{\{1, 2\}} \times \{1, 2\})$.

Proposition 9. Let $A, B \in DG_{P[n]}$ be written as

$$A = \sum_{b \in P[n]} A_b \times \{b\} \quad \text{and} \quad B = \sum_{c \in P[n]} \{c\} \times B_c.$$

Then we have that:

$$A \star B = \sum_{b+c \in A_b} \{b + c\} \times (B_c + b).$$
Figure 1: Representation of the product \((A_{1,2} \times \{1,2\}) \ast (A_{1,2} \times \{1,2\})\), Example 8.

Proof. Using the distributive property for the \(\ast\)-product we get:

\[
A \ast B = \sum_{b,c \in P[n]} (A_b \times \{b\}) \ast (\{c\} \times B_c) = \sum_{b+c \in A_b} \{b+c\} \times (B_c + b).
\]

We show the second identity. Suppose \((a_1, a_2) \in (A_b \times \{b\}) \ast (\{c\} \times B_c)\), then there is an odd number of sets \(e \in P[n]\) such that \((a_1, e) \in A_b \times \{b\}\) and \((a_1 + e, a_2 + e) \in \{c\} \times B_c\). Clearly, the only possibility is \(e = b\), and furthermore \(b + c = a_1 \in A_b\), \(a_2 \in B_c + b\). \(\square\)

Example 10. Let \(A_{1,2}\) and \(B_\emptyset\) in \(PP[4]\) be given, respectively, by

\[
A_{1,2} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}\}
\]

and

\[
B_\emptyset = \{\{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}\}.
\]

Then we have, see Figure 2, that:

\[
(A_{1,2} \times \{\{1,2\}\}) \ast (\emptyset \times B_\emptyset) = \{\{1,2\}\} \times \emptyset, \{\{2,3\}\}, \{\{2,4\}\}, \{\{1,2,3\}\}, \{\{1,2,4\}\}.
\]

Proposition 11. Let \(A, B \in DG_{P[n]}\) be written as

\[
A = \sum_{b \in P[n]} \{b\} \times A_b \quad \text{and} \quad B = \sum_{c \in P[n]} \{c\} \times B_c.
\]
Then we have that:

\[ A \star B = \sum_{b+c\in A_b} \{b\} \times (B_c + b + c). \]

**Proof.** Using the distributive property for the \( \star \)-product we have that:

\[ A \star B = \sum_{b,c\in P[n]} (\{b\} \times A_b) \star (\{c\} \times B_c). \]

A pair \((a_1, a_2)\in P[n] \times P[n]\) belongs to \((\{b\} \times A_b) \star (\{c\} \times B_c)\) if there is an odd number of sets \(e\in P[n]\) such that \((a_1, e)\in \{b\} \times A_b\) and \((a_1 + e, a_2 + e)\in \{c\} \times B_c\). Thus we have that \(a_1 = b, e \in A_b, e = b + c, a_2 \in B_c + b + c\). The desired result follows.

**Example 12.** Let \(B_{\{1,3\}}\) and \(A_\emptyset\) in \(PP[4]\) be given by

\[ A_\emptyset = \{\{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}\} \]

and

\[ B_{\{1,3\}} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}\}. \]
Then, see Figure 3, we have that:

$$((\emptyset \times A) \star (\{1, 3\} \times B_{(1,3)})) = \emptyset \times \{\{1\}, \{3\}, \{2, 3\}, \{1, 2, 3\}, \{1, 3, 4\}\}.$$ 

Example 13. Let $A, B \in \mathcal{DG}_{P[4]}$ be given by

$A = \{(\{4\}, \{4\}), (\{4\}, \{1, 2\}), (\{4\}, \{1, 3\}), (\{1, 2\}, \{4\}), (\{1, 2\}, \{1, 2\}),$

$$((\{1, 2\}, \{1, 3\}), (\{1, 3\}, \{4\}), (\{1, 3\}, \{1, 2\}), (\{1, 3\}, \{1, 3\})), \quad \text{and}$$

$B = \{(\{1, 3\}, \{1, 3\}), (\{1, 3\}, \{1, 4\}), (\{1, 3\}, \{2, 3\}), (\{1, 4\}, \{1, 3\}), (\{1, 4\}, \{1, 4\}),$

$((\{1, 4\}, \{2, 3\}), (\{2, 3\}, \{1, 3\}), (\{2, 3\}, \{1, 4\}), (\{2, 3\}, \{2, 3\}))}.$

The product $A \star B$, see Figure 4, is given by

$$\{(\{1, 2\}, \emptyset), (\{1, 2\}, \{1, 2\}), (\{1, 2\}, \{3, 4\}), (\{1, 3\}, \{1, 3\}), (\{1, 3\}, \{2, 3\}), (\{1, 3\}, \{2, 4\})\}.$$ 

3 M∂ Basis and ∗-Product

In this section we consider the $M\partial$ basis for $BDO_n$, thus we regard a directed graph $A \in \mathcal{DG}_{P[n]}$ as a Boolean differential operator via the map $l_2 : \mathcal{DG}_{P[n]} \rightarrow BDO_n$. 

11
Figure 4: Graphical representation of the product of the digraphs from Example 13.

given by
\[ l_2(A) = \sum_{(c,d) \in A} m^c \partial^d = \sum_{(c,d) \in P[n]} A(c,d) m^c \partial^d, \]
where for \( d \in P[n] \) we set \( \partial^d = \prod_{i \in d} \partial_i. \)

The \( \circ \)-product on \( DG_{P[n]} \) is the pullback via the map \( l_2 \) of the composition product on \( BDO_n \), i.e. the \( \circ \)-product is given for \( A, B \in DG_{P[n]} \) by \( A \circ B = l_2^{-1}(l_2(A)l_2(B)) \). Explicitly, see [2], we have that
\[ A \circ B(c,d) = \sum_{g \subseteq d, e; f \subseteq f \subseteq c} A(c,e)B(f,g). \]
Equivalently, a pair \((c,d) \in P[n] \times P[n]\) belongs to \( A \circ B \in DG_{P[n]} \) if and only if there is an odd number of sets \( e \in P[n] \) and \((f,g) \in B\) such that
\[ g \subseteq d, \quad (c,e) \in A, \quad d \setminus g \subseteq c + f \subseteq c. \]

Note that we can go back and forward from the MS-basis to the M\( \partial \)-basis for Boolean differential operators as follows:
\[ A = \sum_{c,d \in P[n]} A(c,d) m^c \partial^d = \sum_{c,d \in P[n]} \hat{A}(c,d) m^c s^d, \]
indeed with the help of the identities (3) we get that

\[
\hat{A}(c, d) = \sum_{d \subseteq e} A(c, e) \quad \text{and} \quad A(c, d) = \sum_{d \subseteq e} \hat{A}(c, e).
\]

Consider the map \( M_2 : \text{DG}_{P[n]} \rightarrow M_{2^n \times 2^n}(\mathbb{Z}_2) \) sending a directed graph \( A \in \text{DG}_{P[n]} \) to the matrix of the operator

\[
l_2(A) = \sum_{c, d \in P[n]} A(c, d) m^c \partial^d = \sum_{c, e \subseteq d} A(c, d) m^e s^e
\]

in the basis \( \{m^a \mid a \in P[n]\} \), i.e. we have that \( M_2(A) = [l_2(A)] \).

**Theorem 14.** The map \( M_2 : (\text{DG}_{P[n]}, \circ) \rightarrow (M_{2^n \times 2^n}(\mathbb{Z}_2), \cdot) \) is an algebra isomorphism given for \( A \in \text{DG}_{P[n]} \) by

\[
M_2(A)_{a, b} = \sum_{a+b \subseteq c} A(a, c).
\]

The inverse map \( D_2 : (M_{2^n \times 2^n}(\mathbb{Z}_2), \cdot) \rightarrow (\text{DG}_{P[n]}, \circ) \) sends \( N \in M_{2^n \times 2^n}(\mathbb{Z}_2) \) to the directed graph \( D_2(N) \) with characteristic function given by

\[
D_2(N)(a, b) = \sum_{b \subseteq c} N_{a, a+c}.
\]

**Proof.** For \( A \in \text{DG}_{P[n]} \), identifying \( A \) with \( l_2(A) \) and using (7), we get that

\[
M_2(A)_{a, b} = \left[ \sum_{c, d \in P[n]} A(c, d) m^c \partial^d \right]_{a, b} = \left[ \sum_{c, e \subseteq d} A(c, d) m^e s^e \right]_{a, b} = \sum_{c, e \subseteq d} A(c, d) [m^e s^e]_{a, b} = \sum_{c, e \subseteq d} A(c, d) \delta(a, c) \delta(b, c+e) = \sum_{a+b \subseteq d} A(a, d),
\]

since \( c = a \), and \( b = c + e \) implies that \( e = a + b \).

We show that \( D_2 \) is indeed the inverse of \( M_2 \). We have for \( A \in \text{DG}_{P[n]} \) that:

\[
D_2(M_2(A))(a, b) = \sum_{b \subseteq c} M_2(A)_{a, a+c} = \sum_{b \subseteq c} \left( \sum_{a+a+e \subseteq d} A(a, d) \right) = \sum_{b \subseteq c} A(a, d) = A(a, b),
\]
where the last identity is shown as follows:

\[ A(a, d) = \sum_{b \subseteq d} \left( \sum_{c \subseteq d} 1 \right) A(a, d) = \sum_{b \subseteq d} 2^{[d \setminus b]} A(a, d) = A(a, b). \]

\( M_2 \) is an algebra morphism since \( M_2(A) = [l_2(A)] \), and thus we have that:

\[ M_2(A \circ B) = [l_2(A \circ B)] = [l_2(A)][l_2(B)] = M_2(A)M_2(B). \]

\( \square \)

**Corollary 15.** \( |\text{Ker}(l_2(A))| = 2^r \) and \( |\text{Im}(l_2(A))| = 2^{n-r} \), where \( r = \text{rank}(M_2(A)) \).

### 4 XS-Basis and the \(*\)-Product

For \( a \in \mathbb{P}[n] \) consider the Boolean function \( x^a \in \mathbb{B} \mathbb{F}_n \) given on \( b \in \mathbb{P}[n] \) by:

\[ x^a(b) = \begin{cases} 1 & \text{if } a \subseteq b, \\ 0 & \text{otherwise}. \end{cases} \quad (8) \]

One can go back and forward from the \( \{m^a\} \) basis to the \( \{x^a\} \) basis as follows:

\[ m^a = \sum_{a \subseteq b} x^b \quad \text{and} \quad x^a = \sum_{a \subseteq b} m^b. \quad (9) \]

Indeed, the identity on the right follows directly from definitions (2) and (8); the identity on the left follows from the Möbius inversion formula for modules over a \( \mathbb{Z}_2 \)-ring, see [4], which states that for arbitrary maps

\[ f, g : \mathbb{P}[n] \to M, \]

with \( M \) a module over a \( \mathbb{Z}_2 \)-ring, the identities

\[ g(d) = \sum_{c \subseteq d} f(c) \quad \text{and} \quad f(d) = \sum_{c \subseteq d} g(c) \]

are equivalent.

Note that \( x + x = 2x = (1 + 1)x = 0x = 0 \) for all \( x \in M \). The Möbius inversion formula follows from the identities (valid for \( c \in \mathbb{P}[n] \) fixed):

\[ \sum_{a \subseteq b \subseteq c} f(a) = \sum_{a \subseteq c} \left( \sum_{b \subseteq c} 1 \right) f(a) = \sum_{a \subseteq c} 2^{[c \setminus a]} f(a) = f(c). \quad (10) \]
In this section we regard elements of $\text{DG}_P[n]$ as Boolean differential operators via the map $l_3 : \text{DG}_P[n] \to \text{BDO}_n$ given by

$$l_3(A) = \sum_{(c,d) \in A} x^c s^d = \sum_{c,d \in P[n]} A(c,d)x^c s^d.$$ 

The $*$-product on $\text{DG}_P[n]$ is the pullback via the map $l_3$ of the composition product on $\text{BDO}_n$, i.e. for $A, B \in \text{DG}_P[n]$ we have that $A * B = l_3^{-1}(l_3(A)l_3(B))$. Explicitly, see [2], we have that

$$A * B(c,d) = \sum_{e \subseteq c, g \cap h, e \cup h \setminus k = c} |\{k \subseteq g \cap h \mid e \cup h \setminus k = c\}| A(e,g)B(h,d + g).$$

Equivalently, a pair $(c,d) \in P[n] \times P[n]$ belongs to $A * B \in \text{DG}_P[n]$ if and only if there is an odd number of sets $e, g, h, k \in P[n]$ such that

$$e \subseteq c, \quad k \subseteq g \cap h, \quad e \cup h \setminus k = c, \quad (e,g) \in A, \quad (h,d + g) \in B.$$

Note that we can go back and forward from the MS-basis to the XS-basis for differential operators as follows:

$$A = \sum_{c,d \in P[n]} A(c,d)x^c s^d = \sum_{c,d \in P[n]} \hat{A}(c,d)m^c s^d,$$

indeed using (9) we have that

$$\hat{A}(c,d) = \sum_{e \subseteq c} A(e,d) \quad \text{and} \quad A(c,d) = \sum_{e \subseteq c} \hat{A}(e,d).$$

Consider the map $M_3 : \text{DG}_P[n] \to \text{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ sending a directed graph $A \in \text{DG}_P[n]$ to the matrix of the operator

$$l_3(A) = \sum_{c,d \in P[n]} A(c,d)x^c s^d = \sum_{c \subseteq e,d} A(c,d)m^c s^d$$

in the basis $\{m^a \mid a \in P[n]\}$, thus we have that $M_3(A) = l_3(A)$.

**Theorem 16.** The map $M_3 : (\text{DG}_P[n], *) \to (\text{M}_{2^n \times 2^n}(\mathbb{Z}_2), ?)$ is an algebra isomorphism given for $A \in \text{DG}_P[n]$ by

$$M_3(A)_{a,b} = \sum_{c \subseteq a} A(c, a + b).$$
The inverse map $D_3 : (M_{2^n \times 2^n}(\mathbb{Z}_2), .) \rightarrow (DG_{P[n]}, *)$ sends $N \in M_{2^n \times 2^n}(\mathbb{Z}_2)$ to the directed graph $D_3(N)$ with characteristic function given by

$$D_3(N)(a, b) = \sum_{c \subseteq a} N_{c:b+c}.$$ 

**Proof.** We have that

$$M_3(A)_{a,b} = \left[ \sum_{c,d \in P[n]} A(c,d)x^c s^d \right]_{a,b} = \left[ \sum_{c \subseteq e,d} A(c,d)\delta(e,a)\delta(e,b+e) \right]_{a,b} = \sum_{c \subseteq a} A(c,a+b).$$

The map $D_3$ is inverse to $M_3$ since for $A \in DG_{P[n]}$ we have that:

$$D_3(M_3(A))(a, b) = \sum_{c \subseteq a} M_3(A)_{c,b+c} \quad \text{and} \quad M_3(A \circ B) = \left[l_3(A)l_3(B)\right] = M_3(A)M_3(B).$$

**Corollary 17.** $|\text{Ker}(l_3(A))| = 2^r$ and $|\text{Im}(l_3(A))| = 2^{n-r}$, where $r = \text{rank}(M_3(A))$.

### 5 X∂-Basis and the •-Product

In this section we regard elements of $DG_{P[n]}$ as Boolean differential operators via the bijective map $l_4 : DG_{P[n]} \rightarrow \text{BDO}_n$ given by

$$l_4(A) = \sum_{(c,d) \in A} x^c \partial^d = \sum_{c,d \in P[n]} A(c,d)x^c \partial^d.$$ 

The •-product on $DG_{P[n]}$ is the pullback via $l_4$ of the composition product on $\text{BDO}_n$, thus for $A, B \in DG_{P[n]}$ we have that $A \circ B = l_4^{-1}(l_4(A)l_4(B))$. Explicitly we have that:

$$A \cdot B(c, d) = \sum_{e \subseteq c, h \subseteq d, f, g} \left| \{k_1 \subseteq k_2 \subseteq f \cap g \mid e \cup (g \setminus k_2) = c, f \setminus k_1 = d \setminus h\} \right| A(e, f)B(g, h).$$
Equivalently, a pair \((c, d) \in P[n] \times P[n]\) belongs to \(A \bullet B \in DG_{P[n]}\) if and only if there is an odd number of sets \((e, f) \in A, (g, h) \in B, k_1 \subseteq k_2 \subseteq [n]\) such that
\[
eq c, \quad h \subseteq d, \quad k_2 \subseteq f \cap g, \quad e \cup (g \setminus k_2) = c, \quad f \setminus k_1 = d \setminus h.
\]

Note that we can go back and forth from the MS-basis to the \(X\partial\)-basis for Boolean differential operators, using equations (3) and (9), as follows:

\[
A = \sum_{c,d \in P[n]} A(c, d) x^c \partial^d = \sum_{c,d \in P[n]} \widehat{A}(c, d) m^c s^d,
\]

where
\[
\widehat{A}(c, d) = \sum_{e \subseteq a, b \subseteq f} A(e, f) \quad \text{and} \quad A(c, d) = \sum_{e \subseteq a, b \subseteq f} \widehat{A}(e, f).
\]

Consider the map \(M_4 : DG_{P[n]} \rightarrow M_{2^n \times 2^n}(\mathbb{Z}_2)\) sending a directed graph \(A \in DG_{P[n]}\) to the matrix of the operator
\[
l_4(A) = \sum_{c,d \in P[n]} A(c, d) x^c \partial^d = \sum_{c \subseteq e, f \subseteq d} A(c, d) m^e s^f
\]
in the basis \(\{m^a \mid a \in P[n]\}\).

**Theorem 18.** The map \(M_4 : DG_{P[n]} \rightarrow M_{2^n \times 2^n}(\mathbb{Z}_2)\) defines an algebra isomorphism between \((DG_{P[n]}, \bullet)\) and \(M_{2^n \times 2^n}(\mathbb{Z}_2)\). Explicitly, for \(A \in DG_{P[n]}\) we have that:
\[
M_4(A)_{a,b} = \sum_{c \subseteq a, a+b \subseteq d} A(c, d).
\]

The inverse map \(D_4 : M_{2^n \times 2^n}(\mathbb{Z}_2) \rightarrow DG_{P[n]}\) sends \(N \in M_{2^n \times 2^n}(\mathbb{Z}_2)\) to the graph \(D_4(N) \in DG_{P[n]}\) with characteristic function given by:
\[
D_4(N)(a, b) = \sum_{c \subseteq a, b \subseteq d} N_{c, c+d}.
\]

**Proof.** Since \(x^e = \sum_{c \subseteq e} m^c\) and \(\partial^d = \sum_{f \subseteq d} s^f\), we have that
\[
M_4(A)_{a,b} = \left[ \sum_{c,d} A(c, d) x^c \partial^d \right]_{a,b} = \left[ \sum_{c \subseteq e, f \subseteq d} A(c, d) m^e s^f \right]_{a,b} = \left[ \sum_{c \subseteq e, f \subseteq d} A(c, d) m^e s^f \right]_{a,b} = \left[ \sum_{c \subseteq e, f \subseteq d} A(c, d) m^e s^f \right]_{a,b}.
\]
\[ \sum_{c \subseteq e, f \subseteq d} A(c, d)|m^{e,f}|_{a,b} = \sum_{c \subseteq e, f \subseteq d} A(c, d)\delta(e, a)\delta(e, f + b) = \sum_{c \subseteq a, a+b \subseteq d} A(c, d), \]
as \(e = a\), and \(e = f + b\) implies that \(f = a + b\).

The map \(D_4\) is inverse of \(M_4\) since applying (10) we have that:

\[ D_4(M_4(A))(a, b) = \sum_{c \subseteq a, b \subseteq d} M_4(A)_{c,c+d} = \]
\[ \sum_{e \subseteq c \subseteq a, b \subseteq c+c+d \subseteq f} A(e, f) = \sum_{e \subseteq c \subseteq a, b \subseteq d \subseteq f} A(e, f) = A(a, b). \]
The map \(M_4(A) = [l_4(A)]\) is an algebra morphism since:

\[ M_4(A \bullet B) = [l_4(A \bullet B)] = [l_4(A)(l_4(B))] = [l_4(A)][l_4(B)] = M_4(A)M_4(B). \]

**Corollary 19.** \(|\ker(l_4(A))| = 2^r\) and \(|\im(l_4(A))| = 2^{n-r}\), where \(r = \rank(M_4(A))\).

### 6 Final Comments

In this work we considered four combinatorial interpretations using directed graphs for the composition (together with the symmetric difference) of Boolean differential operators, and provided a matrix representation for each of these interpretations. Therefore our work provides set theoretical interpretations for the algebra of Boolean differential operators. It would be nice to find logical interpretations as well, i.e. some sort of non-commutative logic where Boolean differential operators play the role played by Boolean functions in classical propositional logic. Partial results along this line are developed in [2], where a couple of explicit presentations by generators and relations of the algebra of Boolean differential operators are provided.

We thank an anonymous referee for many valuable suggestions.

**References**

[1] F. Brown, Boolean Reasoning, Dover Publications, Mineola, 2003.
[2] R. Díaz, Quantum Boolean Algebras, preprint, http://arxiv.org/abs/1011.5215.

[3] I. Reed, A class of multiple error-correcting codes and decoding scheme, IRE Trans. on Information Theory 4 (1954) 38-49.

[4] G.-C. Rota, Gian-Carlo Rota on Combinatorics, J. Kung (Ed.), Birkhäuser, Boston and Basel, 1995.

jorgerev90@gmail.com
Departamento de Matemáticas
Universidad Nacional de Colombia, Manizales, Colombia

ragadiaz@gmail.com
Instituto de Matemáticas y sus Aplicaciones
Universidad Sergio Arboleda, Bogotá, Colombia
|   | 0 | (11, 0) | (10, 1) | (0, 0) |
|---|---|---------|---------|-------|
| 0 | 0 | 0       | 0       | 0     |
| 1 | 0 | 0       | 0       | 0     |
| (0, 1) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (1, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |
| (0, 0) | 0 | (11, 0) | (10, 1) | (0, 0) |

Table 2: Multiplication table for \((D_{2P}, \cdot)\).