Boolean differential operators

Jorge Catumba, 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

Classification: 05E15, 05C76, 03G05

1. Introduction

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

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

$$\partial_i f(a) = f(a + e_i) + f(a), \tag{1}$$

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 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. BDO_n is the subalgebra of $\mathrm{End}_{\mathbb{Z}_2}(\mathrm{BF}_n)$ generated by the operators of multiplication by Boolean functions, and the partial derivative operators ∂_i defined in (1).

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

$$A : \mathrm{BF}_n \longrightarrow \mathrm{BF}_n \quad \text{such that} \quad A(f + g) = A(f) + A(g), \quad \text{for} \quad f, g \in \mathrm{BF}_n.$$

We are interested in finding a suitable set theoretical interpretation for the algebras BDO_n that extends the above mentioned interpretation of BF_n as the Boolean algebra $\mathrm{PP}[n]$, and may shed a light towards a logical understanding of the $\mathbb{Z}_2$-algebras BDO_n. Indeed, we believe that the $\mathbb{Z}_2$-algebras 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 BDO_n. By dimension counting $\mathrm{BDO}_n = \mathrm{End}_{\mathbb{Z}_2}(\mathrm{BF}_n)$ is non-canonically isomorphic to the $\mathbb{Z}_2$-algebra $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ of square matrices of size 2^n with 0-1 entries. Note that $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ may be identified, via characteristic functions, with $\mathrm{P}(\mathrm{P}[n]\times\mathrm{P}[n])$ the set of subsets of $\mathrm{P}[n]\times\mathrm{P}[n]$, or equivalently, with the set $\mathrm{DG}_{\mathrm{P}[n]}$ of simple directed graphs (possibly with loops) with vertex set $\mathrm{P}[n]$. A matrix $A\in\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)=\mathrm{P}(\mathrm{P}[n]\times\mathrm{P}[n])$ is regarded as a directed graph with vertex set $\mathrm{P}[n]$ by drawing an edge from $b\in\mathrm{P}[n]$ to $a\in\mathrm{P}[n]$ if and only if $(a,b)\in A$. The sum and product of matrices in $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ induce operations of sum and product of digraphs in $\mathrm{DG}_{\mathrm{P}[n]}$. The sum on $\mathrm{DG}_{\mathrm{P}[n]}$ is the symmetric difference. The product AB of digraphs $A,B\in\mathrm{DG}_{\mathrm{P}[n]}$ is such that the pair $(a,b)\in AB$ if and only if there is an odd number of sets $c\in\mathrm{P}[n]$ such that $(a,c)\in A$ and $(c,b)\in B$.

To define an explicit isomorphism $\mathrm{BDO}_n\simeq\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ a choice of basis for BF_n must be made. In this work we only consider the basis $\{m^a \mid a\in\mathrm{P}[n]\}$ for BF_n, where the Boolean function $m^a:\mathbb{Z}_2^n\longrightarrow\mathbb{Z}_2$ is given on $b\in\mathrm{P}[n]$ by:

$$m^a(b)=\begin{cases}1 & \text{if } a=b,\\ 0 & \text{otherwise.}\end{cases} \tag{2}$$

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

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 $l:V\longrightarrow A$ 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 BDO_n induces a $\mathbb{Z}_2$-linear bijective map from $\mathrm{DG}_{\mathrm{P}[n]}$ to BDO_n. In [2] we use four such bijections to pullback the composition product on BDO_n to $\mathrm{DG}_{\mathrm{P}[n]}$, thus we obtain four products on $\mathrm{DG}_{\mathrm{P}[n]}$ denoted, respectively, by $\star$, $\circ$, $\bullet$, $\ast$. Having various presentations for the product on 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 $\star$, $\circ$, $\bullet$, $*$ on $\mathrm{DG}_{\mathrm{P}[n]}$. It turns out that the product $\star$ is the easiest to handle, in Section 2 we discuss some of its basic properties and describe an explicit isomorphism with $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$. In the remaining sections, we present explicit isomorphisms between the products $\circ$, $\bullet$, $*$ and the product on $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$, 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 $\mathrm{P}[n]\times\mathrm{P}[n]$ as a subset of the real plane, and we use the bijective correspondence between $\mathrm{P}[n]=\mathbb{Z}_2^n$ and the natural numbers in the interval $[0,2^n-1]$ resulting in ordering $\mathrm{P}[n]$ by cardinality and lexicographic order within a given cardinality. For example $\mathrm{P}[2]$ 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 $\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ with maps $\mathrm{P}[n]\times\mathrm{P}[n]\longrightarrow\mathbb{Z}_2$ using again the cardinality-lexicographic order on $\mathbb{Z}_2^n=\mathrm{P}[n]$. We use juxtaposition for the product of matrices, and $\mathrm{rank}(A)$ 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 BDO_n of Boolean differential operators on $\mathbb{Z}_2^n$. In this section we consider the MS-basis

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

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

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

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 derivative operators $\partial^d=\prod_{i\in d}\partial_i$. Indeed, it is easy to check that

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

Consider the identifications

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

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 $l_1:\mathrm{DG}_{\mathrm{P}[n]}\rightarrow\mathrm{BDO}_n$ sending a directed graph $A \in \mathrm{DG}_{\mathrm{P}[n]}$ to the Boolean differential operator given by

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

The $\star$-product on $\mathrm{DG}_{\mathrm{P}[n]}$ is the pullback via the map l_1 of the composition product on BDO_n. The $\star$-product, see [2], is given for $A, B \in \mathrm{DG}_{\mathrm{P}[n]}$ by the equivalent identities:

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

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

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

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

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

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

in the basis $\{m^a \mid a \in \mathrm{P}[n]\}$, 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 $M_1 : (\mathrm{DG}_{\mathrm{P}[n]}, \star) \longrightarrow (\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2), \cdot)$ is an algebra isomorphism given for $A \in \mathrm{DG}_{\mathrm{P}[n]}$ by*

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

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

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

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

$$[m^c s^d]_{a,b} = \delta(a,c)\delta(b, c+d). \tag{7}$$

Thus for $A \in \mathrm{DG}_{\mathrm{P}[n]}$ we have that:

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

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

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

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

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

$$\begin{aligned} M_1(A \star B)_{a_1,a_2} &= A \star B(a_1, a_1 + a_2) \\ &= \sum_{b \in \mathrm{P}[n]} A(a_1, b) B(a_1 + b, a_1 + a_2 + b) \\ &= \sum_{b \in \mathrm{P}[n]} M_1(A)(a_1, a_1 + b) M_1(B)(a_1 + b, a_2) \\ &= \sum_{b \in \mathrm{P}[n]} M_1(A)(a_1, b) M_1(B)(b, a_2) = \left(M_1(A) M_1(B)\right)_{a_1,a_2}. \end{aligned}$$

□

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

Example 3. Consider the Jordan-like matrices $\mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ having 1 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 $(\mathrm{DG}_{\mathrm{P}[1]}, \star)$ is given in Table 2.

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

Lemma 5. *Let* $a, b, c, d \in \mathrm{P}[n]$, *then we have that:*

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

n	Operator
1	$m^{\emptyset}s^{\{1\}}+1$
2	$m^{\emptyset}s^{\{1\}}+m^{\{1\}}s^{\{1,2\}}+m^{\{2\}}s^{\{1\}}+1$
3	$m^{\emptyset}s^{\{1\}}+m^{\{1\}}s^{\{1,2\}}+m^{\{2\}}s^{\{2,3\}}+m^{\{3\}}s^{\{1,2,3\}}+m^{\{1,2\}}s^{\{2,3\}}+m^{\{1,3\}}s^{\{1,2\}}+m^{\{2,3\}}s^{\{1\}}+1$
4	$m^{\emptyset}s^{\{1\}}+m^{\{1\}}s^{\{1,2\}}+m^{\{2\}}s^{\{2,3\}}+m^{\{3\}}s^{\{3,4\}}+m^{\{4\}}s^{\{1,2,4\}}+m^{\{1,2\}}s^{\{2,3\}}+m^{\{1,3\}}s^{\{3,4\}}+m^{\{1,4\}}s^{\{1,2,3,4\}}+m^{\{2,3\}}s^{\{3,4\}}+m^{\{2,4\}}s^{\{2,3\}}+m^{\{3,4\}}s^{\{1,2,4\}}+m^{\{1,2,3\}}s^{\{3,4\}}+m^{\{1,2,4\}}s^{\{2,3\}}+m^{\{1,3,4\}}s^{\{1,2\}}+m^{\{2,3,4\}}s^{\{1\}}+1$

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

Proof: Let $(a_1,a_2)\in\{(a,b)\}\star\{(c,d)\}$, then there is an odd number of sets $e\in \mathrm{P}[n]$ 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 $\star$-product on graphs using suitable decompositions of the graphs.

Proposition 6. *Let $A,B\in \mathrm{DG}_{\mathrm{P}[n]}$ be given by*

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

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

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

Proof: Using the distributive property, recall that $(\mathrm{DG}_{\mathrm{P}[n]},\star)\simeq(\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2),\cdot)$, we get

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

Suppose $(a_1,a_2)\in(A_b\times\{b\})\star(B_c\times\{c\})$, then there is an odd number of sets $e\in\mathrm{P}[n]$ 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. □

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

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

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

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

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

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

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

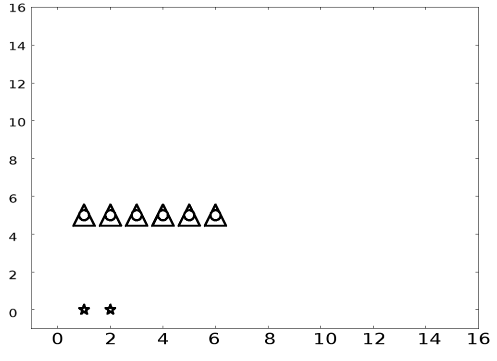

FIGURE 1. Representation of the product $(A_{\{1,2\}} \times \{1,2\}) \star (A_{\{1,2\}} \times \{1,2\})$, Example 8.

Proposition 9. *Let $A, B \in \mathrm{DG}_{\mathrm{P}[n]}$ be written as*

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

Then we have that:

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

PROOF: Using the distributive property for the $\star$-product we get:

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

We show the second identity. Suppose $(a_1, a_2) \in (A_b \times \{b\}) \star (\{c\} \times B_c)$, then there is an odd number of sets $e \in \mathrm{P}[n]$ 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 $\mathrm{PP}[4]$ 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:

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

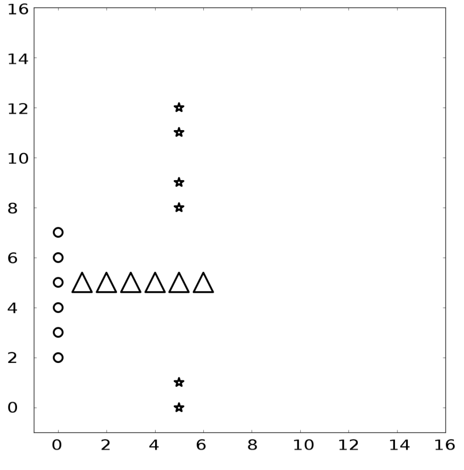

FIGURE 2. Representation of the product $(A_{\{1,2\}} \times \{1,2\}) \star (\emptyset \times B_\emptyset)$ from Example 10.

Proposition 11. *Let $A, B \in \mathrm{DG}_{\mathrm{P}[n]}$ be written as*

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

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:

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

A pair $(a_1, a_2) \in \mathrm{P}[n] \times \mathrm{P}[n]$ belongs to $(\{b\} \times A_b) \star (\{c\} \times B_c)$ if there is an odd number of sets $e \in \mathrm{P}[n]$ 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:

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

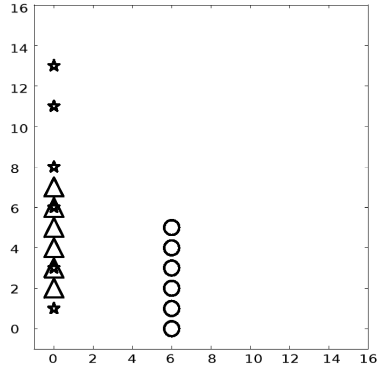

FIGURE 3. Representation of the product $(\{\emptyset\} \times A_\emptyset) \star (\{\{1,3\}\} \times B_{\{1,3\}})$, Example 12.

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

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

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

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

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

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

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

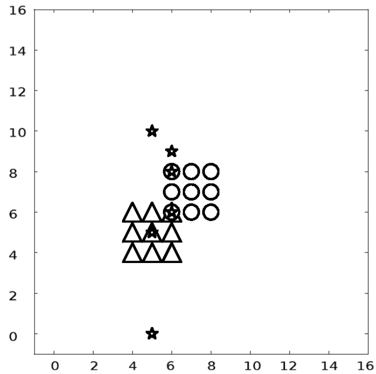

FIGURE 4. Graphical representation of the product of the digraphs from Example 13.

3. M∂ basis and $\circ$-product

In this section we consider the M∂ basis for BDO_n, thus we regard a directed graph $A\in \mathrm{DG}_{\mathrm{P}[n]}$ as a Boolean differential operator via the map $l_2:\mathrm{DG}_{\mathrm{P}[n]}\longrightarrow \mathrm{BDO}_n$ given by

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

where for $d\in \mathrm{P}[n]$ we set $\partial^d=\prod_{i\in d}\partial_i$.

The $\circ$-product on $\mathrm{DG}_{\mathrm{P}[n]}$ is the pullback via the map l_2 of the composition product on BDO_n, i.e. the $\circ$-product is given for $A,B\in \mathrm{DG}_{\mathrm{P}[n]}$ by $A\circ B = l_2^{-1}(l_2(A)l_2(B))$. Explicitly, see [2], we have that

$$A\circ B(c,d)=\sum_{\substack{g\subseteq d,e,f\\ d\setminus g\subseteq c+f\subseteq e}} A(c,e)B(f,g).$$

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

$$g \subseteq d, \quad (c,e) \in A, \quad d \setminus g \subseteq c+f \subseteq e.$$

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

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

indeed with the help of the identities (3) we get that

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

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

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

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

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

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

The inverse map $D_2 : (\mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2), \cdot) \longrightarrow (\mathrm{DG}_{\mathrm{P}[n]}, \circ)$ *sends* $N \in \mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ *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 $A \in \mathrm{DG}_{\mathrm{P}[n]}$, identifying A with $l_2(A)$ and using (7), we get that

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

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 $A \in \mathrm{DG}_{\mathrm{P}[n]}$ that:

$$\begin{aligned} D_2(M_2(A))(a,b) &= \sum_{b\subseteq c} M_2(A)_{a,a+c} \\ &= \sum_{b\subseteq c}\left(\sum_{a+a+c\subseteq d} A(a,d)\right) = \sum_{b\subseteq c\subseteq d} A(a,d) = A(a,b), \end{aligned}$$

where the last identity is shown as follows:

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

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

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

□

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

4. XS-basis and the $*$-product

For $a \in \mathrm{P}[n]$ consider the Boolean function $x^a \in \mathrm{BF}_n$ given on $b \in \mathrm{P}[n]$ by:

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

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

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

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

$$f, g : \mathrm{P}[n] \longrightarrow M,$$

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

$$g(d) = \sum_{c\subseteq d} f(c) \quad \text{and} \quad f(d) = \sum_{c\subseteq d} g(c) \quad \text{are equivalent.}$$

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 $c\in \mathrm{P}[n]$ fixed):

$$\sum_{a\subseteq b\subseteq c} f(a)=\sum_{a\subseteq c}\left(\sum_{a\subseteq b\subseteq c} 1\right) f(a)=\sum_{a\subseteq c} 2^{|c\setminus a|} f(a)=f(c). \tag{10}$$

In this section we regard elements of $\mathrm{DG}_{\mathrm{P}[n]}$ as Boolean differential operators via the map $l_3:\mathrm{DG}_{\mathrm{P}[n]}\to \mathrm{BDO}_n$ given by

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

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

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

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

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

Indeed using (9) we have that

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

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

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

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

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

$$M_3(A)_{a,b} = \sum_{c\subseteq a} A(c, a+b).$$

The inverse map $D_3 : (\mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2), \cdot) \longrightarrow (\mathrm{DG}_{\mathrm{P}[n]}, *)$ *sends* $N \in \mathrm{M}_{2^n\times 2^n}(\mathbb{Z}_2)$ *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

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

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

$$\begin{aligned} D_3(M_3(A))(a,b) &= \sum_{c\subseteq a} M_3(A)_{c,b+c} \\ &= \sum_{c\subseteq a}\left(\sum_{d\subseteq c} A(d,b)\right) = \sum_{d\subseteq c\subseteq a} A(d,b) = A(a,b). \end{aligned}$$

We show that M_3 is an algebra morphism. By definition $M_3(A) = [l_3(A)]$, thus:

$$M_3(A\circ B) = [l_3(A\circ B)] = [l_3(A)l_3(B)] = [l_3(A)][l_3(B)] = M_3(A)M_3(B).$$

$\square$

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

5. X∂-basis and the $\bullet$-product

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

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

The $\bullet$-product on $\mathrm{DG}_{\mathrm{P}[n]}$ is the pullback via l_4 of the composition product on BDO_n, thus for $A, B \in \mathrm{DG}_{\mathrm{P}[n]}$ we have that $A \circ B = l_4^{-1}(l_4(A)l_4(B))$. Explicitly [2] we have that:

$$A \bullet B(c,d) = \sum_{e \subseteq c, h \subseteq d, f, g} |\{k_1 \subseteq k_2 \subseteq f \cap g \mid e \cup (g \setminus k_2) = c, f \setminus k_1 = d \setminus h\}| \, A(e,f)B(g,h).$$

Equivalently, a pair $(c,d) \in \mathrm{P}[n] \times \mathrm{P}[n]$ belongs to $A \bullet B \in \mathrm{DG}_{\mathrm{P}[n]}$ 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

$$e \subseteq c, \quad h \subseteq d, \quad k_2 \subseteq f \cap g, \quad e \cup (g \setminus k_2) = c, \quad f \setminus k_1 = d \setminus h.$$

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

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

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 $M_4 : \mathrm{DG}_{\mathrm{P}[n]} \longrightarrow \mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ sending a directed graph $A \in \mathrm{DG}_{\mathrm{P}[n]}$ to the matrix of the operator

$$l_4(A) = \sum_{c,d \in \mathrm{P}[n]} A(c,d) x^c \partial^d = \sum_{c \subseteq e,\ f \subseteq d} A(c,d) m^e s^f$$

in the basis $\{m^a \mid a \in \mathrm{P}[n]\}$.

Theorem 18. *The map $M_4 : \mathrm{DG}_{\mathrm{P}[n]} \longrightarrow \mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ defines an algebra isomorphism between $(\mathrm{DG}_{\mathrm{P}[n]}, \bullet)$ and $\mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$. Explicitly, for $A \in \mathrm{DG}_{\mathrm{P}[n]}$ we have that:*

$$M_4(A)_{a,b} = \sum_{c \subseteq a,\ a+b \subseteq d} A(c,d).$$

The inverse map $D_4 : \mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2) \longrightarrow \mathrm{DG}_{\mathrm{P}[n]}$ sends $N \in \mathrm{M}_{2^n \times 2^n}(\mathbb{Z}_2)$ to the graph $D_4(N) \in \mathrm{DG}_{\mathrm{P}[n]}$ with characteristic function given by:

$$D_4(N)(a,b) = \sum_{c \subseteq a,\ b \subseteq d} N_{c,c+d}.$$

Proof: Since $x^c = \sum_{c\subseteq e} m^e$ and $\partial^d = \sum_{f\subseteq d} s^f$, we have that

$$\begin{aligned} M_4(A)_{a,b} &= \left[\sum_{c,d} A(c,d)x^c\partial^d\right]_{a,b} = \left[\sum_{c\subseteq e,\ f\subseteq d} A(c,d)m^e s^f\right]_{a,b} \\ &= \sum_{c\subseteq e,\ f\subseteq d} A(c,d)[m^e s^f]_{a,b} = \sum_{c\subseteq e,\ f\subseteq d} A(c,d)\delta(e,a)\delta(e,f+b) \\ &= \sum_{c\subseteq a,\ a+b\subseteq d} A(c,d), \end{aligned}$$

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:

$$\begin{aligned} D_4(M_4(A))(a,b) &= \sum_{c\subseteq a,\ b\subseteq d} M_4(A)_{c,c+d} \\ &= \sum_{e\subseteq c\subseteq a,\ b\subseteq c+c+d\subseteq f} A(e,f) = \sum_{e\subseteq c\subseteq a,\ b\subseteq d\subseteq f} A(e,f) = A(a,b). \end{aligned}$$

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. $|\mathrm{Ker}(l_4(A))| = 2^r$ *and* $|\mathrm{Im}(l_4(A))| = 2^{n-r}$, *where* $r = \mathrm{rank}(M_4(A))$.

6. Final comments

In this work we considered four combinatorial interpretations for the composition (together with the symmetric difference) of Boolean differential operators using directed graphs, 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.

Acknowledgments. We thank an anonymous referee for many valuable suggestions.

References

[1] Brown F., *Boolean Reasoning*, Dover Publications, Mineola, 2003.
[2] Díaz R., *Quantum Boolean algebras*, preprint, http://arxiv.org/abs/1011.5215.
[3] Reed I., *A class of multiple error-correcting codes and decoding scheme*, IRE Trans. on Information Theory **4** (1954), 38–49.
[4] Rota G.-C., *Gian-Carlo Rota on Combinatorics*, J. Kung (Ed.), Birkhäuser, Boston and Basel, 1995.

Departamento de Matemáticas, Universidad Nacional de Colombia, Manizales, Colombia

E-mail: jorgerev90@gmail.com

Instituto de Matemáticas y sus Aplicaciones, Universidad Sergio Arboleda, Bogotá, Colombia

E-mail: ragadiaz@gmail.com

(*Received* December 15, 2012*, revised* November 12, 2013)

$\star$	0	{(1, 0)}	{(0, 1)}	{(0, 0)}
0	0	0	0	0
{(1, 0)}	0	{(1, 0)}	0	0
{(0, 1)}	0	{(0, 1)}	0	0
{(0, 0)}	0	0	{(0, 1)}	{(0, 0)}
{(1, 1)}	0	0	{(1, 0)}	{(1, 1)}
{(1, 0), (0, 1)}	0	{(1, 0), (0, 1)}	0	0
{(1, 0), (0, 0)}	0	{(1, 0)}	{(0, 1)}	{(0, 0)}
{(1, 0), (1, 1)}	0	{(1, 0)}	{(1, 0)}	{(1, 1)}
{(0, 1), (0, 0)}	0	{(0, 1)}	{(0, 1)}	{(0, 0)}
{(0, 1), (1, 1)}	0	{(0, 1)}	{(1, 0)}	{(1, 1)}
{(0, 0), (1, 1)}	0	0	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0)}	0	{(1, 0), (0, 1)}	{(0, 1)}	{(0, 0)}
{(1, 0), (0, 1), (1, 1)}	0	{(1, 0), (0, 1)}	{(1, 0)}	{(1, 1)}
{(1, 0), (0, 0), (1, 1)}	0	{(1, 0)}	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}
{(0, 1), (0, 0), (1, 1)}	0	{(0, 1)}	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0), (1, 1)}	0	{(1, 0), (0, 1)}	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}

$\star$	{(1, 1)}	{(1, 0), (0, 1)}	{(1, 0), (0, 0)}	{(1, 0), (1, 1)}
0	0	0	0	0
{(1, 0)}	{(1, 1)}	{(1, 0)}	{(1, 0)}	{(1, 0), (1, 1)}
{(0, 1)}	{(0, 0)}	{(0, 1)}	{(0, 1)}	{(0, 1), (0, 0)}
{(0, 0)}	0	{(0, 1)}	{(0, 0)}	0
{(1, 1)}	0	{(1, 0)}	{(1, 1)}	0
{(1, 0), (0, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1)}	{(1, 0), (0, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 0)}	{(1, 1)}	{(1, 0), (0, 1)}	{(1, 0), (0, 0)}	{(1, 0), (1, 1)}
{(1, 0), (1, 1)}	{(1, 1)}	0	{(1, 0), (1, 1)}	{(1, 0), (1, 1)}
{(0, 1), (0, 0)}	{(0, 0)}	0	{(0, 1), (0, 0)}	{(0, 1), (0, 0)}
{(0, 1), (1, 1)}	{(0, 0)}	{(1, 0), (0, 1)}	{(0, 1), (1, 1)}	{(0, 1), (0, 0)}
{(0, 0), (1, 1)}	0	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}	0
{(1, 0), (0, 1), (0, 0)}	{(0, 0), (1, 1)}	{(1, 0)}	{(1, 0), (0, 1), (0, 0)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 1), (1, 1)}	{(0, 0), (1, 1)}	{(0, 1)}	{(1, 0), (0, 1), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 0), (1, 1)}	{(1, 1)}	{(0, 1)}	{(1, 0), (0, 0), (1, 1)}	{(1, 0), (1, 1)}
{(0, 1), (0, 0), (1, 1)}	{(0, 0)}	{(1, 0)}	{(0, 1), (0, 0), (1, 1)}	{(0, 1), (0, 0)}
{(1, 0), (0, 1), (0, 0), (1, 1)}	{(0, 0), (1, 1)}	0	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}

$\star$	{(0, 1), (0, 0)}	{(0, 1), (1, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0)}
0	0	0	0	0
{(1, 0)}	0	{(1, 1)}	{(1, 1)}	{(1, 0)}
{(0, 1)}	0	{(0, 0)}	{(0, 0)}	{(0, 1)}
{(0, 0)}	{(0, 1), (0, 0)}	{(0, 1)}	{(0, 0)}	{(0, 1), (0, 0)}
{(1, 1)}	{(1, 0), (1, 1)}	{(1, 0)}	{(1, 1)}	{(1, 0), (1, 1)}
{(1, 0), (0, 1)}	0	{(0, 0), (1, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1)}
{(1, 0), (0, 0)}	{(0, 1), (0, 0)}	{(0, 1), (1, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0)}
{(1, 0), (1, 1)}	{(1, 0), (1, 1)}	{(1, 0), (1, 1)}	0	{(1, 1)}
{(0, 1), (0, 0)}	{(0, 1), (0, 0)}	{(0, 1), (0, 0)}	0	{(0, 0)}
{(0, 1), (1, 1)}	{(1, 0), (1, 1)}	{(1, 0), (0, 0)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (1, 1)}
{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0)}	{(0, 1), (0, 0)}	{(0, 1), (0, 0), (1, 1)}	{(1, 1)}	{(1, 0), (0, 0)}
{(1, 0), (0, 1), (1, 1)}	{(1, 0), (1, 1)}	{(1, 0), (0, 0), (1, 1)}	{(0, 0)}	{(0, 1), (1, 1)}
{(1, 0), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (1, 1)}	{(0, 0)}	{(0, 1), (0, 0), (1, 1)}
{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0)}	{(1, 1)}	{(1, 0), (0, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	0	{(0, 0), (1, 1)}

$\star$	{(1, 0), (0, 1), (1, 1)}	{(1, 0), (0, 0), (1, 1)}	{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
0	0	0	0	0
{(1, 0)}	{(1, 0), (1, 1)}	{(1, 0), (1, 1)}	{(1, 1)}	{(1, 0), (1, 1)}
{(0, 1)}	{(0, 1), (0, 0)}	{(0, 1), (0, 0)}	{(0, 0)}	{(0, 1), (0, 0)}
{(0, 0)}	{(0, 1)}	{(0, 0)}	{(0, 1), (0, 0)}	{(0, 1), (0, 0)}
{(1, 1)}	{(1, 0)}	{(1, 1)}	{(1, 0), (1, 1)}	{(1, 0), (1, 1)}
{(1, 0), (0, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 0)}	{(1, 0), (0, 1), (1, 1)}	{(1, 0), (0, 0), (1, 1)}	{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (1, 1)}	{(1, 1)}	{(1, 0)}	{(1, 0)}	0
{(0, 1), (0, 0)}	{(0, 0)}	{(0, 1)}	{(0, 1)}	0
{(0, 1), (1, 1)}	{(1, 0), (0, 1), (0, 0)}	{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(0, 0), (1, 1)}	{(1, 0), (0, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0)}	{(1, 0), (0, 0), (1, 1)}	{(1, 0), (0, 1), (1, 1)}	{(0, 1), (1, 1)}	{(1, 0), (1, 1)}
{(1, 0), (0, 1), (1, 1)}	{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 1), (0, 0)}	{(1, 0), (0, 0)}	{(0, 1), (0, 0)}
{(1, 0), (0, 0), (1, 1)}	{(0, 1), (1, 1)}	{(1, 0), (0, 0)}	{(1, 0), (0, 1), (0, 0)}	{(0, 1), (0, 0)}
{(0, 1), (0, 0), (1, 1)}	{(1, 0), (0, 0)}	{(0, 1), (1, 1)}	{(1, 0), (0, 1), (1, 1)}	{(1, 0), (1, 1)}
{(1, 0), (0, 1), (0, 0), (1, 1)}	{(0, 0), (1, 1)}	{(1, 0), (0, 1)}	{(1, 0), (0, 1)}	0

TABLE 2. Multiplication table for $(\mathrm{DG}_{\mathrm{P}[1]}, \star)$.