Quantum Boolean Algebras

Rafael Díaz

Abstract

We introduce quantum Boolean algebras which are the analogue of the Weyl algebras for Boolean affine spaces. We study quantum Boolean algebras from the logical and set theoretical viewpoints.

1 Introduction

After Stone [17] and Zhegalkin [19], Boole's main contribution to science [3] can be understood as the realization that the mathematics of logical phenomena is controlled – to a large extend – by the field $\mathbb{Z}_2 = \{0, 1\}$ with two elements; in contrast the mathematics of classical physical phenomena is controlled – to a large extend – by the field $\mathbb{R}$ of real numbers. The switch from $\mathbb{Z}_2$ to $\mathbb{R}$ corresponds with a deep ontological jump from logical to physical phenomena. The switch from $\mathbb{R}$ to $\mathbb{C}$ corresponds to the jump from classical to quantum physics.

What makes the logic/physics jump possible is the fact that $\mathbb{Z}_2$ may be regarded as an object of two different categories. On the one hand, it is a field $(\mathbb{Z}_2, +, .)$ with sum and product defined by making 0 the neutral element and 1 the product unit. On the other hand, it is a set of truth values with 0 and 1 representing falsity and truth, respectively. Indeed, $(\mathbb{Z}_2, \vee, \wedge, \overline{(\ )})$ is a Boolean algebra: a complemented distributive lattice with minimum 0 and maximum 1. The operations $\vee, \wedge$, and $\overline{(\ )}$ correspond with the logical connectives OR, AND, and NOT. The two viewpoints are related by the identities: $a \vee b = a + b + ab$, $a \wedge b = ab$, $\overline{a} = a + 1$. These identities, together with the inverse relation $a + b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$, allow us to switch back and forth from the algebraic to the logical viewpoint.

By and large, the logical and algebraic viewpoints have remained separated. In this work, in order to explore quantum-like phenomena in characteristic 2, we place ourselves at the jump. Our algebraic viewpoint is, in a sense, complementary to the quantum logic approach initiated by Birkhoff and von Neumann [1]. For example, while the meet in quantum logic is a commutative connective, our quantum analogue for the meet turns out to be non-commutative. The appearance of non-commutative operations is a common tread in quantum physics [5].

We take as our guide the well-known fact that the quantization of canonical phase space may be identified with the algebra of differential operators on configuration space. In analogy with the real/complex case, we introduce BDO_n the algebra of Boolean differential operators on $\mathbb{Z}_2^n$. We provide a couple of presentations by generators and relations of BDO_n, giving rise to the Boole-Weyl algebras BW_n and the shifted Boole-Weyl algebras SBW_n. We call these algebras the quantum Boolean algebras. We study the structural coefficients of BW_n and SBW_n in various bases.

Having introduced the quantum Boolean algebras, we proceed to study them from the logical and set theoretical viewpoints. For us, the main difference between classical and quantum logic is that classical observations, propositions, can be measured without, in principle, modifying the state of the system; quantum observations, in contrast, are quantum operators: the measuring process changes the state of the system. Indeed, regardless of the actual state of the system, after measurement the system will be in an eigenstate of the observable. Quantum observables are operators acting on the states of the system, and thus quite different to classical observables which are descriptions of the state of the system.

This work is organized as follows. In Section 2 we review some elementary facts on regular functions on affine spaces over $\mathbb{Z}_2$. In Section 3 we introduce BDO_n the algebra of Boolean differential operators on $\mathbb{Z}_2^n$. In Section 4 we introduce the Boole-Weyl algebra BW_n which is a presentation by generators and relations of BDO_n. We describe the structural coefficients of BW_n in several bases. In Section 5 we introduce the shifted Boole-Weyl algebra SBW_n which is another presentation by generators and relations of BDO_n. We describe the structural coefficients of SBW_n in several bases. In Section 6 we discuss the logical aspects of our constructions. We propose a quantum operational calculus for which Boolean differential operators play the same role that truth functions play in the classical propositional calculus. In Section 6 we adopt a set theoretical viewpoint; we show that just as the classical propositional calculus is intimately related with $\mathrm{PP}(x)$, the algebra of sets of subsets of x, the quantum operational calculus is intimately related with $\mathrm{PP}(x \sqcup x)$ the algebra of sets of subsets of two disjoint copies of x. In Section 8 we make some closing remarks and mention a few topics for future research.

2 Regular Functions on Boolean Affine Spaces

Our main goal in this work is to study the Boolean analogue for the Weyl algebras, and to describe those algebras from a logical viewpoint. Fixing a field k the Weyl algebra W_n can be identified with the k-algebra of algebraic differential operators on the affine space $\mathbb{A}^n(k) = k^n$. By definition [12, 16] the ring $k[\mathbb{A}^n]$ of regular functions on k^n is the ring of functions $f : k^n \to k$ such that there exists a polynomial $F \in k[x_1, ..., x_n]$ with $f(a) = F(a)$ for all $a \in k^n$. If k is

a field of characteristic zero, then the ring of regular functions on k^n can be identified with $k[x_1, ..., x_n]$ the ring of polynomials over k. Let $\partial_1, ..., \partial_n$ be the derivations of $k[x_1, ..., x_n]$ given by $\partial_i x_j = \delta_{i,j}$ for $i, j \in [n] = \{1, ..., n\}$. The algebra DO_n of differential operators on k^n is the subalgebra of $\mathrm{End}_k(k[x_1, ..., x_n])$ generated by ∂_i and the operators of multiplication by x_i for $i \in [n]$.

By definition, the Weyl algebra W_n is the k-algebra defined via generators and relations as

$$k < x_1, ..., x_n, y_1, ..., y_n > / < x_i x_j - x_j x_i,\ y_i y_j - y_j y_i,\ y_i x_j - x_j y_i,\ y_i x_i - x_i y_i - 1 >,$$

where $k < x_1, ..., x_n, y_1, ..., y_n >$ is the free associative k-algebra generated by $x_1, ..., x_n, y_1, ..., y_n$, and $< x_i x_j - x_j x_i,\ y_i y_j - y_j y_i,\ y_i x_j - x_j y_i,\ y_i x_i - x_i y_i - 1 >$ is the ideal generated by the relations $x_i x_j = x_j x_i$ and $y_i y_j = y_j y_i$ for $i, j \in [n]$, $y_i x_j - x_j y_i$ for $i \neq j \in [n]$, and $y_i x_i = x_i y_i + 1$ for $i \in [n]$.

The Weyl algebra W_n comes with a natural representation $\mathrm{W}_n \to \mathrm{End}_k(k[x_1, ..., x_n])$ which sends y_i to ∂_i and x_i to the operator of multiplication by x_i. This representation induces an isomorphism of algebras $\mathrm{W}_n \to \mathrm{DO}_n$.

We proceed to study the analogue of the Weyl algebras for the Boolean affine spaces $\mathbb{A}^n(\mathbb{Z}_2) = \mathbb{Z}_2^n$. First, we review some basic facts on regular functions on $\mathbb{Z}_2^n$. Let $\mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ be the ring of maps from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ with pointwise addition and multiplication. The ring $\mathbb{Z}_2[\mathbb{A}^n]$ of regular functions on $\mathbb{Z}_2^n$ is the sub-ring of $\mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ containing the maps $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ for which there exists a polynomial $F \in \mathbb{Z}_2[x_1, ..., x_n]$ such that $f(a) = F(a)$ for all $a \in \mathbb{Z}_2^n$. In this case $\mathbb{Z}_2[\mathbb{A}^n]$ is not a polynomial ring; instead we have the following result.

Lemma 1. There is an exact sequence of $\mathbb{Z}_2$-algebras

$$0 \longrightarrow < x_1^2 + x_1, ..., x_n^2 + x_n > \longrightarrow \mathbb{Z}_2[x_1, ..., x_n] \longrightarrow \mathbb{Z}_2[\mathbb{A}^n] \longrightarrow 0$$

where $< x_1^2 + x_1, ..., x_n^2 + x_n >$ is the ideal generated by the relations $x_i^2 = x_i$ for $i \in [n]$.

Proof. The map $\mathbb{Z}_2[x_1, ..., x_n] \to \mathbb{Z}_2[\mathbb{A}^n]$ sends a polynomial P to the map $p : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by $p(a) = P(a)$. Clearly x_i^2 and x_i define the same map $\mathbb{Z}_2^n \to \mathbb{Z}_2$. Thus $< x_1^2 + x_1, ..., x_n^2 + x_n >$ is in the kernel of the map $\mathbb{Z}_2[x_1, ..., x_n] \to \mathbb{Z}_2[\mathbb{A}^n]$. Let $P \in \mathbb{Z}_2[x_1, ..., x_n]$ be such that $P(a) = 0$ for all $a \in \mathbb{Z}_2^n$. We can write $P = (x_1^2 + x_1)Q + R$, where $R \in \mathbb{Z}_2[x_1, ..., x_n]$ is a degree 1 polynomial in x_1. Therefore $R = x_1 S + T$ where $S, T \in \mathbb{Z}_2[x_2, ..., x_n]$. Since $R(a) = 0$ for all $a \in \mathbb{Z}_2^n$, then $T(b) = R(0, b) = 0$ for all $b \in \mathbb{Z}_2^{n-1}$, and thus we obtain that $S(b) = S(b) + T(b) = R(1, b) = 0$. We have shown that the polynomials S and T define the 0 function thus, by induction, we conclude that $S, T \in < x_2^2 + x_2, ..., x_n^2 + x_n >$, which implies that R and therefore P belong to $< x_1^2 + x_1, ..., x_n^2 + x_n >$. ∎

Therefore the ring $\mathbb{Z}_2[\mathbb{A}^n]$ of regular functions on $\mathbb{Z}_2^n$ can be identified with the quotient ring

$$\mathbb{Z}_2[x_1, ..., x_n]/ < x_1^2 + x_1, ..., x_n^2 + x_n > .$$

Often we think of $\mathbb{Z}_2^n$ as a ring, with coordinate-wise sum and product. We identify $\mathbb{Z}_2^n$ with $\mathrm{P}[n]$, the set of subsets of $[n]$, as follows: $a \in \mathbb{Z}_2^n$ is identified with the subset $a \subseteq [n]$ such that $i \in a$ iff $a_i = 1$. With this identification the product ab of elements in $\mathbb{Z}_2^n$ agrees with the intersection $a \cap b$ of the sets a and b; the sum $a + b$ corresponds with the symmetric difference $a+b = (a \cup b) \setminus (a \cap b)$; the element $a + (1, ..., 1)$ is identified with the complement $\overline{a}$ of a. Note that $a \cup b = a+b+ab$. Note also that $\mathrm{PP}[n]$ denotes the set of all families of subsets of $[n]$.

For $a \in \mathrm{P}[n]$ let $m^a : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be the map such that

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

For $a \in \mathrm{P}[n]$ non-empty let $x^a \in \mathbb{Z}_2[x_1, ..., x_n]$ be the monomial $x^a = \prod_{i \in a} x_i$. Also set $x^{\emptyset} = 1$. The monomial x^a defines the map $x^a : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by

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

For $a \in \mathrm{P}[n]$ non-empty let $w^a \in \mathbb{Z}_2[x_1, ..., x_n]$ be the monomial $w^a = \prod_{i \in a}(x_i + 1)$. Also set $w^{\emptyset} = 1$. The monomial w^a defines the map $w^a : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by

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

Lemma 2 below follows from the definitions and the Möbius inversion formula [15] which can be stated as follows: given maps $f, g : \mathrm{P}[n] \to R$, with R a ring of characteristic 2, then

$$f(b) = \sum_{a \subseteq b} g(a) \quad \text{iff} \quad g(b) = \sum_{a \subseteq b} f(a).$$

Lemma 2. The following identities hold in $\mathbb{Z}_2[\mathbb{A}^n]$:

$$1)\ m^a = x^a w^{\overline{a}}. \quad 2)\ x^a = \sum_{a \subseteq b} m^b. \quad 3)\ m^a = \sum_{a \subseteq b} x^b. \quad 4)\ w^b = \sum_{a \subseteq \overline{b}} m^a.$$

$$5)\ m^a = \sum_{\overline{a} \subseteq b} w^b. \quad 6)\ w^b = \sum_{a \subseteq b} x^a. \quad 7)\ x^b = \sum_{a \subseteq b} w^a.$$

$$8)\ m^a m^b = \delta_{ab} m^a. \quad 9)\ x^a x^b = x^{a \cup b}. \quad 10)\ w^a w^b = w^{a \cup b}.$$

Notice that $\mathbb{Z}_2[\mathbb{A}^n] = \mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)$, indeed a map $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ can be written as

$$f = \sum_{f(a)=1} m^a = \sum_{f(a)=1} x^a w^{\overline{a}} = \sum_{f(a)=1} \prod_{i \in a} x_i \prod_{i \in \overline{a}} (x_i + 1)$$

$$= \sum_{f(a)=1,\ b \subseteq \overline{a}} x^{a \cup b} = \sum_{f(a)=1,\ a \subseteq b} x^b.$$

From Lemma 2 we see that there are several natural bases for the $\mathbb{Z}_2$-vector space

$$\mathbb{Z}_2[\mathbb{A}^n] = \mathbb{Z}_2[x_1, ..., x_n] / < x_1^2 + x_1, ..., x_n^2 + x_n >,$$

namely we can pick $\{m^a \mid a \in \mathrm{P}[n]\}$, $\{x^a \mid a \in \mathrm{P}[n]\}$, or $\{w^a \mid a \in \mathrm{P}[n]\}$. We use the following notation to write the coordinates of $f \in \mathbb{Z}_2[\mathbb{A}^n]$ in each one of these bases

$$f = \sum_{a \in \mathrm{P}[n]} f(a) m^a = \sum_{a \in \mathrm{P}[n]} f_x(a) x^a = \sum_{a \in \mathrm{P}[n]} f_w(a) w^a.$$

We obtain three linear maps $f \to f$, $f \to f_x$, and $f \to f_w$ from $\mathbb{Z}_2[\mathbb{A}^n]$ to $\mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)$. The coordinates f, f_x and f_w are connected, via the Möbius inversion formula, by the relations:

$$f_x(b) = \sum_{a \subseteq b} f(a), \quad f(b) = \sum_{a \subseteq b} f_x(a), \quad f_w(b) = \sum_{a \subseteq b} f(\overline{a}),$$

$$f(b) = \sum_{a \subseteq \overline{b}} f_w(a), \quad f_x(a) = \sum_{a \subseteq b} f_w(b), \quad f_w(a) = \sum_{a \subseteq b} f_x(b).$$

The maps $f \to f_x$ and $f \to f_w$ fail to be ring morphisms. Instead we have the identities:

$$(fg)_x(c) = \sum_{a \cup b = c} f_x(a) g_x(b) \quad \text{and} \quad (fg)_w(c) = \sum_{a \cup b = c} f_w(a) g_w(b).$$

We define a predicate O on finite sets as follows: given a finite set a, then Oa holds iff the cardinality of a is an odd number. In other words, O is the map from finite sets to $\mathbb{Z}_2$ such that $Oa = 1$ iff the cardinality of a is odd.

Example 3. Let $C \in \mathrm{PP}[n]$. A k-covering of $a \in \mathrm{P}[n]$ is a sequence $c_1, ..., c_k \in C$ such that $c_1 \cup ... \cup c_k = a$. Let $k\text{-}Cov_C(a)$ be the set of k-coverings of a by elements of C. Then a belongs to C iff $|k\text{-}Cov_C(a)|$ is odd for every $k \geq 1$. Indeed, let $f \in \mathbb{Z}_2[\mathbb{A}^n]$ be given by

$$f = \sum_{c \in C} x^c = \sum_{a \in \mathrm{P}[n]} 1_C(a) x^a,$$

where $1_C : \mathrm{P}[n] \to \mathbb{Z}_2$ is the characteristic function of C. Since $f^k = f$ for every $f \in \mathbb{Z}_2[\mathbb{A}^n]$, we have that

$$\sum_{a \in \mathrm{P}[n]} 1_C(a) x^a = f = f^k = \sum_{a \in \mathrm{P}[n]} \left(\sum_{a_1 \cup ... \cup a_k = a} \prod_{i=1}^{k} 1_C(a_i) \right) x^a = \sum_{a \in \mathrm{P}[n]} O(k\text{-}Cov_C(a)) x^a.$$

We conclude that $1_C(a) = O(k\text{-}Cov_C(a))$, and thus $a \in C$ iff $|k\text{-}Cov_C(a)|$ is odd.

3 Differential Operators on Boolean Affine Spaces

Next we consider the algebra of differential operators on affine Boolean spaces. Note that the derivations ∂_i, although well-defined on $\mathbb{Z}_2[x_1, ..., x_n]$, do not define operators on $\mathbb{Z}_2[\mathbb{A}^n]$; indeed if we had such an operator, then $0 = x_i + x_i = \partial_i x_i^2 = \partial_i x_i = 1$. It is thus necessary to introduce an alternative definition for ∂_i. The Boolean partial derivative $\partial_i f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ of a map $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is given [4, 14] by

$$\partial_i f(x) = f(x + e_i) + f(x)$$

where $e_i \in \mathbb{Z}_2^n$ has vanishing entries except at position i. With this definition $\partial_i x_i = \partial_i x_i^2 = 1$, the contradiction above does not arise, and we obtained well-defined operators

$$\partial_i : \mathbb{Z}_2[\mathbb{A}^n] \longrightarrow \mathbb{Z}_2[\mathbb{A}^n].$$

The operators ∂_i fail to be derivations; instead they satisfy the twisted Leibnitz identity

$$\partial_i(fg) = \partial_i f g + s_i f \partial_i g$$

where the shift operators $s_i : \mathbb{Z}_2[\mathbb{A}^n] \longrightarrow \mathbb{Z}_2[\mathbb{A}^n]$ are given by $s_i f(x) = f(x + e_i)$. Indeed:

$$\begin{aligned} \partial_i(fg)(x) &= f(x + e_i)g(x + e_i) + f(x)g(x) \\ &= [f(x + e_i) + f(x)]g(x) + f(x + e_i)[g(x + e_i) + g(x)] \\ &= \partial_i f(x)g(x) + s_i f(x)\partial_i g(x). \end{aligned}$$

The operators ∂_i are nilpotent, $\partial_i^2 = 0$, since:

$$\partial_i^2 f(x) = \partial_i f(x + e_i) + \partial_i f(x) = f(x) + f(x + e_i) + f(x + e_i) + f(x) = 0.$$

Definition 4. The algebra BDO_n of Boolean differential operators on $\mathbb{Z}_2^n$ is the subalgebra of $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ generated by ∂_i and the operators of multiplication by x_i for $i \in [n]$.

Theorem 5. The following identities hold for $i \in [n]$ and $x_i, \partial_i, s_i \in \mathrm{BDO}_n$:

1. $x_i^2 = x_i$. 2. $\partial_i^2 = 0$. 3. $s_i^2 = 1$. 4. $\partial_i = s_i + 1$. 5. $\partial_i s_i = s_i \partial_i = \partial_i$.

6. $s_i = \partial_i + 1$. 7. $s_i x_i = x_i s_i + s_i = (x_i + 1)s_i$. 8. $\partial_i x_i = x_i \partial_i + s_i = x_i \partial_i + \partial_i + 1$.

Proof. We have already shown that $x_i^2 = x_i$ and $\partial_i^2 = 0$. For the other identities we have that:

$$s_i^2 f(x) = s_i f(x + e_i) = f(x + e_i + e_i) = f(x);$$

$$\partial_i f(x) = f(x + e_i) + f(x) = s_i f(x) + f(x) = (s_i + 1)f(x);$$

$$s_i \partial_i f(x) = \partial_i f(x + e_i) = f(x + e_i + e_i) + f(x + e_i) = f(x) + f(x + e_i) = \partial_i f(x);$$

$$\partial_i s_i f(x) = s_i f(x+e_i) + s_i f(x) = f(x+e_i+e_i) + f(x+e_i) = f(x) + f(x+e_i) = \partial_i f(x);$$

$$s_i x_i f(x) = (x_i+1) f(x+e_i) = x_i f(x+e_i) + f(x+e_i) = x_i s_i f(x) + s_i f(x) = (x_i s_i + s_i) f(x);$$

$$s_i f(x) = f(x+e_i) = f(x+e_i) + f(x) + f(x) = \partial_i f(x) + f(x) = (\partial_i + 1) f(x);$$

$$\partial_i (x_i f)(x) = x_i f(x+e_i) + f(x+e_i) + x_i f(x) = x_i (f(x+e_i) + f(x)) + f(x+e_i),$$

$$\text{thus} \quad \partial_i (x_i f) = x_i \partial_i f + f(x+e_i) = (x_i \partial_i + s_i) f = (x_i \partial_i + \partial_i + 1) f.$$

□

The operator ∂_i acts on the bases $m^a,\ x^a$ and w^a as follows:

$$\partial_i m^a = m^{a+e_i} + m^a, \quad \partial_i x^a = \begin{cases} x^{a \backslash i} & \text{if } i \in a \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \partial_i w^a = \begin{cases} w^{a \backslash i} & \text{if } i \in a \\ 0 & \text{otherwise.} \end{cases}$$

From these expressions we obtain that:

- $\partial_i f(a) = 1$ if and only if $f(a) \neq f(a+e_i)$, i.e. $\partial_i f = \sum_{f(a) \neq f(a+e_i)} m^a$.
- $(\partial_i f)_x(a) = f_x(a \cup i)$ if $i \notin a$ and $(\partial_i f)_x(a) = 0$ if $i \in a$, i.e. $\partial_i f = \sum_{i \in a \in \mathrm{P}[n]} f_x(a) x^{a-i}$.
- $(\partial_i f)_w(a) = f_w(a \cup i)$ if $i \notin a$ and $(\partial_i f)_w(a) = 0$ if $i \in a$, i.e. $\partial_i f = \sum_{i \in a \in \mathrm{P}[n]} f_w(a) w^{a-i}$.

More generally one can show by induction, for $a, b \in \mathrm{P}[n]$, that:

$$\partial^b m^a = \sum_{c \subseteq b} m^{a+c}, \quad \partial^b x^a = \begin{cases} x^{a \backslash b} & \text{if } b \subseteq a \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \partial^b w^a = \begin{cases} w^{a \backslash b} & \text{if } b \subseteq a \\ 0 & \text{otherwise} \end{cases}$$

By definition $\mathrm{BDO}_n \subseteq \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ acts naturally on $\mathbb{Z}_2[\mathbb{A}^n]$, so we have a map

$$\mathrm{BDO}_n \otimes_{\mathbb{Z}_2} \mathbb{Z}_2[\mathbb{A}^n] \to \mathbb{Z}_2[\mathbb{A}^n].$$

Proposition 6. Consider maps $D : \mathrm{P}[n] \times \mathrm{P}[n] \to \mathbb{Z}_2$ and $f : \mathrm{P}[n] \to \mathbb{Z}_2$.

1. Let $D = \sum_{a,b \in \mathrm{P}[n]} D(a,b) m^a \partial^b \in \mathrm{BDO}_n$, $f = \sum_{c \in \mathrm{P}[n]} f(c) m^c \in \mathbb{Z}_2[\mathbb{A}^n]$, and $Df = \sum_{a \in \mathrm{P}[n]} Df(a) m^a$. Then we have that

$$Df(a) = \sum_{e \subseteq b} D(a,b) f(a+e).$$

2. Let $D = \sum_{a,b \in \mathrm{P}[n]} D_x(a,b) x^a \partial^b \in \mathrm{BDO}_n,\ f = \sum_{c \in \mathrm{P}[n]} f_x(c) x^c \in \mathbb{Z}_2[\mathbb{A}^n],$ and $Df = \sum_{e \in \mathrm{P}[n]} Df_x(e) x^e$. Then

$$Df_x(e) = \sum_{\substack{a,\ b \subseteq c \\ a \cup (c \backslash b) = e}} D_x(a,b) f_x(c).$$

Proof.

1. $$Df = \sum_{a,b,c\in \mathrm{P}[n]} D(a,b)f(c)m^a\partial^b m^c = \sum_{a,e\subseteq b,c} D(a,b)f(c)m^a m^{c+e}$$

$$= \sum_{a,e\subseteq b} D(a,b)f(a+e)m^a = \sum_{a\in \mathrm{P}[n]} \left(\sum_{e\subseteq b} D(a,b)f(a+e) \right) m^a.$$

2. $$Df = \sum_{a,b,c\in \mathrm{P}[n]} D_x(a,b)f_x(c)x^a\partial^b x^c = \sum_{a,b\subseteq c} D_x(a,b)f_x(c)x^{a\cup c\setminus b}$$

$$= \sum_{e\in \mathrm{P}[n]} \left(\sum_{\substack{a,\ b\subseteq c \\ a\cup(c\setminus b)=e}} D_x(a,b)f_x(c) \right) x^e.$$

□

Theorem 7. For $n \geq 1$ we have that $\mathrm{BDO}_n = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$.

Proof. Note that $\dim\left(\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])\right) = \dim(\mathbb{Z}_2[\mathbb{A}^n])\dim(\mathbb{Z}_2[\mathbb{A}^n]) = 2^n 2^n = 2^{2n}$. The set $\{x^a\partial^b \mid a,b \in \mathrm{P}[n]\}$ has 2^{2n} elements and generates BDO_n as a $\mathbb{Z}_2$ vector space, thus it is enough to show that it is a linearly independent set. Suppose that

$$\sum_{a,b\in \mathrm{P}[n]} f(a,b)x^a\partial^b = \sum_{b\in \mathrm{P}[n]} \left(\sum_{a\in \mathrm{P}[n]} f(a,b)x^a \right) \partial^b = 0.$$

Pick a minimal set $c \in \mathrm{P}[n]$ such that $\sum_{a\in \mathrm{P}[n]} f(a,c)x^a \neq 0$. We have that:

$$\left(\sum_{a,b\in \mathrm{P}[n]} f(a,b)x^a\partial^b \right)(x^c) = \sum_{b\in \mathrm{P}[n]} \left(\sum_{a\in \mathrm{P}[n]} f(a,b)x^a \right) \partial^b(x^c) = \sum_{a\in \mathrm{P}[n]} f(a,c)x^a = 0.$$

Therefore, since $\{x^a \mid a \in \mathrm{P}[n]\}$ is a basis for the regular functions we have that $f(a,c) = 0$ in contradiction with the fact $\sum_{a\in \mathrm{P}[n]} f(a,c)x^a \neq 0$. We conclude that $\dim\left(\mathrm{BDO}_n\right) = 2^{2n}$ yielding the desired result.

□

Put together Proposition 6 and Theorem 7 provide a couple of explicit ways of identifying BDO_n with $\mathrm{M}_{2^n}(\mathbb{Z}_2)$ the algebra of square matrices of size 2^n with coefficients in $\mathbb{Z}_2$. Note that $\mathrm{M}_{2^n}(\mathbb{Z}_2)$ may be identified with $\mathrm{M}(\mathrm{P}[n]\times\mathrm{P}[n],\mathbb{Z}_2)$. Moreover, we can identify $\mathrm{M}(\mathrm{P}[n]\times\mathrm{P}[n],\mathbb{Z}_2)$ with the set of directed graphs with vertex set $\mathrm{P}[n]$ and without multiple edges as follows: given a matrix $M \in \mathrm{M}_{2^n}(\mathbb{Z}_2)$ its associated graph has an edge from b to a iff $M_{a,b} = 1$.

Let $\mathrm{R} : \mathrm{BDO}_n \to \mathrm{M}_{2^n}(\mathbb{Z}_2)$ be the $\mathbb{Z}_2$-linear map constructed as follows. Consider the bases $\{m^a\partial^b \mid a, b \in \mathrm{P}[n]\}$ for BDO_n and $\{m^a \mid a \in \mathrm{P}[n]\}$ for $\mathbb{Z}_2[\mathbb{A}^n]$. For $a, b \in \mathrm{P}[n]$, let $\mathrm{R}(m^a\partial^b)$ be the matrix of $m^a\partial^b$ on the basis m^a. The action of $m^a\partial^b$ on m^c is given by

$$m^a\partial^b m^c = m^a \sum_{e\subseteq b} m^{c+e} = \sum_{e\subseteq b} m^a m^{c+e} = m^a \quad \text{if} \quad c + a \subseteq b \quad \text{and zero otherwise.}$$

Therefore, the matrix $\mathrm{R}(m^a\partial^b)$ is given for $c, d \in \mathrm{P}[n]$ by the rule

$$\mathrm{R}(m^a\partial^b)_{c,d} = \begin{cases} 1 & \text{if } c = a \text{ and } \ d + a \subseteq b \\ 0 & \text{otherwise} \end{cases}$$

Example 8. The graph of $\mathrm{R}(m^{\{1,2\}}\partial^{\{2,3\}})$ is show in Figure 1.

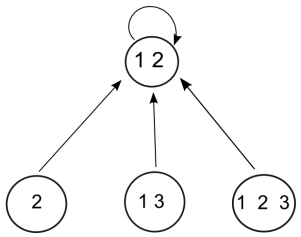

Figure 1: Graph of the matrix $\mathrm{R}(m^{\{1,2\}}\partial^{\{2,3\}})$.

For a second representation consider the $\mathbb{Z}_2$-linear map $\mathrm{S} : \mathrm{BDO}_n \to \mathrm{M}_{2^n}(\mathbb{Z}_2)$ constructed as follows. Consider the bases $\{x^a\partial^b \mid a, b \in \mathrm{P}[n]\}$ for BDO_n and $\{x^a \mid a \in \mathrm{P}[n]\}$ for $\mathbb{Z}_2[\mathbb{A}^n]$. For $a, b \in \mathrm{P}[n]$ let $\mathrm{S}(x^a\partial^b)$ be the matrix of $x^a\partial^b$ on the basis x^a. The action of $x^a\partial^b$ on x^c is given by

$$x^a\partial^b x^c = \begin{cases} x^{a\cup c\setminus b} & \text{if } b \subseteq c \\ 0 & \text{otherwise} \end{cases}$$

Therefore, the matrix $\mathrm{S}(x^a\partial^b)$ is given for $c, d \in \mathrm{P}[n]$ by the rule

$$\mathrm{S}(x^a\partial^b)_{c,d} = \begin{cases} 1 & \text{if } c = a \cup d \setminus b \text{ and } \ b \subseteq d \\ 0 & \text{otherwise} \end{cases}$$

Example 9. The graph associated to the matrix $\mathrm{S}(m^{\{1\}}\partial^{\{3\}})$ is shown in Figure 2.

4 Boole-Weyl Algebras

Let us motivate from the viewpoint of canonical quantization our definition of Boole-Weyl algebras. Canonical phase space, for a field k of characteristic zero, can be identified with the affine space $k^n \times k^n$. The Poisson bracket on $k[x_1, ..., x_n, y_1, ..., y_n]$ in canonical coordinates

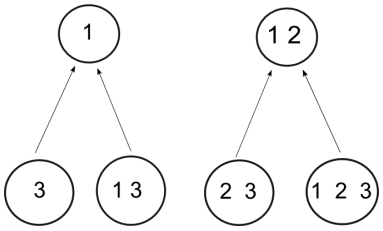

Figure 2: Graph of the matrix $\mathrm{S}(m^{\{1\}}\partial^{\{3\}})$.

$x_1, ..., x_n, y_1, ..., y_n$ on $k^n \times k^n$ is given by $\{x_i, x_j\} = 0, \{y_i, y_j\} = 0, \{x_i, y_j\} = \delta_{i,j}$. Equivalently, the Poisson bracket is given for $f, g \in k[x_1, ..., x_n, y_1, ..., y_n]$ by

$$\{f, g\} = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial y_i} - \frac{\partial f}{\partial y_i}\frac{\partial f}{\partial x_i}.$$

Canonical quantization may be formulated as the problem of promoting the commutative variables x_i and y_j into non-commutative operators $\widehat{x}_i$ and $\widehat{y}_j$ satisfying the commutation relations:

$$[\widehat{x}_i, \widehat{x}_j] = 0, \quad [\widehat{y}_i, \widehat{y}_j] = 0, \quad [\widehat{y}_i, \widehat{x}_j] = \delta_{i,j}.$$

Note that the free algebra generated by $\widehat{x}_i$ and $\widehat{y}_j$ subject to the above relations is precisely what is called the Weyl algebra.

Now let $k = \mathbb{Z}_2$ and consider the affine phase spaces $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$. Let $x_1, ..., x_n, y_1, ..., y_n$ be canonical coordinates on $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$. The analogue of the Poisson bracket

$$\{\ ,\ \} : \mathbb{Z}_2[\mathbb{A}^{2n}] \otimes \mathbb{Z}_2[\mathbb{A}^{2n}] \to \mathbb{Z}_2[\mathbb{A}^{2n}]$$

can be expressed for $f, g \in \mathbb{Z}_2[\mathbb{A}^{2n}]$ as

$$\{f, g\} = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial y_i} + \frac{\partial f}{\partial y_i}\frac{\partial f}{\partial x_i},$$

where $\frac{\partial}{\partial x_i}$ and $\frac{\partial}{\partial y_i}$ are the Boolean derivatives along the coordinates x_i and y_i. Clearly, the full set of axioms for a Poisson bracket will not longer hold, e.g. Boolean derivatives are not derivations. Nevertheless, the bracket is still determined by its values on the canonical coordinates: $\{x_i, x_j\} = 0, \{y_i, y_j\} = 0, \{x_i, y_j\} = \delta_{i,j}$. Canonical quantization consists in promoting the commutative variables x_i and y_j into non-commutative operators $\widehat{x}_i$ and $\widehat{y}_j$ satisfying the commutation relations:

$$[\widehat{x}_i, \widehat{x}_j] = 0, \quad [\widehat{y}_i, \widehat{y}_j] = 0, \quad [\widehat{y}_i, \widehat{x}_j] = 0, \text{ for } i \neq j, \text{ and } \quad [\widehat{y}_i, \widehat{x}_i]_{s_i} = 1.$$

Note that in the last relation we did not use the commutator but the shifted commutator

$$[f,g]_{s_i} = fg + s_i fg;$$

this choice is expected since the operators $\widehat{y}_i$ are twisted derivations instead of usual derivations. The relation $[\widehat{y}_i, \widehat{x}_i]_{s_i} = 1$ can be equivalently written using the commutator as

$$[\widehat{y}_i, \widehat{x}_i] = \widehat{y}_i + 1.$$

We are ready to introduce the Boole-Weyl algebras BW_n, which we also call quantum Boolean algebras. The Boole-Weyl algebra BW_n is the free algebra generated by $\widehat{x}_i$ and $\widehat{y}_j$ subject to the relations above. The algebras BW_n are the analogue of the Weyl algebras in the Boolean context.

Definition 10. The algebra BW_n is the quotient of $\mathbb{Z}_2 < x_1, ..., x_n, y_1, ..., y_n >$, the free associative $\mathbb{Z}_2$-algebra generated by $x_1, ..., x_n, y_1, ..., y_n$, by the ideal

$$< x_i^2 + x_i,\ x_i x_j + x_j x_i,\ y_i y_j + y_j y_i,\ y_i^2,\ y_i x_j + x_j y_i,\ y_i x_i + x_i y_i + y_i + 1 >,$$

generated by the relations $x_i^2 = x_i$, $y_i^2 = 0$, and $y_i x_i = x_i y_i + y_i + 1$ for $i \in [n]$, $x_i x_j = x_j x_i$ and $y_i y_j = y_j y_i$ for $i, j \in [n]$, and $y_i x_j + x_j y_i$ for $i \neq j \in [n]$.

Theorem 11. The map $\mathbb{Z}_2 < x_1, ..., x_n, y_1, ..., y_n > \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ sending x_i to the operator of multiplication by x_i, and y_i to ∂_i, descends to an isomorphism $\mathrm{BW}_n \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ of $\mathbb{Z}_2$-algebras.

Proof. By Theorem 5 the given map descends. By definition it is a surjective map

$$\mathrm{BW}_n \to \mathrm{BDO}_n = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n]).$$

Moreover, this map is an isomorphisms since $\dim(\mathrm{BW}_n) = \dim(\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n]))$. Indeed using the commutation relations it is easy to check that the natural map

$$\mathbb{Z}_2[x_1, ..., x_n]/ < x_i^2 + x_i > \otimes\, \mathbb{Z}_2[y_1, ..., y_n]/ < y_i^2 > \longrightarrow \mathrm{BW}_n$$

is surjective. If $\sum_{a,b \in \mathrm{P}[n]} f(a,b) x^a \otimes y^b$ is in the kernel of the latter map, then the Boolean differential operator $\sum_{a,b \in \mathrm{P}[n]} f(a,b) x^a \partial^b$ would vanish, and therefore the coefficients $f(a,b)$ must vanish as well. Thus

$$\dim(\mathrm{BW}_n) = \dim(\mathbb{Z}_2[x_1, ..., x_n]/ < x_i^2 + x_i >)\dim(\mathbb{Z}_2[y_1, ..., y_n]/ < y_i^2 >) = 2^n 2^n$$

$$= \dim(\mathbb{Z}_2[\mathbb{A}^n])\dim(\mathbb{Z}_2[\mathbb{A}^n]) = \dim(\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])).$$

□

Theorem 12. The map $\mathbb{Z}_2 < x_1, ..., x_n, y_1, ..., y_n > \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ sending x_i to the operator of multiplication by $w_i = x_i + 1$, and y_i to the operator ∂_i, descends to an isomorphism $\mathrm{BW}_n \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ of $\mathbb{Z}_2$-algebras.

Proof. Follows from the fact that w_i and ∂_j satisfy exactly the same relation as x_i and ∂_j. □

Corollary 13. Any identity in BW_n involving x_i and ∂_j has an associated identity involving w_i and ∂_j obtained by replacing x_i by w_i.

Lemma 14. For $a, b, c, d \in \mathrm{P}[n]$ the following identities hold in BW_n :

$$1.\ y^b m^c = \sum_{b_1 \subseteq b_2 \subseteq b} m^{c+b_2} y^{b_1}. \qquad 2.\ m^a y^b m^c y^d = \sum_{\substack{d \subseteq e \\ e \setminus d \subseteq a+c \subseteq b}} m^a y^e.$$

$$3.\ y^b x^c = \sum_{k_1 \subseteq k_2 \subseteq b \cap c} x^{c \setminus k_2} y^{b \setminus k_1}. \quad 4.\ x^a y^b x^c y^d = \sum_{a \subseteq e,\ d \subseteq f} c(a,b,c,d,e,f) x^e y^f,$$

where

$$c(a,b,c,d,e,f) = O\left\{k_1 \subseteq k_2 \subseteq b \cap c \ \mid\ a \cup (c \setminus k_2) = e,\ \ b \setminus k_1 = f \setminus d\right\}.$$

Proof. 1. By Theorem 11 it is enough to show that the differential operators associated with both sides of the equation are equal. Consider the operator of multiplication by $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and let $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be any other map. The twisted Leibnitz rule $y_i f(g) = y_i(f)g + s_i(f)\partial_i g$ can be extended, since s_i and y_i commute, to the identity:

$$y^b f(g) = \sum_{b_1 \sqcup b_2 = b} s^{b_2} y^{b_1}(f) y^{b_2}(g) \quad \text{thus} \quad y^b f = \sum_{b_1 \sqcup b_2 = b} s^{b_2} y^{b_1}(f) y^{b_2}.$$

In particular we obtain that

$$y^b m^c = \sum_{e \sqcup b_2 = b} s^{b_2} y^e(m^c) y^{b_2} = \sum_{b_1 \sqcup b_2 \subseteq b} s^{b_2} s^{b_1}(m^c) y^{b_2} =$$

$$= \sum_{b_1 \sqcup b_2 \subseteq b} m^{c+b_1+b_2} y^{b_2} = \sum_{b_1 \subseteq b_2 \subseteq b} m^{c+b_2} y^{b_1}.$$

2. We have that:

$$m^a y^b m^c y^d = \sum_{b_1 \subseteq b_2 \subseteq b} m^a m^{c+b_2} y^{b_1} y^d = \sum_{b_1 \subseteq b_2 \subseteq b} \delta_{a,c+b_2} m^a y^{b_1 \sqcup d}$$

$$= \sum_{b_1 \subseteq a+c \subseteq b} m^a y^{b_1 \sqcup d} = \sum_{\substack{d \subseteq e \\ e \setminus d \subseteq a+c \subseteq b}} m^a y^e.$$

where the last identity follows from the fact that $b_2 = a + c$, $e = b_1 \sqcup d$.

3. From the relations $y_i x_j = x_j y_i$ for $i \neq j$ and $y_i x_i = x_i y_i + y_i + 1$ we can argue as follows. If a letter y_i is placed just to the left of a x_j we can move it to the right, since these letters commute. If instead we have a product $y_i x_i$, then three options arises: a) y_i moves to the right of x_i; b) y_i absorbs x_i; c) x_i and y_i annihilate each other leaving an 1. Call k_1 the set of indices for which c) occurs, and k_2 the set of indices for which either b) or c) occur. Then $k_1 \subseteq k_2 \subseteq b \cap c$ and the set for which option a) occurs is $b \cap c \setminus k_2$. Thus the desired identity is obtained.

4. We have that:

$$x^a y^b x^c y^d = \sum_{k_1 \subseteq k_2 \subseteq b \cap c} x^{a \cup c \setminus k_2} y^{(b \setminus k_1) \sqcup d} = \sum_{a \subseteq e,\ d \subseteq f} c(a,b,c,d,e,f) x^e y^f,$$

where

$$c(a,b,c,d,e,f) = O\left\{k_1 \subseteq k_2 \subseteq b \cap c \mid a \cup (c \setminus k_2) = e, \quad b \setminus k_1 = f \setminus d\right\}.$$

□

Example 15.

$$y^{\{1\}} m^{\{1\}} = m^{\{1\}} + m^{\emptyset} + m^{\{\emptyset\}} y^{\{1\}}; \quad m^{\{1\}} y^{\{1\}} m^{\{1\}} y^{\{1\}} = m^{\{1\}} y^{\{1\}};$$

$$y^{\{1\}} m^{\{1,2\}} = m^{\{1,2\}} + m^{\{2\}} + m^{\{2\}} y^{\{1\}}; \quad m^{\{2\}} y^{\{1\}} m^{\{1,2\}} y^{\{1\}} = m^{\{2\}} y^{\{1\}};$$

$$y^{\{1,2\}} m^{\{1,2,3\}} = m^{\{1,2,3\}} + m^{\{2,3\}} + m^{\{1,3\}} + m^{\{1\}} + m^{\{2,3\}} y^{\{1\}} + m^{\{3\}} y^{\{1\}}$$

$$+ m^{\{1,3\}} y^{\{2\}} + m^{\{3\}} y^{\{2\}} + m^{\{3\}} y^{\{1,2\}}; \quad m^{\{3\}} y^{\{1,2\}} m^{\{1,2,3\}} y^{\{1\}} = m^{\{3\}} y^{\{1,2\}}.$$

Example 16. For $i \in [k]$ let $A_i \in \mathrm{PP}[n]$ and $f_i = \sum_{a \in A_i} y^a$. Then

$$f_1 ... f_k = \sum_{b \in \mathrm{P}[n]} O\{(a_1, ..., a_k) \in A_1 \times ... \times A_k \mid a_1 \sqcup ... \sqcup a_k = b\ \} y^b.$$

In particular, for $A \in \mathrm{PP}[n]$ and $f = \sum_{a \in A} y^a$, we get that

$$f^k = \sum_{b \in \mathrm{P}[n]} O\{a_1, ..., a_k \in A \mid a_1 \sqcup ... \sqcup a_k = b\ \} y^b.$$

For example, if $A = \mathrm{P}[n]$ then for $k \geq 2$ we have that:

$$f^k = \sum_{b \in \mathrm{P}[n]} O\{a_1, ..., a_k \in \mathrm{P}[n] \mid a_1 \sqcup .... \sqcup a_k = b\ \} y^b = \sum_{b \in \mathrm{P}[n]} (k^{|b|} \bmod 2)\ y^b,$$

thus $f^k = f$ if k is odd, and $f^k = 1$ if k is even.

From Lemma 2 we see that there are several natural basis for BW_n, namely:

$$\{m^a y^b \mid a,b \in \mathrm{P}[n]\ \},\quad \{x^a y^b \mid a,b \in \mathrm{P}[n]\ \},\quad \{w^a y^b \mid a,b \in \mathrm{P}[n]\ \}.$$

We write the coordinates of $f \in \mathrm{BW}_n$ in these bases as:

$$f = \sum_{a,b\in \mathrm{P}[n]} f_m(a,b) m^a y^b = \sum_{a,b\in \mathrm{P}[n]} f_x(a,b) x^a y^b = \sum_{a,b\in \mathrm{P}[n]} f_w(a,b) w^a y^b.$$

These coordinates systems are connected by the relations:

$$f_x(b,c) = \sum_{a\subseteq b} f_m(a,c),\quad f_m(b,c) = \sum_{a\subseteq b} f_x(a,c),\quad f_w(b,c) = \sum_{a\subseteq b} f_m(\overline{a},c),$$

$$f_m(b,c) = \sum_{a\subseteq \overline{b}} f_w(a,c),\quad f_x(a,c) = \sum_{a\subseteq b} f_w(b,c),\quad f_w(a) = \sum_{a\subseteq b} f_x(b,c).$$

Theorem 17. For $f,g \in \mathrm{BW}_n$ the following identities hold for $a,e,h \in \mathrm{P}[n]$:

1. $(fg)_m(a,e) = \sum\limits_{\substack{b,c,d\subseteq e\\ e\setminus d\subseteq a+c\subseteq b}} f_m(a,b) g_m(c,d).$

2. $(fg)_x(e,h) = \sum\limits_{a\subseteq e, b,c, d\subseteq h} c(a,b,c,d,e,h) f_x(a,b) g_x(c,d),$ where

$$c(a,b,c,d,e,h) = O\left\{k_1 \subseteq k_2 \subseteq b\cap c \ \mid\ a\cup(c\setminus k_2) = e,\ \ b\setminus k_1 = h\setminus d\right\}.$$

Proof. 1. Let $f = \sum_{a,b\in \mathrm{P}[n]} f_m(a,b) m^a y^b$, $g = \sum_{c,d\in \mathrm{P}[n]} g_m(c,d) m^c y^d$, then we have that:

$$\begin{aligned} fg &= \sum_{a,b,c,d\in \mathrm{P}[n]} f_m(a,b) g_m(c,d) m^a y^b m^c y^d \\ &= \sum_{a,b,c,d,e\in \mathrm{P}[n]} f_m(a,b) g_m(c,d) \sum_{\substack{d\subseteq e\\ e\setminus d\subseteq a+c\subseteq b}} m^a y^e \\ &= \sum_{d\subseteq e,\ e\setminus d\subseteq a+c\subseteq b} f_m(a,b) g_m(c,d) m^a y^e. \end{aligned}$$

2. Let $f = \sum_{a,b\in \mathrm{P}[n]} f_x(a,b) x^a y^b$, $g = \sum_{c,d\in \mathrm{P}[n]} g_x(c,d) x^c y^d$, then we have that:

$$\begin{aligned} fg &= \sum_{a,b,c,d\in \mathrm{P}[n]} f_x(a,b) g_x(c,d) x^a y^b x^c y^d \\ &= \sum_{a,b,c,d\in \mathrm{P}[n]} \sum_{a\subseteq e,\ d\subseteq h} f_x(a,b) g_x(c,d) c(a,b,c,d,e,h) x^e y^h, \end{aligned}$$

where

$$c(a,b,c,d,e,h) = O\left\{k_1 \subseteq k_2 \subseteq b\cap c \mid a\cup(c\setminus k_2) = e,\ \ b\setminus k_1 = h\setminus d\right\}.$$

□

Example 18. Let $x^r y^r = \sum_{a,b\in \mathrm{P}[n]} f_m(a,b) m^a y^b$ and $x^s y^s = \sum_{a,b\in \mathrm{P}[n]} g_m(a,b) m^a y^b$. Then

$$(fg)^2_m(a,e) = \sum_{\substack{b,c,d\subseteq e \\ e\setminus d\subseteq a+c\subseteq b}} f_m(a,b) g_m(c,d).$$

For a non-vanishing summand we must have that $a = b = r$, $c = d = s$, and $s \subseteq e$. The conditions $e \setminus s \subseteq r + s \subseteq r$ implies that $s \subseteq r$ and $e \setminus s \subseteq r \setminus s$, thus $e \subseteq r$. We conclude that $(fg)^2_m(a,e) = 1$ iff $s \subseteq r$, $a = r$ and $s \subseteq e \subseteq r$. Thus $x^r y^r x^s y^s = 0$ if $s \nsubseteq r$. For $s \subseteq r$ we get

$$x^r y^r x^s y^s = \sum_{s\subseteq e\subseteq r} x^r y^e.$$

In particular we get that $(x^r y^r)^n = x^r y^r$.

Example 19. Let $f = \sum_{a,b\in \mathrm{P}[n]} m^a y^b = \sum_{a,b\in \mathrm{P}[n]} f_m(a,b) m^a y^b$. We have that

$$f^2_m(a,e) = \sum_{\substack{b,c,d\subseteq e \\ e\setminus d\subseteq a+c\subseteq b}} 1 = O\{b,c,d \mid d \subseteq e,\ e \setminus d \subseteq a + c \subseteq b\}.$$

Note that if $a+c$ is not equal to $[n]$, then there are an even number of choices for b, thus we can assume that $c = \overline{a}$ and $b = [n]$. The condition $e \setminus d \subseteq a + c = [n]$ becomes trivial, and therefore $f^2(a,e) = O\mathrm{P}[|e|] = 0$ if $e \neq \emptyset$ and $f^2(a,e) = 1$ if $e = \emptyset$. Therefore we have that

$$f^2 = \sum_{a\in \mathrm{P}[n]} m^a.$$

Example 20. Let $r = \sum_{i\in[n]} x^{\{i\}} y^{\{i\}} = \sum_{a,b\in \mathrm{P}[n]} r_x(a,b) x^a y^b \in \mathrm{BW}_n$ then we have that:

$$r^2_x(e,f) = \sum_{a\subseteq e,b,c,d\subseteq f} c(a,b,c,d,e,f) r_x(a,b) r_x(c,d), \text{ where}$$

$$c(a,b,c,d,e,f) = O\left\{k_1 \subseteq k_2 \subseteq b \cap c \ \mid \ a \cup (c \setminus k_2) = e, \ \ b \setminus k_1 = f \setminus d\right\}.$$

Clearly $|a| = |b| = |c| = |d| = 1$, $a = b$, and $c = d$. Moreover, we have that $|b \cap c| \leq 1$. If $|b \cap c| = 1$, then $a = b = c = d = e = \{i\}$ for some $i \in [n]$. If $k_1 = \emptyset$, then there are two options for k_2 leading to a vanishing coefficient. Thus we may assume that $k_1 = k_2 = \{i\}$ and then necessarily $f = \{i\}$. Thus we conclude that $r^2_x(\{i\},\{i\}) = 1$. If instead $|b \cap c| = 0$, then $k_1 = k_2 = \emptyset$, $a \cup c = e$ and $b = f \setminus d$. Let $i \neq j$ and suppose that $a = b = \{i\}$ and $c = d = \{j\}$. Then $e = f = \{i,j\}$ and $r^2_x(\{i,j\},\{i,j\}) = 1$. All together we conclude that

$$r^2 = \sum_{i\in[n]} x^{\{i\}} y^{\{i\}} + \sum_{i\neq j\in[n]} x^{\{i,j\}} y^{\{i,j\}}.$$

Example 21. From Corollary 13 we see that if $s = \sum_{i\in[n]} w^{\{i\}}y^{\{i\}}$ then

$$s^2 = \sum_{i\in[n]} w^{\{i\}}y^{\{i\}} + \sum_{i\neq j\in[n]} w^{\{i,j\}}y^{\{i,j\}}.$$

Equivalently, if $s = \sum_{i\in[n]} y^{\{i\}} + \sum_{i\in[n]} x^{\{i\}}y^{\{i\}}$ then

$$s^2 = \sum_{i\in[n]} y^{\{i\}} + \sum_{i\in[n]} x^{\{i\}}y^{\{i\}} + \sum_{i\neq j\in[n]} y^{\{i,j\}} + \sum_{i\neq j\in[n]} x^{\{i,j\}}y^{\{i,j\}} + + \sum_{i\neq j\in[n]} \left(x^{\{i\}} + x^{\{j\}}\right) y^{\{i,j\}}.$$

5 A Shifted Presentation

So far, the operators ∂_i have played the main role. In this section we take an alternative viewpoint and let the operators s_i be the main characters. Recall that the Boolean derivatives and the Boolean shift operators are related by the identities $y_i = s_i + 1$ and $s_i = y_i + 1$. For $a, b \in \mathrm{P}[n]$ let $y^a = \prod_{i\in a} y_i$ and $s^a = \prod_{i\in a} s_i$. We get that:

$$y^b = \prod_{i\in b} y_i = \prod_{i\in b}(s_i + 1) = \sum_{a\subseteq b} s^a \text{ and by the Möbius inversion formula } s^b = \sum_{a\subseteq b} y^a.$$

Proposition 22. Consider maps $D : \mathrm{P}[n] \times \mathrm{P}[n] \to \mathbb{Z}_2$ and $f : \mathrm{P}[n] \to \mathbb{Z}_2$.

1. Let $D = \sum_{a,b\in\mathrm{P}[n]} D(a,b)m^a s^b \in \mathrm{BDO}_n$, $f = \sum_{c\in\mathrm{P}[n]} f(c)m^c \in \mathbb{Z}_2[\mathbb{A}^n]$, and $Df = \sum_{a\in\mathrm{P}[n]} Df(a)m^a$. Then we have that
$$Df(a) = \sum_{b\in\mathrm{P}[n]} D(a,b)f(a+b).$$

2. Let $D = \sum_{a,b\in\mathrm{P}[n]} D_x(a,b)x^a s^b \in \mathrm{BDO}_n$, $f = \sum_{c\in\mathrm{P}[n]} f_x(c)x^c \in \mathbb{Z}_2[\mathbb{A}^n]$, and $Df = \sum_{d\in\mathrm{P}[n]} Df_x(d)x^d$. Then
$$Df_x(d) = \sum_{\substack{a,\ e\subseteq b\cap c \\ a\cup(c\setminus e)=d}} D_x(a,b)f_x(c).$$

Proof.

1. $Df = \sum_{a,b,c\in\mathrm{P}[n]} D(a,b)f(c)m^a s^b m^c = \sum_{a,b,c} D(a,b)f(c)m^a m^{b+c} = \sum_{a,b} D(a,b)f(a+b)m^a$
$= \sum_{a\in\mathrm{P}[n]} \left(\sum_{b\in\mathrm{P}[n]} D(a,b)f(a+b)\right) m^a.$

2. $Df = \sum_{a,b,c\in\mathrm{P}[n]} D_x(a,b)f_x(c)x^a s^b x^c = \sum_{a,e\subseteq b\cap c} D_x(a,b)f_x(c)x^{a\cup c\setminus e}$

$$= \sum_{d \in \mathrm{P}[n]} \left(\sum_{\substack{a,\ e \subseteq b \cap c \\ a \cup (c \setminus e) = d}} D_x(a,b) f_x(c) \right) x^d.$$

□

Proposition 22 and Theorem 7 provide a couple of explicit ways of identifying BDO_n with $\mathrm{M}_{2^n}(\mathbb{Z}_2)$ the algebra of square matrices of size 2^n with coefficients in $\mathbb{Z}_2$. Consider the $\mathbb{Z}_2$-linear map $\mathrm{R} : \mathrm{BDO}_n \to \mathrm{M}_{2^n}(\mathbb{Z}_2)$ sending $m^a s^b$ to $\mathrm{R}(m^a s^b)$ the matrix of $m^a s^b$ on the basis m^a. The action of $m^a s^b$ on m^c is given by $m^a s^b m^c = m^a$ if $c = a + b$ and 0 otherwise. Therefore, the matrix $\mathrm{R}(m^a s^b)$ is given for $c, d \in \mathrm{P}[n]$ by the rule

$$\mathrm{R}(m^a s^b)_{c,d} = \begin{cases} 1 & \text{if } c = a \text{ and } \ d = a + b \\ 0 & \text{otherwise} \end{cases}$$

Example 23. The graph of the matrix $\mathrm{R}(m^a s^b)_{c,d}$ is shown in Figure 3.

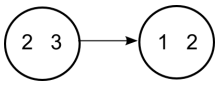

Figure 3: Graph of the matrix $\mathrm{R}(m^{\{1,2\}} \partial^{\{2,3\}})$.

For a second representation consider $\mathbb{Z}_2$-linear the map $\mathrm{S} : \mathrm{BDO}_n \to \mathrm{M}_{2^n}(\mathbb{Z}_2)$ sending $x^a s^b$ to $\mathrm{S}(x^a s^b)$, the matrix of $x^a s^b$ on the basis x^a. The action of $x^a s^b$ on x^c is given by

$$x^a s^b x^c = \sum_{e \subseteq b \cap c} x^{a \cup c \setminus e}.$$

Therefore, the matrix $\mathrm{S}(x^a s^b)$ is given for $c, d \in \mathrm{P}[n]$ by the rule

$$\mathrm{S}(x^a s^b)_{c,d} = \begin{cases} 1 & \text{if} \quad O\{e \subseteq b \cap d \mid c = a \cup d \setminus e\} \\ 0 & \text{otherwise} \end{cases}$$

Example 24. The graph of the matrix $\mathrm{S}(x^{\{1,2\}} s^{\{1,3\}})$ is shown in Figure 4.

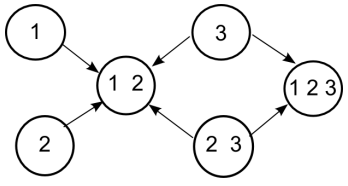

Figure 4: Graph of the matrix $\mathrm{R}(m^{\{1,2\}} \partial^{\{2,3\}})$.

Next we introduce the shifted Boole-Weyl algebra SBW_n, a quite useful and easy to handle presentation for the algebra of Boolean differential operators BDO_n.

Definition 25. The algebra SBW_n is the quotient of $\mathbb{Z}_2 < x_1, ..., x_n, s_1, ..., s_n >$, the free associative $\mathbb{Z}_2$-algebra generated by $x_1, ..., x_n, s_1, ..., s_n$, by the ideal

$$< x_i^2 + x_i,\ x_i x_j + x_j x_i,\ s_i s_j + s_j s_i,\ s_i^2 + 1,\ s_i x_j + x_j s_i,\ s_i x_i + x_i s_i + s_i >,$$

generated by the relations $x_i^2 = x_i,\ s_i^2 = 1$, and $s_i x_i = x_i s_i + s_i$ for $i \in [n]$, $x_i x_j = x_j x_i$ and $y_i y_j = y_j y_i$ for $i, j \in [n]$, and $s_i x_j + x_j s_i$ for $i \neq j \in [n]$.

Theorem 26. The map $\mathbb{Z}_2 < x_1, ..., x_n, s_1, ..., s_n > \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ sending x_i to the operator of multiplication by x_i, and s_i to the shift operator in the i-direction, descends to an isomorphism $\mathrm{SBW}_n \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ of $\mathbb{Z}_2$-algebras.

Proof. The map $\mathbb{Z}_2 < x_1, ..., x_n, s_1, ..., s_n > \to \mathbb{Z}_2 < x_1, ..., x_n, y_1, ..., y_n >$ sending x_i to x_i and s_i to $y_i + 1$ descends to an algebra isomorphisms $\mathrm{SBW}_n \to \mathrm{BW}_n$. The result then follows from Theorem 11. □

Theorem 27. The map $\mathbb{Z}_2 < x_1, ..., x_n, s_1, ..., s_n > \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ sending x_i to the operator of multiplication by $w_i = x_i + 1$, and s_i to the shift operator in the i-direction, descends to an isomorphism $\mathrm{SBW}_n \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ of $\mathbb{Z}_2$-algebras.

Proof. Follows from the fact that w_i and s_j satisfy exactly the same relation as x_i and s_j. □

Corollary 28. Any identity in SBW_n involving x_i and s_j has an associated identity involving w_i and s_j obtained by replacing x_i by w_i.

Lemma 29. For $a, b, c, d \in \mathrm{P}[n]$ the following identities hold in SBW_n :

1. $s^b m^c = m^{b+c} s^b$.
2. $m^a s^b m^c s^d = \delta_{a,b+c} m^a s^{b+d}$.
3. $s^b x^c = \sum_{k \subseteq b \cap c} x^{c \setminus k} s^b$.
4. $x^a s^b x^c s^d = \sum_{e \subseteq b \cap c} x^{a \cup c \setminus e} s^{b+d}$.

Proof. 1. For any $f \in \mathbb{Z}_2[\mathbb{A}^n]$ we have that:

$$(s^b m^c f)(x) = m^c(x + b) f(x + b) = m^{b+c}(x) f(x + b) = m^{b+c} s^b f(x),\ \text{thus } s^b m^c = m^{b+c} s^b.$$

2. $m^a s^b m^c s^d = m^a m^{b+c} s^b s^d = \delta_{a,b+c} m^{b+c} s^{b+d}$.

3. From the identity $s_i x_i = x_i s_i + s_i$ we see that as s_i pass to the right of x_i, it may or may not absorb x_i. The set $k \subseteq b \cap c$ is the set of indices for which x_i is absorbed by s_i.

4. $x^a s^b x^c s^d = \sum_{e \subseteq b \cap c} x^a x^{c \setminus e} s^b s^d = \sum_{e \subseteq b \cap c} x^{a \cup c \setminus e} s^{b+d}$.

□

Example 30.

$$1.\ s^{[n]}m^c = m^{\overline{c}}s^{[n]},\ \ \overline{c} = [n] \setminus c. \qquad 2.\ m^{\overline{c}}s^{[n]}m^c s^d = m^{\overline{c}}s^{\overline{d}}.$$

$$3.\ s^{[n]}x^c = \sum_{k \subseteq c} x^k s^{[n]}. \qquad 4.\ x^a s^{[n]} x^c s^d = \sum_{k \subseteq c} x^{a \cup k} s^{\overline{d}}.$$

From Lemma 2 we see that there are several natural basis for BW_n, namely:

$$\{m^a s^b \mid a, b \in \mathrm{P}[n]\ \}, \quad \{x^a s^b \mid a, b \in \mathrm{P}[n]\ \}, \quad \{w^a s^b \mid a, b \in \mathrm{P}[n]\ \}.$$

We write the coordinates of $f \in \mathrm{SBW}_n$ in these bases as:

$$f = \sum_{a,b \in \mathrm{P}[n]} f_{m,s}(a,b) m^a s^b = \sum_{a,b \in \mathrm{P}[n]} f_{x,s}(a,b) x^a s^b = \sum_{a,b \in \mathrm{P}[n]} f_{w,s}(a,b) w^a s^b.$$

These coordinates systems are connected by the relations:

$$f_{x,s}(b,c) = \sum_{a \subseteq b} f_{m,s}(a,c), \quad f_{m,s}(b,c) = \sum_{a \subseteq b} f_{x,s}(a,c), \quad f_{w,s}(b,c) = \sum_{a \subseteq b} f_{m,s}(\overline{a},c),$$

$$f_{m,s}(b,c) = \sum_{a \subseteq \overline{b}} f_{w,s}(a,c), \quad f_{x,s}(a,c) = \sum_{a \subseteq b} f_{w,s}(b,c), \quad f_{w,s}(a) = \sum_{a \subseteq b} f_{x,s}(b,c).$$

Theorem 31. For $f, g \in \mathrm{SBW}_n$ the following identities hold for $a, b, e, h \in \mathrm{P}[n]$:

1. $(fg)_{m,s}(a,b) = \sum_{c \in \mathrm{P}[n]} f_{m,s}(a,c) g_{m,s}(a+c, b+c)$.
2. $(fg)_{x,s}(e,h) = \sum_{a \subseteq e,\ b,c \in \mathrm{P}[n]} O\{k \subseteq b \cap c \mid a \cup c \setminus k = e\ \} f_{x,s}(a,b) g_{x,s}(c, b+h)$.

Proof. 1. Let $f = \sum_{a,b \in \mathrm{P}[n]} f_{m,s}(a,b) m^a s^b$, $g = \sum_{c,d \in \mathrm{P}[n]} g_{m,s}(c,d) m^c s^d$, then we have that:

$$fg = \sum_{a,b,c,d \in \mathrm{P}[n]} f_{m,s}(a,b) g_{m,s}(c,d) m^a s^b m^c s^d =$$

$$\sum_{b,c,d \in \mathrm{P}[n]} f_{m,s}(b+c,b) g_{m,s}(c,d) m^{b+c} s^{b+d}$$

$$= \sum_{e,f \in \mathrm{P}[n]} \left(\sum_{\substack{b+c=e \\ b+d=f}} f_{m,s}(b+c,b) g_{m,s}(c,d) \right) m^e s^f$$

$$= \sum_{e,f \in \mathrm{P}[n]} \left(\sum_{b \in \mathrm{P}[n]} f_{m,s}(e,b) g_{m,s}(e+b, f+b) \right) m^e s^f.$$

2. Let $f = \sum_{a,b\in \mathrm{P}[n]} f_{x,s}(a,b)x^a s^b$, $g = \sum_{c,d\in \mathrm{P}[n]} g_{x,s}(c,d)x^c s^d$, then we have that:

$$fg = \sum_{a,b,c,d\in \mathrm{P}[n]} f_{x,s}(a,b)g_{x,s}(c,d)x^a s^b x^c s^d$$

$$= \sum_{a,b,c,d\in \mathrm{P}[n],\ k\subseteq b\cap c} f_{x,s}(a,b)g_{x,s}(c,d)x^{a\cup c\setminus k}\, s^{b+d}$$

$$= \sum_{e,h\in \mathrm{P}[n]} \left(\sum_{\substack{a,b,c,d\in \mathrm{P}[n] \\ k\subseteq b\cap c \\ a\cup c\setminus k=e,\ b+d=h}} f_{x,s}(a,b)g_{x,s}(c,d) \right) x^e s^h$$

$$= \sum_{e,h\in \mathrm{P}[n]} \left(\sum_{\substack{a\subseteq e,\ b,c\in \mathrm{P}[n] \\ k\subseteq b\cap c \\ a\cup c\setminus k=e}} f_{x,s}(a,b)g_{x,s}(c,b+h) \right) x^e s^h =$$

$$= \sum_{e,h\in \mathrm{P}[n]} \left(\sum_{a\subseteq e,\ b,c\in \mathrm{P}[n]} O\{k\subseteq b\cap c \mid a\cup c\setminus k = e\ \} f_{x,s}(a,b)g_{x,s}(c,b+h) \right) x^e s^h.$$

□

Example 32. Suppose that $f = \sum_{a,b\in \mathrm{P}[n]} f_{m,s}(a,b)m^a s^b$, and $g = \sum_{c,d\in \mathrm{P}[n]} g_{m,s}(c,d)m^c s^d$, are actually regular functions on $\mathbb{Z}_2^n$, i.e. $f_{m,s}(a,b) = 0$ if $b \neq \emptyset$, and $g_{m,s}(c,d) = 0$ if $d \neq \emptyset$. A non-vanishing term in the formula

$$(fg)_{m,s}(a,b) = \sum_{c\in \mathrm{P}[n]} f_{m,s}(a,c)g_{m,s}(a+c,b+c)$$

must have $c = \emptyset$, and then we must also have that $c = \emptyset + c = \emptyset$, and $a + c = a + \emptyset = a$. Thus in this case the product fg is, as expected, just the pointwise product of functions on $\mathbb{Z}_2^n$.

Example 33. Let $f = \sum_{a,b\in \mathrm{P}[n]} f_{m,s}(a,b)m^a s^b$, and suppose that $g = \sum_{c,d\in \mathrm{P}[n]} g_{m,s}(c,d)m^c s^d$ is such that $g_{m,s}(c,d) = 0$ if $c \neq [n]$. Then a non-vanishing summand in the formula

$$(fg)_{m,s}(a,b) = \sum_{c\in \mathrm{P}[n]} f_{m,s}(a,c)g_{m,s}(a+c,b+c)$$

can only arise for $c = \overline{a}$. Therefore $(fg)_{m,s}(a,b) = f_{m,s}(a,\overline{a})g_{m,s}([n],b+\overline{a})$. For example, we have that

$$\left(\sum_{a\in \mathrm{P}[n]} m^a s^{\overline{a}} \right) \left(\sum_{d\in \mathrm{P}[n]} m^{[n]} s^d \right) = \sum_{a,b\in \mathrm{P}[n]} m^a s^b.$$

As another example consider $f = \sum_{a,b \in \mathrm{P}[n]} m^a s^b$ and $g = m^{[n]} s^{[n]}$. In this case we get that:

$$\left(\sum_{a,b \in \mathrm{P}[n]} m^a s^b \right) \left(m^{[n]} s^{[n]} \right) = \sum_{a \in \mathrm{P}[n]} m^a s^a.$$

6 Logical Viewpoint

In this section we study quantum Boolean algebras from a logical viewpoint. We assume the reader to be familiar with the language of operads and props [2, 10, 11, 13]. First we review the basic principles of classical propositional logic [4] which may be summarized as:

- Propositions are words in a certain language. Propositions are either simple or composite. Let x be the finite set of simple propositions and $\mathbb{P}(x)$ the set of all propositions. Composite propositions are obtained from the simple propositions using the logical connectives. There are several options for the choice of connectives, the most common ones being $\{\vee, \wedge, \rightarrow, \neg\}$.
- A truth function $\widehat{p} : \mathbb{Z}_2^x \rightarrow \mathbb{Z}_2$ is associated to each proposition $p \in \mathbb{P}(x)$, where $\mathbb{Z}_2^x$ is the set of maps from x to $\mathbb{Z}_2$. The map $\mathbb{P}(x) \rightarrow \mathrm{M}(\mathbb{Z}_2^x, \mathbb{Z}_2) = \mathbb{Z}_2[\mathbb{A}^x]$ sending p to $\widehat{p}$ is such that $\widehat{a}$ is the evaluation at a for each $a \in x$, and $\widehat{p \vee q} = \widehat{p} \vee \widehat{p}$, $\widehat{p \wedge q} = \widehat{p} \wedge \widehat{p}$, $\widehat{p \rightarrow q} = \widehat{p} \rightarrow \widehat{p}$, $\widehat{\neg p} = \neg \widehat{p}$, where the action of the connectives on truth functions are induced by the corresponding operations on $\mathbb{Z}_2$.

The map $\mathbb{P}(x) \rightarrow \mathbb{Z}_2[\mathbb{A}^x]$ is surjective, and there is a systematic procedure to tell when two propositions have the same associated truth function. For our purposes, it is convenient to describe $\mathbb{P}(x)$ using the binary connectives . and +, and the constants $0, 1$. In logical terms the product . is the logical conjunction, + the exclusive or, and 0 and 1 represent falsity and truth, respectively.

$\mathbb{P}(x)$ is defined recursively as the set of words in the symbols $a \in x, ., +, 0, 1, (,)$ such that:

- $x \subseteq \mathbb{P}(x)$, $0 \in \mathbb{P}(x)$, and $1 \in \mathbb{P}(x)$.
- If $p, q \in \mathbb{P}(x)$, then (pq) and $(p + q)$ are also in $\mathbb{P}(x)$.

We defined recursively the notion of sub-words on $\mathbb{P}(x)$ as follows. For all $p, q, r \in \mathbb{P}(x)$ we set: p is a sub-word of p; p is a sub-word of (pq) and $(p + q)$; if p is a sub-word of q and q is a sub-word r, then p is a sub-word of r.

Next we define an equivalence relation $\mathbb{R}(x)$, also denoted by $\sim$, on $\mathbb{P}(x)$. Given $p, q \in \mathbb{P}(x)$ we set:

$$p \; \mathbb{R}(x) \; q \quad \text{iff} \quad \widehat{p} = \widehat{q}.$$

The relation $\mathbb{R}(x)$ can be defined in purely syntactic terms as follows: p and q are related iff $p = q$ or there exists a sequence $p_1, ..., p_k$, for some $k \geq 1$, such that $p_1 = p$, and $p_k = q$, and p_{i+1} is obtained from p_i by replacing a sub-word of p_i by an equivalent word according to the following relations:

- Associativity and commutativity for . and +: $p(qr) \sim (pq)r$, $pq \sim qp$, $(p + q) + r \sim p + (q + r)$, $p + q \sim q + p$.
- Distributivity: $p(q + r) \sim pq + pr$.
- Additive and multiplicative units: $0 + p \sim p$ and $1p \sim p$.
- Additive nilpotency: $p + p \sim 0$.
- Multiplicative idempotency: $pp \sim p$.

Let Set be the category of sets and mappings, and set the category of finite sets. Let $\mathrm{BR} : \mathrm{set}^\circ \to \mathrm{set}$ the functor sending x to the free Boolean ring generated by x, i.e. $\mathrm{BR}(x) = \mathrm{P}(x) = \mathbb{Z}_2^x$. For a map $f : x \to y$ the map $\mathrm{BR}(f) : \mathbb{Z}_2^y \to \mathbb{Z}_2^x$ is such that $\mathrm{BR}(f)(g) = g \circ f$ for any $g : y \to \mathbb{Z}_2$. Let $\mathrm{BF} = \mathrm{BR}^2 : \mathrm{set} \to \mathrm{set}$ be the functor given by $\mathrm{BF}(x) = \mathrm{BR}(\mathrm{BR}(x))$. Thus we have that:

$$\mathrm{BF}(x) = \mathrm{BR}(\mathrm{BR}(x)) = \mathbb{Z}_2^{\mathbb{Z}_2^x} = \mathbb{Z}_2[\mathbb{A}^x],$$

i.e. $\mathrm{BF}(x)$ is the ring of Boolean functions on $\mathbb{Z}_2^x$.

Note that the sequence $\{\mathrm{BF}[n] \mid n \geq 0\}$ can be identified with the endomorphism operad of $\mathbb{Z}_2$ in Set, i.e. $\mathrm{BF}[n] = \mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)$ as sets with S_n-actions.

Let $\mathbb{P}$ be the free operad in Set generated by $+, . \in \mathbb{P}(2)$ and $0, 1 \in \mathbb{P}(0)$. For given $x \in \mathrm{set}$, the set of all propositions $\mathbb{P}(x)$ is actually equal to the free $\mathbb{P}$-algebra generated by x.

We also denote by $\mathbb{P}$ the functor $\mathbb{P} : \mathrm{set} \to \mathrm{Set}$ sending x to the $\mathbb{P}(x)$, and $f : x \to y$ to its natural extension $\mathbb{P}(f) : \mathbb{P}(x) \to \mathbb{P}(y)$ sending x to y via f, and respecting the logical connectives.

Let Req be the category of equivalence relations. Objects in Req are pairs (X, R) where R is an equivalence relation on X. A morphism $f : (X, R) \to (Y, S)$ in Req is a map $f : X \to Y$ such that $fR \subseteq S$. We have a functor $\mathrm{Req} \to \mathrm{Set}$ sending (X, R) to the quotient set X/R.

The pair $(\mathbb{P}, \mathbb{R})$ yields a functor $(\mathbb{P}, \mathbb{R}) : \mathrm{set} \to \mathrm{Req}$, sending x to $(\mathbb{P}(x), \mathbb{R}(x))$, and the corresponding functor $\mathbb{P}/\mathbb{R} : \mathrm{set} \to \mathrm{set}$. Moreover, the results of Section 2 imply the identification

$$\mathbb{P}/\mathbb{R} = \mathrm{BF}, \text{ in particular, } \mathbb{P}(x)/\mathbb{R}(x) = \mathbb{Z}_2[\mathbb{A}^x] \text{ as Boolean rings.}$$

Note also that we obtain a purely syntactic description of the operad $\{\mathrm{BF}[n] \mid n \geq 0\}$ as

$$\{\mathbb{P}[n]/\mathbb{R}[n] \mid n \geq 0\}.$$

Classical logic main concern is the pre-order $\vdash$ of entailment on $\mathbb{P}(x)$. Recall that $\mathbb{Z}_2[\mathbb{A}^x]$ is a poset with $f \leq g$ if $f(a) \leq g(a)$ for all $a \in \mathbb{Z}_2^x$.

For $p, q \in \mathbb{P}(x)$, we set $p \vdash q$ iff $\widehat{p} \leq \widehat{q}$, or equivalently, iff there is $r \in \mathbb{P}(x)$ such that $\widehat{p} = \widehat{q}\widehat{r}$. The entailment relation $\vdash$ can be defined syntactically terms as follows:

$$p \vdash q \quad \text{iff there exists } r \in \mathbb{P}(x) \text{ such that } \ p \sim qr.$$

Next we move from the classical to the quantum situation. As mentioned in the introduction, quantum observables are operators instead of propositions. In analogy with the classical case we identify operators with words in a certain language. Truth functions are replaced by Boolean differential operators. We think of quantum logic as arising from the following principles:

- We find again the simple/composite dichotomy. For a set x we let $\widetilde{x} = \{\widetilde{a} \mid a \in x\}$ be a set disjoint from x whose elements are of the form $\widetilde{a}$ for $a \in x$. Given x we let $\mathbb{O}(x)$ be the set of all quantum observables; $\mathbb{O}(x)$ is a set of words in a certainly language to be specified below. Elements of $\mathbb{O}(x)$ are called operators. The set of operators $\mathbb{O}(x)$ is obtained from the set of simple operators $x \sqcup \widetilde{x} \subseteq \mathbb{O}(x)$ using the binary connectives product . and sum $+$, and the constants $0, 1$; i.e. $\mathbb{O}(x)$ is defined recursively as the set of words in the symbols $a \in x \sqcup \widetilde{x}, ., +, 0, 1, (,)$ such that:
  - $x \sqcup \widetilde{x} \subseteq \mathbb{O}(x)$, $0 \in \mathbb{O}(x)$, and $1 \in \mathbb{O}(x)$.
  - If $p, q \in \mathbb{O}(x)$, then (pq) and $(p + q)$ are also in $\mathbb{O}(x)$.
- The logical interpretation of the connectives . and $+$ are as follows. The product pq correspond with the logical AND, but there is also a temporal dimension to it: pq may be interpreted as "act with the operator q, and then act with the operator p." The connective $+$ correspond to XOR, the exclusive or. The constants 0 and 1 may be interpreted as: "reset to 0" and "leave it as it is".
- Let $\mathrm{BDO}_x = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x]) = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[a \mid a \in x])$ be the algebra of Boolean differential operators on $\mathbb{Z}_2^x$. We think of BDO_x as the quantum analogue of the Boolean algebra $\mathbb{Z}_2[\mathbb{A}^x]$ of truth functions. Just as we have a map from propositions to truth functions, we have a map $\mathbb{O}(x) \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$ from operators to Boolean differential operators given by:
  - $\widehat{a}$ is the operator of multiplication by a, for $a \in x$.
  - $\widehat{\widetilde{a}}$ is ∂_a the Boolean derivative along a, for $a \in x$.

– $\widehat{p+q} = \widehat{p} + \widehat{q}$ and $\widehat{p}\widehat{q} = \widehat{p}\widehat{q}$ for $p, q \in \mathbb{O}(x)$.

– $\widehat{0} = 0$, the operator identically equal to 0, and $\widehat{1}$ is the identity operator.

We think of the composition $\circ$ of operators in $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$ as the quantum analogue of the meet $\wedge$, or equivalently the product, on $\mathbb{Z}_2[\mathbb{A}^x] = \mathrm{M}(\mathbb{Z}_2^x, \mathbb{Z}_2)$. Indeed $\circ$ is an extension of the classical meet. Consider the inclusion map $\mathbb{Z}_2[\mathbb{A}^x] \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$ sending $f \in \mathbb{Z}_2[\mathbb{A}^x]$ into the operator of multiplication by f. This map is additive and multiplicative, thus showing that the quantum structures are, as they should, an extension of the classical ones.

The map $\mathbb{O}(x) \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$ turns out to be surjective, and there is a well-defined procedure to tell when two operators are assigned the same Boolean differential operator. Sub-words are defined in $\mathbb{O}(x)$ as in the classical. We define an equivalence relation $\mathbb{R}(x)$, also denoted by $\sim$, on $\mathbb{O}(x)$. For $p, q \in \mathbb{O}(x)$ we set:

$$p \; \mathbb{R}(x) \; q \quad \text{iff} \quad \widehat{p} = \widehat{q}.$$

$\mathbb{R}(x)$ is defined syntactically as follows: p and q are related iff $p = q$ or there exists a sequence $p_1, ..., p_k$, for some $k \geq 1$, such that $p_1 = p$, and $p_k = q$, and p_{i+1} is obtained from p_i by replacing a sub-word of p_i by an equivalent word according to the following relations:

- Associativity for the product: $p(qr) \sim (pq)r$.
- Associativity and commutativity for $+$: $(p+q)+r \sim p+(q+r)$, $p+q \sim q+p$.
- Distributivity: $p(q+r) \sim pq + pr$.
- Additive and multiplicative units: $0 + p \sim p$ and $1p \sim p$
- Additive nilpotency: $p + p \sim 0$.
- Multiplicative idempotency and nilpotency: $aa \sim a$ and $\widetilde{a}\widetilde{a} \sim 0$, for $a \in x$.
- Commutation relations: $ba \sim ab$ and $\widetilde{a}\widetilde{b} \sim \widetilde{b}\widetilde{a}$, for $a, b \in x$, $\widetilde{b}a \sim a\widetilde{b}$ for $a \neq b \in x$, and $\widetilde{a}a \sim a\widetilde{a} + \widetilde{a} + 1$ for $a \in x$.

Let $\mathbb{B}$ be the category of finite sets and bijections [9]. We regard $\mathbb{O}, \mathbb{R}$, and $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^{(\ )}])$ as functors $\mathbb{B} \to \mathrm{Set}$. The pair $(\mathbb{O}, \mathbb{R})$ defines a functor $(\mathbb{O}, \mathbb{R}) : \mathbb{B} \to \mathrm{Req}$. The results of Section 4 imply the following identification

$$\mathbb{O}/\mathbb{R} = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^{(\ )}]) \quad \text{in particular} \quad \mathbb{O}(x)/\mathbb{R}(x) = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x]).$$

Next we define the quantum entailment pre-order $\vdash$ on $\mathbb{O}(x)$. First we define a pre-order on $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$; for $S, T \in \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^x])$ we set

$$S \leq T \quad \text{iff there exists } R \text{ such that } S = TR.$$

For example, if S and T are projections onto the subspaces A and B of $\mathbb{Z}_2[\mathbb{A}^x]$, respectively, then $S \leq T$ iff $A \subseteq B$.

For $p, q \in \mathbb{O}(x)$, we set $p \vdash q$ iff there is $r \in \mathbb{O}(x)$ such that $\widehat{p} = \widehat{qr}$. Equivalently, the entailment relation $\vdash$ can be defined syntactically as:

$$p \vdash q \quad \text{iff} \quad \text{there is } r \in \mathbb{O}(x) \text{ such that } p \sim qr.$$

As expected, quantum entailment is an extension of classical entailment. Indeed, we have functors $(\mathbb{P}, \vdash)$, $(\mathbb{O}, \vdash)$, $(\mathbb{Z}_2[\mathbb{A}^{(\ )}], \leq)$, $(\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^{(\ )}]), \leq)$ from $\mathbb{B}$ to the category of pre-ordered sets. These functors fit into the following commutative diagram of natural transformations:

$$\begin{array}{ccc} (\mathbb{P}, \vdash) & \longrightarrow & (\mathbb{O}, \vdash) \\ \downarrow & & \downarrow \\ (\mathbb{Z}_2[\mathbb{A}^{(\ )}], \leq) & \longrightarrow & (\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^{(\ )}]), \leq) \end{array}$$

where the top horizontal arrow is the natural inclusion, the bottom horizontal arrow sends f into the operator of multiplication by f, and the vertical arrows are the valuation maps from propositions and operators to truth functions and differential operators, respectively.

Our previous considerations yield a syntactic presentation of the diagonal of the endomorphism prop of $\mathbb{Z}_2[\mathbb{A}^1]$ in the category $\mathbb{Z}_2$-vect. Indeed we have that:

$$\mathbb{O}[n]/\mathbb{R}[n] = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n]) = \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^1]^{\otimes n}).$$

7 Set Theoretical Viewpoint

The link between classical propositional logic and the algebra of sets arises as follows. Recall that there is a map $\mathbb{P}(x) \to \mathrm{M}(\mathbb{Z}_2^x, \mathbb{Z}_2)$ sending each proposition to its truth function. Since $\mathrm{M}(\mathbb{Z}_2^x, \mathbb{Z}_2)$ can be identified with $\mathrm{PP}(x)$ we obtain a map $\mathbb{P}(x) \to \mathrm{PP}(x)$ assigning to each proposition p a set $\widehat{p}$ of subsets of x. Moreover, the logical connectives intertwine nicely with the set theoretical operations on subsets, namely:

$$\widehat{p + q} = (\widehat{p} \cup \widehat{q}) \setminus (\widehat{p} \cap \widehat{q}), \quad \widehat{pq} = \widehat{p \wedge q} = \widehat{p} \cap \widehat{q}, \quad \widehat{\neg p} = \overline{\widehat{p}}, \quad \widehat{p \vee q} = \widehat{p} \cup \widehat{q} \quad \widehat{p \to q} = \overline{\widehat{p}} \cup \widehat{q}.$$

We stress the, often overlooked, fact that classical propositional logic describes the set theoretical operations present in $\mathrm{PP}(x)$ that are common to all sets of the form $\mathrm{P}(y)$, i.e. the extra algebraic structures present in $\mathrm{P}(y)$ when $y = \mathrm{P}(x)$ play no significative role in the logic/set theory relation outlined above. This is why whereas $\mathrm{P}(x)$ have been massively studied, the algebraic structures on $\mathrm{P}^n(x)$, for $n \geq 2$, have seldom attracted any attention.

We proceed to consider the analogue statements in the quantum scenario. We present our results for sets of the form $[n]$. It should be clear, however, that the same constructions apply for arbitrary finite sets.

As in the classical case we have a map $\mathbb{O}_n \to \mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ sending operators (words in a certain language) to Boolean differential operators. As shown in Section 4 it is possible to identify $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n])$ with the Boolean-Weyl algebra BW_n, and with the symmetric Boolean-Weyl algebra SBW_n. Moreover, we described several explicit bases for these algebras. For example, each $f \in \mathrm{BW}_n$ can be written in an unique way as:

$$f = \sum_{a,b \in \mathrm{P}[n]} f(a,b) x^a y^b.$$

Thus Boolean differential operators can be identified with maps from $\mathrm{P}[n] \times \mathrm{P}[n]$ to $\mathbb{Z}_2$, and we get the identifications:

$$\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n]) \simeq \mathrm{BDO}_n \simeq \mathrm{BW}_n \simeq \mathrm{M}(\mathrm{P}[n] \times \mathrm{P}[n], \mathbb{Z}_2) \simeq \mathrm{P}(\mathrm{P}[n] \times \mathrm{P}[n]) \simeq \mathrm{PP}([n] \sqcup [n]).$$

We adopt the following conventions. We identify $[n] \sqcup [n]$ with the set

$$[n, \widetilde{n}] = \{1, 2, ..., n, \widetilde{1}, \widetilde{2}, ..., \widetilde{n}\}.$$

Given $a \subseteq [n]$ we let $\widetilde{a} = \{\widetilde{i} \mid i \in a\}$ be the corresponding subset of $[\widetilde{n}] = \{\widetilde{1}, \widetilde{2}, ..., \widetilde{n}\}$. An element $a \in \mathrm{P}[n, \widetilde{n}]$ will be written as $a = a_1 \sqcup \widetilde{a}_2$ with $a_1, a_2 \in \mathrm{P}[n]$. Note that we have a natural map $\pi : \mathrm{P}[n, \widetilde{n}] \to \mathrm{P}[n] \times \mathrm{P}[n]$ given by $\pi(a) = (\pi_1(a), \pi_2(a)) = (a_1, a_2)$. We use indices without tilde to denote monomials of regular functions, and indices with tilde to denote the Boolean derivatives or shift operators. The identification $\mathrm{End}_{\mathbb{Z}_2}(\mathbb{Z}_2[\mathbb{A}^n]) = \mathrm{PP}[n, \widetilde{n}]$ allow us to give set theoretical interpretations to the algebraic structures on Boolean differential operators. Unlike the classical case, the quantum structures are not defined for an arbitrary sets of the form $\mathrm{P}(y)$, quite the contrary, they very much depend on the fact that $y = \mathrm{P}[n, \widetilde{n}]$.

Below we consider pairs (A, M) where A is a $\mathbb{Z}_2$-algebra and M is an A-module. A morphism $(f, g) : (A_1, M_1) \to (A_2, M_2)$ between such pairs, is given by $\mathbb{Z}_2$-linear maps $f : A_1 \to A_2$ and $g : M_1 \to M_2$ such that f is an algebra morphism, and $g(am) = f(a)g(m)$ for all $a \in A, m \in M$.

The additive structure $+ : \mathrm{PP}[n, \widetilde{n}] \times \mathrm{PP}[n, \widetilde{n}] \to \mathrm{PP}[n, \widetilde{n}]$ on $\mathrm{PP}[n, \widetilde{n}]$ is given by

$$A + B = A \cup B \setminus (A \cap B).$$

We consider several isomorphic products $\circ, \bullet, \star$, and $*$ on $\mathrm{PP}[n, \widetilde{n}]$ displaying different combinatorial properties. The various products correspond with the various bases for BW_n and SBW_n.

Theorem 34. There are maps $\circ : \mathrm{PP}[n,\widetilde{n}] \times \mathrm{PP}[n,\widetilde{n}] \to \mathrm{PP}[n,\widetilde{n}]$ and $\circ : \mathrm{PP}[n,\widetilde{n}] \times \mathrm{PP}[n] \to \mathrm{PP}[n]$, turning $\mathrm{PP}[n,\widetilde{n}]$ into a $\mathbb{Z}_2$-algebra and $\mathrm{PP}[n]$ into a module over $\mathrm{PP}[n,\widetilde{n}]$, such that the pair $(\mathrm{PP}[n,\widetilde{n}], \mathrm{PP}[n])$ is isomorphic to $(\mathrm{End}_{\mathbb{Z}_2}(\mathrm{M}(\mathbb{Z}_2^n,\mathbb{Z}_2)), \mathrm{M}(\mathbb{Z}_2^n,\mathbb{Z}_2))$ via the maps

$$A \to \sum_{a\in A} m^{a_1}\partial^{a_2} \quad \text{and} \quad F \to \sum_{a\in F} m^a.$$

Proof. From Theorem 17 and Proposition 6 we see that the desired products $\circ$ are constructed as follows. For $A, B \in \mathrm{PP}[n,\widetilde{n}]$, the product $AB \in \mathrm{PP}[n,\widetilde{n}]$ is given by

$$A \circ B = \left\{ a \in \mathrm{P}[n,\widetilde{n}] \mid O\{b \in \mathrm{P}[n], c \in B \mid c_2 \subseteq a_2,\ a_1 \sqcup \widetilde{b} \in A,\ a_2 \setminus c_2 \subseteq a_1 + c_1 \subseteq b\} \right\}.$$

Let $A \in \mathrm{PP}[n,\widetilde{n}]$ and $F \in \mathrm{PP}[n]$, then $AF \in \mathrm{PP}[n]$ is given by

$$A \circ F = \{\ a \in \mathrm{P}[n] \ \mid\ O\{b \subseteq c \in \mathrm{P}[n] \mid a \sqcup \widetilde{c} \in A,\ a+b \in F\}\ \}.$$

□

Example 35. In $\mathrm{PP}[3,\widetilde{3}]$ we have that $\{\{1,2,\overline{2},\overline{3}\}\} \circ \{\{1,3,\overline{1},\overline{2}\}\} = \{\{1,2,\overline{1},\overline{2}\},\ \{1,2,\overline{1},\overline{2},\overline{3}\}\}$. Indeed $a \in \{\{1,2,\overline{2},\overline{3}\}\} \circ \{\{1,3,\overline{1},\overline{2}\}\}$ if there is a odd number of pairs b, c with certain properties. Note that $c = \{1,3,\overline{1},\overline{2}\}$, $\{1,2\} \subseteq a_2$, $a_1 \sqcup \widetilde{b} = \{1,2,\overline{2},\overline{3}\}$, and thus necessarily $a_1 = \{1,2\}$ and $b = \{2,3\}$. Moreover, we must have that $a_2 \setminus \{1,2\} \subseteq \{1,2\} + \{1,3\} \subseteq \{2,3\}$, that is $a_2 \setminus \{1,2\} \subseteq \{2,3\}$. Thus either $a_2 = \{1,2\}$ or $a_2 = \{1,2,3\}$ yielding the desired result.

Example 36. For $A \in \mathrm{PP}[n]$ set $A' = \pi_2^{-1}(A)$. Let $F \in \mathrm{PP}[n]$, the we have that:

$$A' \circ F = \{\ a \in \mathrm{P}[n] \ \mid\ O\{b \subseteq c \in \mathrm{P}[n] \mid \widetilde{c} \in A,\ a+b \in F\}\ \}.$$

Note that $\sum_{a\in \mathrm{P}[n]} m^a = 1$ and thus:

$$\left(\sum_{a\in A} \partial^a\right) \circ \left(\sum_{b\in F} m^b\right) = \sum_{a\in A'\circ F} m^a.$$

Example 37. For $A \in \mathrm{PP}[n]$ let $\widehat{A} = \{a \in \mathrm{P}[n,\widetilde{n}] \mid a_1 = a_2 \in A\ \}$. Let $F \in \mathrm{PP}[n]$, then

$$\widehat{A} \circ F = \{\ a \in \mathrm{P}[n] \ \mid\ O\{e \subseteq a \mid\ a+e \in F\}\ \} \quad \text{and therefore}$$

$$\left(\sum_{a\in A} m^a\partial^a\right) \circ \left(\sum_{b\in F} m^b\right) = \sum_{a\in \widehat{A}\circ F} m^a.$$

Theorem 38. There are maps $\bullet : \mathrm{PP}[n,\widetilde{n}] \times \mathrm{PP}[n,\widetilde{n}] \to \mathrm{PP}[n,\widetilde{n}]$ and $\bullet : \mathrm{PP}[n,\widetilde{n}] \times \mathrm{PP}[n] \to \mathrm{PP}[n]$ such that the pair $(\mathrm{PP}[n,\widetilde{n}], \mathrm{PP}[n])$ is isomorphic to $(\mathrm{End}_{\mathbb{Z}_2}(\mathrm{M}(\mathbb{Z}_2^n,\mathbb{Z}_2)), \mathrm{M}(\mathbb{Z}_2^n,\mathbb{Z}_2))$ via the maps

$$A \to \sum_{a\in A} x^{a_1}\partial^{a_2} \quad \text{and} \quad F \to \sum_{a\in F} x^a.$$

Proof. From Theorem 17 and Proposition 6 we see that the desired products $\bullet$ are constructed as follows. For $A, B \in \mathrm{PP}[n, \widetilde{n}]$, the product $A \bullet B \in \mathrm{PP}[n, \widetilde{n}]$ is such that $a \in A \bullet B$ iff

$$O\{b \in A, c \in B, k_1 \subseteq k_2 \mid b_1 \subseteq a_1,\ c_1 \subseteq a_2,\ k_2 \subseteq b_2 \cap c_1,\ b_1 \cup (c_1 \setminus k_2) = a_1,\ b_2 \setminus k_1 = a_2 \setminus c_2\}.$$

Let $A \in \mathrm{PP}[n, \widetilde{n}]$ and $F \in \mathrm{PP}[n]$, then $A \bullet F \in \mathrm{PP}[n]$ is given by

$$A \bullet F = \{\ a \in \mathrm{P}[n]\ \mid\ O\{b \in A, c \in F \mid b_2 \subseteq c,\ b_1 \cup (c \setminus b_2) = a\}\ \}\,.$$

□

Example 39. In $\mathrm{PP}[3, \widetilde{3}]$ we have that $\{\{1,3,\overline{2}\}\}\bullet\{\{2,\overline{1}\}\} = \{\{1,2,3,\overline{1},\overline{2}\},\{1,3,\overline{1},\overline{2}\},\{1,3,\overline{1}\}\}$. Indeed, we must have $b = \{1,3,\overline{2}\}$ and $c = \{2,\overline{1}\}$, and thus there are three options for $k_1 \subseteq k_2 \subseteq [2]$, namely, $\emptyset \subseteq \emptyset$, $\emptyset \subseteq \{2\}$, and $\{2\} \subseteq \{2\}$ giving rise to the sets $\{1,2,3,\overline{1},\overline{2}\}, \{1,3,\overline{1},\overline{2}\}, \{1,3,\overline{1}\}$, respectively.

Example 40. For $A \in \mathrm{PP}[n]$ set $A' = \pi^{-1}(\{\emptyset\} \times A)$. Let $F \in \mathrm{PP}[n]$ then we have that:

$$A' \bullet F = \{\ a \in \mathrm{P}[n]\ \mid\ O\{b \in A, c \in F \mid b \subseteq c,\ c \setminus b = a\}\ \}$$

Therefore we get that

$$\left(\sum_{a \in A} \partial^a\right) \circ \left(\sum_{b \in F} x^b\right) = \sum_{a \in A' \bullet F} x^a.$$

Example 41. For $A \in \mathrm{PP}[n]$ let $\widehat{A} = \{a \in \mathrm{P}[n, \widetilde{n}] \mid a_1 = a_2 \in A\ \}$. Let $F \in \mathrm{PP}[n]$, then

$$\widehat{A} \bullet F = \{\ a \in F\ \mid\ O\{b \in A \mid\ b \subseteq a\}\ \} \quad \text{and therefore}$$

$$\left(\sum_{a \in A} x^a \partial^a\right) \circ \left(\sum_{b \in F} x^b\right) = \sum_{a \in \widehat{A} \bullet F} x^a = \sum_{a \in F} O\{b \in A \mid b \subseteq a\} x^a.$$

In particular we have that: $\widehat{\mathrm{P}[n]} \bullet \mathrm{P}[n] = \{\emptyset\}$ and thus

$$\left(\sum_{a \in \mathrm{P}[n]} x^a \partial^a\right) \circ \left(\sum_{b \in \mathrm{P}[n]} x^b\right) = 1.$$

Theorem 42. There are maps $\star : \mathrm{PP}[n, \widetilde{n}] \times \mathrm{PP}[n, \widetilde{n}] \to \mathrm{PP}[n, \widetilde{n}]$ and $\star : \mathrm{PP}[n, \widetilde{n}] \times \mathrm{PP}[n] \to \mathrm{PP}[n]$, turning $\mathrm{PP}[n, \widetilde{n}]$ into a $\mathbb{Z}_2$-algebra and $\mathrm{PP}[n]$ into a module over $\mathrm{PP}[n, \widetilde{n}]$, such that the pair $(\mathrm{PP}[n, \widetilde{n}], \mathrm{PP}[n])$ is isomorphic to $(\mathrm{End}_{\mathbb{Z}_2}(\mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)), \mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2))$ via the maps

$$A \to \sum_{a \in A} m^{a_1} s^{a_2} \quad \text{and} \quad F \to \sum_{a \in F} m^a.$$

Proof. From Theorem 31 and Proposition 22 we see that the desired products $\star$ are constructed as follows. For $A, B \in \mathrm{PP}[n, \widetilde{n}]$, the product $A \star B \in \mathrm{PP}[n, \widetilde{n}]$ is given by

$$A \star B = \left\{ a \in \mathrm{P}[n, \widetilde{n}] \mid O\{b \in \mathrm{P}[n] \mid a_1 \sqcup \widetilde{b} \in A,\ \widetilde{(a_1 + b) \sqcup (a_2 + b)} \in B\} \right\}.$$

Let $A \in \mathrm{PP}[n, \widetilde{n}]$ and $F \in \mathrm{PP}[n]$, then $A \star F \in \mathrm{PP}[n]$ is given by

$$A \star F = \left\{ a \in \mathrm{P}[n] \ \mid \ O\{b \in \mathrm{P}[n] \mid a \sqcup \widetilde{b} \in A,\ a + b \in F\} \right\}.$$

□

Example 43. In $\mathrm{PP}[3, \widetilde{3}]$ we have that $\{\{1, 2, 3, \overline{3}\}\} \star \{\{1, 2, \overline{2}, \overline{3}\}\} = \{\{1, 2, 3, \overline{2}\}\}$. From the equation $a_1 \sqcup \widetilde{b} \in A$ we see that $a_1 = \{1, 2, 3\}$ and $b = \{3\}$. Also we must have $a_1 + \{3\} = \{1, 2\}$, which holds, and $a_2 + \{3\} = \{2, 3\}$ which implies that $a_2 = \{2\}$.

Example 44. For $A \in \mathrm{PP}[n]$ set $A' = \pi_2^{-1}(A)$. Let $F \in \mathrm{PP}[n]$, the we have that:

$$A' \star F = \{a \in \mathrm{P}[n] \ \mid \ O\{b \in A \mid a + b \in F\} \ \}.$$

Therefore

$$\left(\sum_{a \in A} s^a\right) \circ \left(\sum_{b \in F} m^b\right) = \sum_{a \in A' \star F} m^a \quad \text{in particular} \quad \left(\sum_{a \in A} s^a\right) \circ \left(\sum_{b \in \mathrm{P}[n]} m^b\right) = OA \sum_{a \in \mathrm{P}[n]} m^a.$$

Example 45. For $A \in \mathrm{PP}[n]$ set $\widehat{A} = \{a \in \mathrm{P}[n, \widetilde{n}] \mid a_1 = a_2 \in A\ \}$. Let $F \in \mathrm{PP}[n]$, then $\widehat{A} \star F = \emptyset$ if $\emptyset \notin F$ and $\widehat{A} \star F = A$ if $\emptyset \in F$. Therefore

$$\left(\sum_{a \in A} m^a s^a\right) \circ \left(\sum_{b \in F} m^b\right) = c \sum_{a \in A} m^a,$$

where $c = 1$ if $\emptyset \in F$ and $c = 0$ if $\emptyset \notin F$.

Example 46. Let $\widehat{A}$ be as in the previous example, then $\widehat{A} \star \widehat{A} = \widehat{A}$ if $\emptyset \in A$ and $\widehat{A} \star \widehat{A} = \emptyset$ otherwise. Indeed, $a \in \mathrm{P}[n, \widetilde{n}]$ belongs to $\widehat{A} \star \widehat{A}$ if $a_1 \sqcup \widetilde{b} \in \widehat{A}$, i.e. $a_1 = b \in A$, and $\widetilde{(a_1 + b) \sqcup (a_2 + b)} \in \widehat{A}$, i.e. $\emptyset \in A$ and $a_1 = a_2 \in A$.

Example 47. For $A \in \mathrm{PP}[n]$ set $\widetilde{A} = \{a \in \mathrm{P}[n, \widetilde{n}] \mid \overline{a_1} = a_2 \in A\ \}$. Then $\widetilde{A} \star \widetilde{A} = \widetilde{A}$ if $[n] \in A$ and $\widehat{A} \star \widehat{A} = \emptyset$ if $\widetilde{[n]} \notin A$. Indeed, $a \in \mathrm{P}[n, \widetilde{n}]$ belongs to $\widetilde{A} \star \widetilde{A}$ if $a_1 \sqcup \widetilde{b} \in \widetilde{A}$, i.e. $\overline{a}_1 = b \in A$, and $\widetilde{(a_1 + b) \sqcup (a_2 + b)} \in \widehat{A}$, i.e. $[n] \in A$ and $a_2 = \emptyset + b = b = \overline{a}_1$.

Theorem 48. There are maps $* : \mathrm{PP}[n, \widetilde{n}] \times \mathrm{PP}[n, \widetilde{n}] \to \mathrm{PP}[n, \widetilde{n}]$ and $* : \mathrm{PP}[n, \widetilde{n}] \times \mathrm{PP}[n] \to \mathrm{PP}[n]$, turning $\mathrm{PP}[n, \widetilde{n}]$ into a $\mathbb{Z}_2$-algebra and $\mathrm{PP}[n]$ into a module over $\mathrm{PP}[n, \widetilde{n}]$, such that the pair $(\mathrm{PP}[n, \widetilde{n}], \mathrm{PP}[n])$ is isomorphic to $(\mathrm{End}_{\mathbb{Z}_2}(\mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2)), \mathrm{M}(\mathbb{Z}_2^n, \mathbb{Z}_2))$ via the maps

$$A \to \sum_{a \in A} x^{a_1} s^{a_2} \quad \text{and} \quad F \to \sum_{a \in F} x^a.$$

Proof. From Theorem 31 and Proposition 22 we see that the desired products $\star$ are constructed as follows. For $A, B \in \mathrm{PP}[n, \widetilde{n}]$, the product $A * B \in \mathrm{PP}[n, \widetilde{n}]$ is given by

$$\left\{ a \in \mathrm{P}[n, \widetilde{n}] \mid O\{b, c, d, e \in \mathrm{P}[n] \mid e \subseteq c \cap d,\ b \cup d \setminus e = a_1,\ b \sqcup \widetilde{c} \in A,\ d \sqcup \widetilde{(c + a_2)} \in B\} \right\}.$$

Let $A \in \mathrm{PP}[n, \widetilde{n}]$ and $F \in \mathrm{PP}[n]$, then $A * F \in \mathrm{PP}[n]$ is given by

$$A * F = \left\{ \ a \in \mathrm{P}[n] \ \mid \ O\{b, c, d \in \mathrm{P}[n], e \in F \mid c \subseteq d \cap e,\ b \cup e \setminus c = a,\ b \sqcup \widetilde{d} \in A \ \} \ \right\}.$$

□

Example 49. In $\mathrm{PP}[3, \widetilde{3}]$ we have that $\{\{1, \overline{2}\}\} * \{\{2, 3, \overline{1}, \overline{2}\}\} = \{\{1, 3, \overline{1}\}, \{1, 2, 3, \overline{1}\}\}$. Indeed we must have $b = \{1\}$, $c = \{2\}$, $d = \{2, 3\}$, and $a_2 = \{2\} + \{1, 2\} = \{1\}$. Since $e \subseteq \{2\} \cap \{2, 3\} = \{2\}$, there are two options, either $e = \emptyset$ and then $a_1 = \{1, 2, 3\}$ and $a = \{1, 2, 3, \overline{1}\}$, or $e = \{2\}$ and then $a_1 = \{1, 3\}$ and $a = \{1, 3, \overline{1}\}$.

Example 50. For $A \in \mathrm{PP}[n]$ set $A' = \pi^{-1}(\{\emptyset\} \times A)$. Let $F \in \mathrm{PP}[n]$ then we have that:

$$A' * F = \{ \ a \in \mathrm{P}[n] \ \mid \ O\{c \in \mathrm{P}[n], d \in A, e \in F \mid c \subseteq d \cap e,\ e \setminus c = a\} \ \}.$$

Therefore

$$\left(\sum_{a \in A} s^a \right) \circ \left(\sum_{b \in F} x^b \right) = \sum_{a \in A' * F} x^a.$$

Example 51. For $A \in \mathrm{PP}[n]$ let $\widehat{A} = \{a \in \mathrm{P}[n, \widetilde{n}] \mid a_1 = a_2 \in A \ \}$. Let $F \in \mathrm{PP}[n]$, then

$$\widehat{A} * F = \{ \ a \in \mathrm{P}[n] \ \mid \ O\{b \in A, c \in \mathrm{P}[n], e \in F \mid c \subseteq b \cap e,\ b \cup e \setminus c = a \ \} \ \}.$$

$$\left(\sum_{a \in A} x^a s^a \right) \circ \left(\sum_{b \in F} x^b \right) = \sum_{a \in \widehat{A} * F} x^a.$$

8 Final Remarks

We introduced an approach for the study of quantum-like phenomena in characteristic 2. Our approach is developed as follows:

1) Quantization of the canonical phase space $k^n \times k^n$ over a field k of characteristic zero may be identified with the k-algebra of algebraic differential operators on k^n. The Weyl algebra provides an explicit description by generators and relations of the latter algebra.

2) Classical propositional logic may be identified, to a good extend, with the study of regular functions on $\mathbb{Z}_2^n$. We introduced the algebra BDO_n as a suitable analogue for algebraic differential operators on $\mathbb{Z}_2^n$. We showed that BDO_n coincides with the algebra of linear endomorphisms

of regular functions on $\mathbb{Z}_2^n$. We introduced a couple of presentations by generators and relations for BDO_n, namely, the quantum Boolean algebras BW_n and SBW_n.

3) We shift back from the algebro-geometric viewpoint, and study the quantum Boolean algebras from the logical and set theoretical viewpoints.

Our work leaves several open questions and problems for future research:

1) We considered the structural aspects of quantization in characteristic 2. The dynamical aspects will be considered elsewhere.

2) We studied the analogue for the Weyl algebra in characteristic 2. Recently, [6, 7, 18], there have been a remarkable interest in characteristic 1. It would be interesting to study the analogue for the Weyl algebra in characteristic 1.

3) Categorification of the Weyl algebra has been considered in [9]; categorification of the Boole-Weyl and shifted Boole-Weyl algebras remain to be addressed.

4) The symmetric powers of Weyl algebras and linear Boolean algebras in characteristic zero were studied in [8] and [10], respectively. The analogue problems for the quantum Boolean algebras and the linear quantum Boolean algebras are open.

5) Our logical interpretation of quantum Boolean algebras was based on a specific choice of connectives. It remains to study other connectives, perhaps with a more direct logical meaning.

References

[1] G. Birkhoff, J. von Neumann, The Logic of Quantum Mechanics, Ann. Math. 37 (1936) 823-843.

[2] J. Boardman, R. Vogt, Homotopy invariant algebraic structures on topological spaces, Lecture Notes in Math. 347, Springer-Verlag, Berlin 1973.

[3] G. Boole, An Investigation of the Laws of Thought, Dover Publications, New York 1958.

[4] F. Brown, Boolean Reasoning, Dover Publications, New York 2003.

[5] A. Connes, Noncommutative Geometry, Academic Press, San Diego 1990.

[6] A. Connes, C. Consani, M. Marcolli, Fun with F_1, J. Number Theory 129 (2009) 1532-1561.

[7] A. Deitmar, Schemes over F1, in G. van der Geer, B. Moonen, R. Schoof (Eds.), Number Fields and Function Fields - Two Parallel Worlds, Progress in Mathematics 239, Birkhäuser, Basel 2005, pp. 87-100.

[8] R. Díaz, E. Pariguan, Quantum Symmetric Functions, Comm. Alg. 33 (2005) 1947-1978.

[9] R. Díaz, E. Pariguan, Super, Quantum and Non-Commutative Species, Afr. Diaspora J. Math. 8 (2009) 90-130.

[10] R. Díaz, M. Rivas, Symmetric Boolean Algebras, Acta Math. Univ. Comenianae LXXIX (2010) 181-197.

[11] V. Ginzburg, M. Kapranov, Kozul duality for operads, Duke Math. J. 76 (1994) 203-272.

[12] J. Harris, Algebraic Geometry, Springer-Verlag, Berlin 1992.

[13] M. Markl, S. Shnider, J. Stasheff, Operads in algebra, topology and physics, Math. Surveys and Monographs 96, Amer. Math. Soc., Providence 2002.

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

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

[16] I. Shafarevich, Basic Algebraic Geometry 1, Springer-Verlag, Berlin 1994.

[17] M. Stone, The Theory of Representations for Boolean Algebras, Trans. Amer. Math. Soc. 40 (1936) 37-111.

[18] C. Soulé, Les variétés sur le corps à un élément, Moscow Math. J. 4 (2004) 217-244.

[19] I. Zhegalkin, On the Technique of Calculating Propositions in Symbolic Logic, Mat. Sb. 43 (1927) 9-28.

ragadiaz@gmail.com
Instituto de Matemáticas y sus Aplicaciones, Universidad Sergio Arboleda, Bogotá, Colombia