

# Equational Reasoning with Controlled ZXW Diagrams

Edwin Agnew

Lia Yeh

Richie Yeung

Matthew Wilson

## 1 Abstract

asdf

## 2 Introduction

asdf

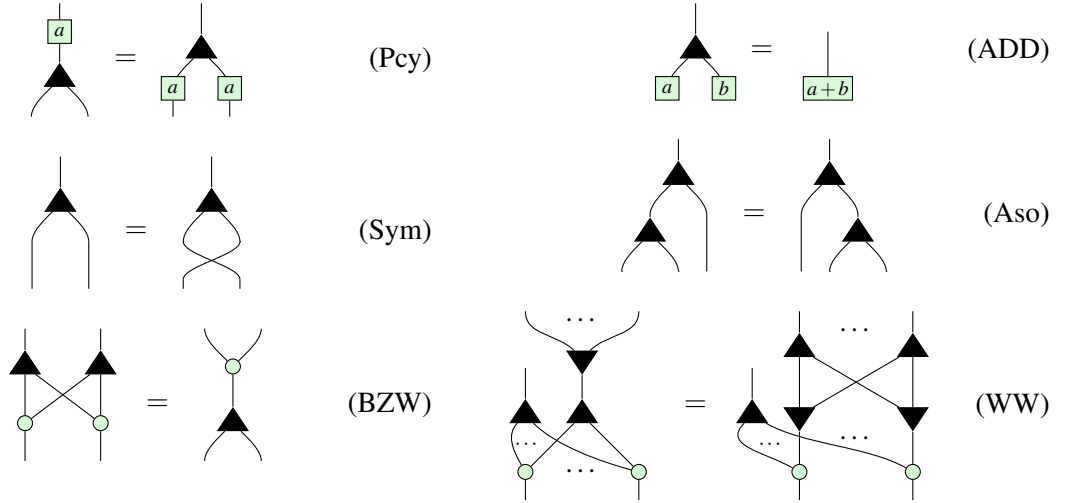
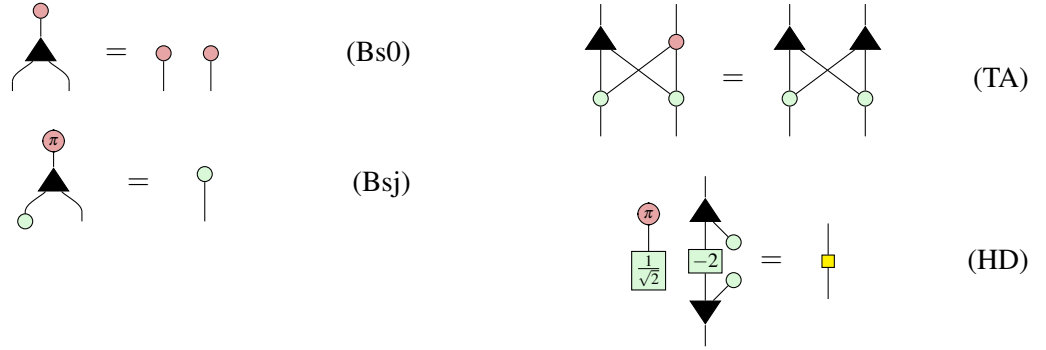
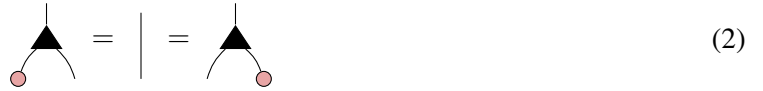
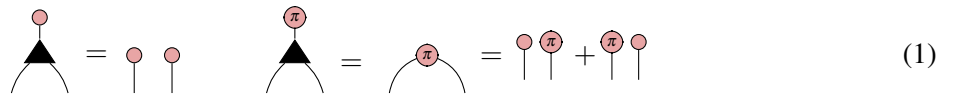
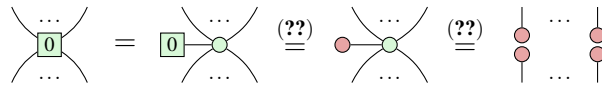
### 3 ZXW Calculus

### 3.1 Rules

### ZX Rules:

Where  $k \in \{0, 1\}$ .

### ZW Rules:

**ZXW Rules:****Lemmas:****Lemma 3.1.***Proof.*

□

**Lemma 3.2.**

$$\begin{array}{c} \blacktriangle \\ \hline \boxed{a} \quad \boxed{b} \\ \hline \blacktriangledown \end{array} = \boxed{a+b} \quad (4)$$

*Proof.*

$$\begin{array}{c} \blacktriangle \\ \hline \boxed{a} \quad \boxed{b} \\ \hline \blacktriangledown \end{array} = \begin{array}{c} \blacktriangle \\ \hline \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \\ \hline \blacktriangledown \end{array} = \begin{array}{c} \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \\ \diagup \quad \diagdown \\ \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \end{array} \stackrel{??}{=} \begin{array}{c} \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \\ \diagup \quad \diagdown \\ \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \end{array} \stackrel{??}{=} \boxed{a+b}$$

□

$$\begin{array}{c} \blacktriangle \\ \hline \textcircled{\pi} \\ \hline \blacktriangledown \end{array} = \begin{array}{c} \blacktriangle \\ \hline \boxed{1} \quad \boxed{-1} \\ \hline \blacktriangledown \end{array} \stackrel{??}{=} \boxed{0} \stackrel{??}{=} \begin{array}{c} \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \\ \diagup \quad \diagdown \\ \textcircled{\phantom{a}} \quad \textcircled{\phantom{b}} \end{array} \quad (5)$$

## 4 Controlled Diagrams

### 4.1 Definitions

As defined in [?],

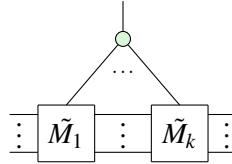
**Definition 4.1.** For an arbitrary square matrix  $D$ , the controlled matrix of  $D$  is the diagram  $\tilde{D}$  such that:

$$\begin{array}{c} \textcircled{\phantom{a}} \\ \hline \boxed{\tilde{D}} \\ \hline \vdots \quad \vdots \end{array} = \begin{array}{c} \vdots \quad \vdots \end{array} \quad (6)$$

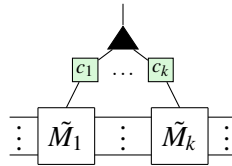
$$\begin{array}{c} \textcircled{\pi} \\ \hline \boxed{\tilde{D}} \\ \hline \vdots \quad \vdots \end{array} = \begin{array}{c} \boxed{D} \\ \hline \vdots \quad \vdots \end{array} \quad (7)$$

It is possible to perform matrix arithmetic with controlled diagrams.

**Proposition 1.** Given controlled matrices  $\tilde{M}_1, \dots, \tilde{M}_k$ , the controlled matrix  $\widetilde{\prod_i \tilde{M}_i}$  is given by



Given controlled matrices  $\tilde{M}_1, \dots, \tilde{M}_k$  and complex numbers  $c_1, \dots, c_k$ , the controlled matrix  $\widetilde{\sum_i c_i \tilde{M}_i}$  is given by



*Proof.* See propositions 3.3 and 3.4 in [?]

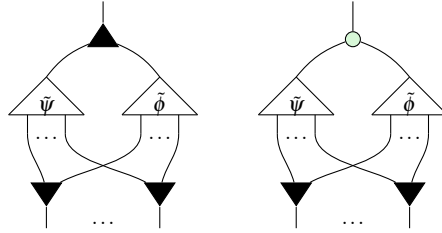
□

We can also defined the analogue for states

**Definition 4.2.** For an arbitrary state  $\psi$ , the controlled state of  $\psi$  is the diagram  $\tilde{\psi}$  such that:

$$\begin{array}{c} \text{red circle} \\ | \\ \triangleup \\ \tilde{\psi} \\ | \dots | \end{array} = \begin{array}{c} \text{red circle} \quad \text{red circle} \\ | \quad | \\ \dots \end{array} \quad \begin{array}{c} \text{red circle with } \pi \\ | \\ \triangleup \\ \tilde{\psi} \\ | \dots | \end{array} = \begin{array}{c} \triangleup \\ \psi \\ | \dots | \end{array} \quad (8)$$

The addition and multiplication of controlled states are defined similarly to controlled matrix arithmetic, except that a layer of  $\blacktriangledown$  s are appended at the bottom to preserve the number of outputs.



The role of  $\blacktriangledown$  is to *copy* inputs, as shown in the next subsection.

## 4.2 Functor

The operation of turning a square matrix to its controlled diagram can be made into a lax monoidal functor  $F : \mathbf{EndVect} \rightarrow \mathbf{Vect}$ , where  $\mathbf{EndVect}$  is the category of vector space endomorphisms (i.e. square matrices). An additional horizontal wire is required to facilitate composition. Let  $D \in \text{Hom}_{\mathbf{EndVect}}(V, V)$ .

$$F :: V \xrightarrow{D} V \mapsto V \xrightarrow{\tilde{D}} V \quad (9)$$

In the functorial box notation of [?], this would be:

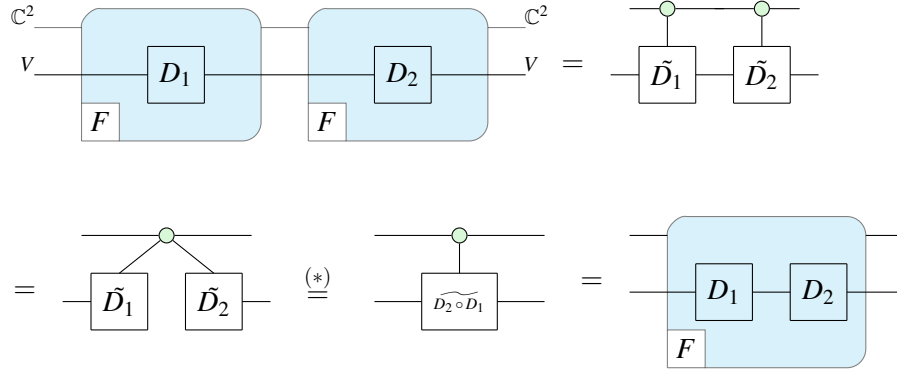
$$\begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} \begin{array}{c} \text{blue box} \\ \text{containing } D \\ \text{and } F \end{array} \begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} = \begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} \begin{array}{c} \text{green circle} \\ | \\ \tilde{D} \end{array} \begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} \quad (10)$$

**Proposition 2.** The map  $F$  defined in (??) is a lax monoidal functor.

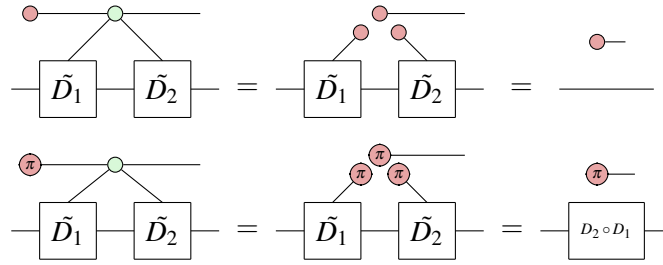
*Proof.* On  $\text{id}_V : V \rightarrow V$ :

$$\begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} \begin{array}{c} \text{blue box} \\ \text{containing } F \end{array} \begin{array}{c} \mathbb{C}^2 \\ | \\ V \end{array} = \begin{array}{c} \text{green circle} \\ | \\ \text{green circle} \end{array} = \text{empty box}$$

Composing  $F(D_2) \circ F(D_1)$ :

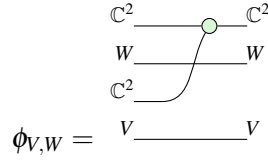


Where  $(*)$  follows from

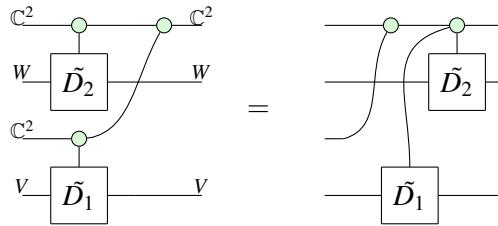


$F$  preserves the monoidal unit since  $\mathbf{1}_{\text{EndVect}} = \mathbf{1}_{\text{Vect}} = \begin{smallmatrix} \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{smallmatrix}$

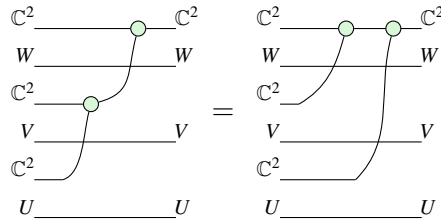
$F$  is lax thanks to the following structure morphism:  $\phi_{V,W} : F(V) \otimes F(W) \rightarrow F(V \otimes W)$ :



$\phi$  is natural since for any  $D_1 : V \rightarrow V, D_2 : W \rightarrow W$ , we have:



Finally,  $\phi$  satisfies the coherence condition since for any  $U, V, W$ :



□

### 4.3 Monad?

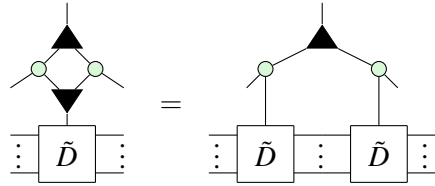
## 5 Polynomials

### 5.1 Rings

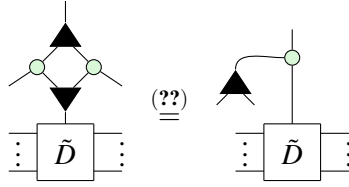
**Most of this will be moved to the appendix**

Let  $\tilde{E}_n$  be the set of controlled square matrices on  $n$  qubits. The goal of this section is to prove that the addition and multiplication operations introduced above induce a ring on  $\tilde{E}_n$ . Before doing so, we prove a few important lemmas. The first lemma enables us to copy controlled matrices.

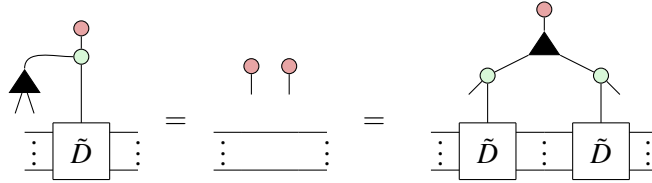
**Lemma 5.1.** *For any square matrix  $D$ ,*


(11)

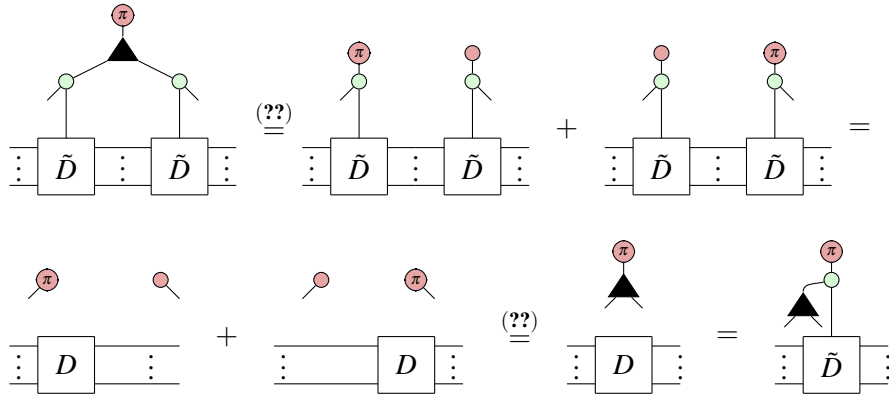
*Proof.* First of all, using (??) we can rewrite the LHS to



Then clearly



Meanwhile,



Thus the two sides are equal over the Z basis and so are equal as diagrams. □

Now we show that controlled matrix addition and multiplication satisfy the ring axioms. Associativity of  $+$ ,  $\times$  follow immediately from (??, ??), respectively. Commutativity of addition follows from the commutativity of matrix addition.

**Lemma 5.2.** *Let  $M_1, M_2$  be  $n \times n$  matrices.*

$$\begin{array}{c} \text{---} \blacktriangle \text{---} \\ | \\ \vdots \boxed{\tilde{M}_1} \vdots \boxed{\tilde{M}_2} \vdots \end{array} = \begin{array}{c} \text{---} \blacktriangle \text{---} \\ | \\ \vdots \boxed{\tilde{M}_2} \vdots \boxed{\tilde{M}_1} \vdots \end{array} \quad (12)$$

*Proof.* We prove by plugging red and commutativity of matrix addition. By definition of controlled matrices, plugging  $\text{---} \overset{\circ}{\pi} \text{---}$  gives  $I_n$  on both sides. Meanwhile, plugging  $\text{---} \overset{\circ}{\pi} \text{---}$  gives:

$$\begin{aligned} \begin{array}{c} \text{---} \overset{\circ}{\pi} \text{---} \\ | \\ \vdots \boxed{\tilde{M}_1} \vdots \boxed{\tilde{M}_2} \vdots \end{array} &= \begin{array}{c} \vdots \boxed{M_1} \vdots \end{array} + \begin{array}{c} \vdots \boxed{M_2} \vdots \end{array} \\ &= \begin{array}{c} \vdots \boxed{M_2} \vdots \end{array} + \begin{array}{c} \vdots \boxed{M_1} \vdots \end{array} = \begin{array}{c} \text{---} \overset{\circ}{\pi} \text{---} \\ | \\ \vdots \boxed{\tilde{M}_2} \vdots \boxed{\tilde{M}_1} \vdots \end{array} \end{aligned}$$

□

The additive identity is defined as  $\text{---} \overset{\circ}{\pi} \otimes I_n$ :

$$\begin{array}{c} \text{---} \blacktriangle \text{---} \\ | \\ \vdots \boxed{\tilde{M}_1} \vdots \end{array} \overset{(\text{??})}{=} \begin{array}{c} \text{---} \\ | \\ \vdots \boxed{\tilde{M}_1} \vdots \end{array}$$

The multiplicative identity is defined very similarly as  $\text{---} \overset{\circ}{\pi} \otimes I_n$ . The existence of additive inverses relies on the copying lemma from before.

**Lemma 5.3.** *The additive inverse of  $\tilde{M}$  is  $\text{---} \boxed{-1} \circ \tilde{M}$*

*Proof.*

$$\begin{array}{c} \text{---} \blacktriangle \text{---} \\ | \\ \vdots \boxed{\tilde{M}} \vdots \boxed{\tilde{M}} \vdots \end{array} \overset{(\text{??})}{=} \begin{array}{c} \text{---} \blacktriangle \text{---} \\ | \\ \vdots \boxed{\tilde{M}} \vdots \end{array} \overset{(\text{??})}{=} \begin{array}{c} \text{---} \overset{\circ}{\pi} \text{---} \\ | \\ \vdots \boxed{\tilde{M}} \vdots \end{array} = \begin{array}{c} \text{---} \overset{\circ}{\pi} \text{---} \\ | \\ \vdots \vdots \end{array}$$

□

Finally, we prove distributivity.

**Lemma 5.4.**

*Proof.*

□

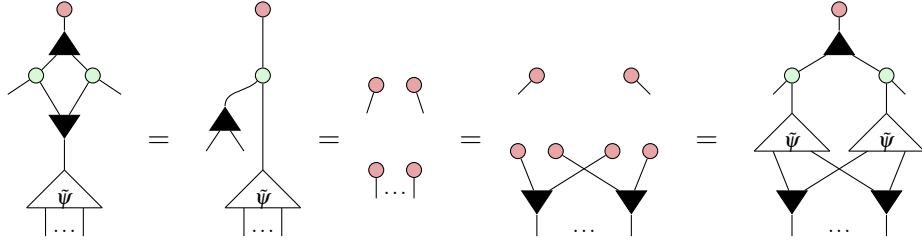
Combining the lemmas of this section shows that controlled matrices form a ring. A similar result can be shown for controlled states. Once again, we start with the ability to copy controlled states.

**Lemma 5.5.** *For any state  $\psi$ ,*

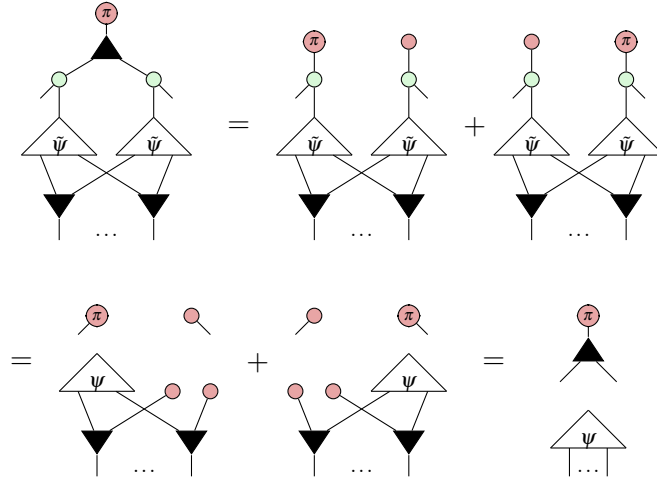
(13)



*Proof.* As before, plugging  $|0\rangle$  gives



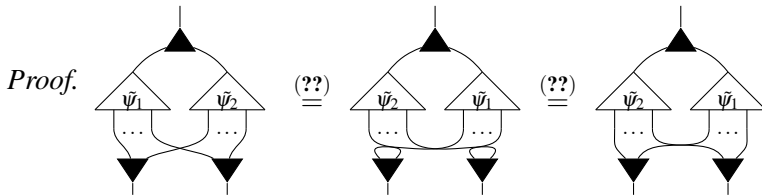
Meanwhile, plugging  $|1\rangle$  gives



Completing the proof □

Many of the ring axioms follow directly from basic ZXW rules. For example we can show commutativity of addition as follows:

**Lemma 5.6.** For  $n$ -partite states  $\psi_1, \psi_2$ ,  $\tilde{\psi}_1 \boxplus \tilde{\psi}_2 = \tilde{\psi}_2 \boxplus \tilde{\psi}_1$

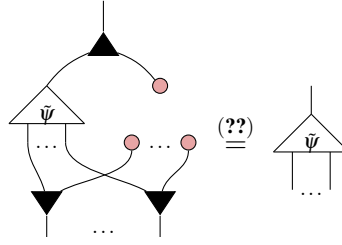


Associativity of  $\boxplus$  follows similarly, using (??). Next we have the additive identity.

**Lemma 5.7.**  $\tilde{\psi} \boxplus \tilde{\mathbf{0}} = \tilde{\psi}$

*Proof.* It is clear that is the controlled state  $\tilde{\mathbf{0}}$ .

Then we have:

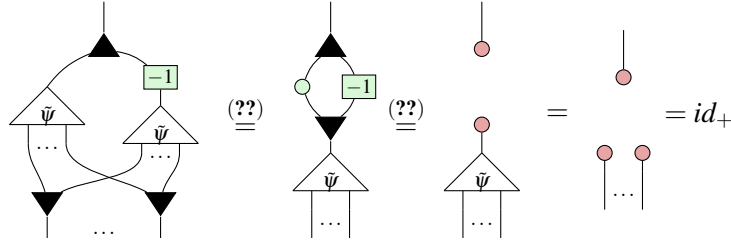


□

The additive inverse is defined similarly to the case of controlled matrices.

**Lemma 5.8.** For a controlled state  $\tilde{\psi}$ , its additive inverse is  $\tilde{\psi} \circ \boxed{-1}$

*Proof.*  $\tilde{\psi} \circ \boxed{-1}$  is still a controlled state since  $\boxed{-1}$  does nothing to  $\bullet$ . Then  $\tilde{\psi} \circ \boxed{-1}$  inverts  $\tilde{\psi}$  since:

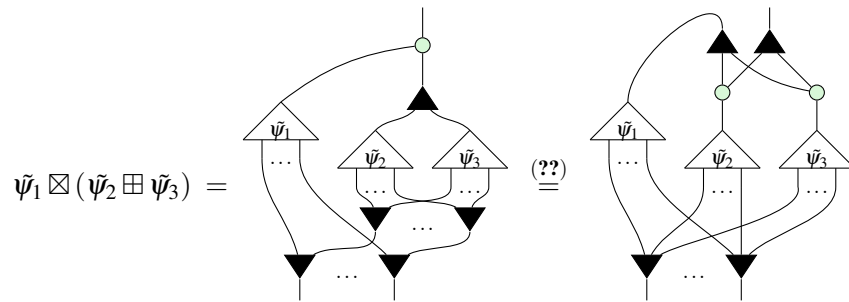


□

Associativity and commutativity of  $\boxtimes$  follow as before, using (??) for  $\bullet$ . Finally, we must prove distributivity.

**Lemma 5.9.**  $\tilde{\psi}_1 \boxtimes (\tilde{\psi}_2 \boxplus \tilde{\psi}_3) = (\tilde{\psi}_1 \boxtimes \tilde{\psi}_2) \boxplus (\tilde{\psi}_1 \boxtimes \tilde{\psi}_3)$

*Proof.*



$$= (\tilde{\psi}_1 \boxtimes \tilde{\psi}_2) \boxplus (\tilde{\psi}_1 \boxtimes \tilde{\psi}_3)$$

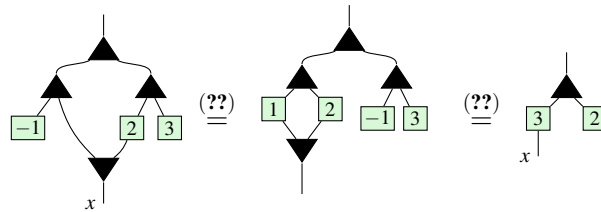
□

## 5.2 Arithmetic

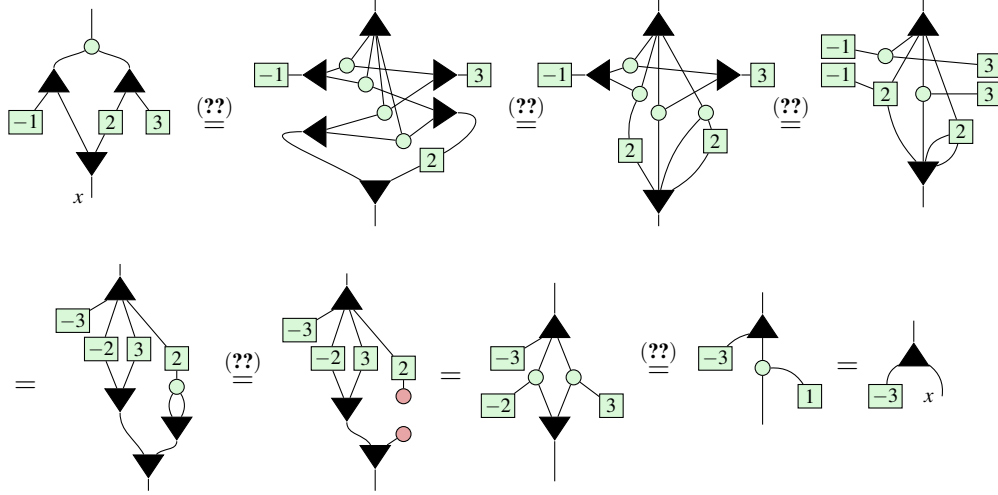
Recall from (??, ??) that  $\blacktriangle$ ,  $\circ$  can be used to add and multiply numberstates  $\boxed{a}$ , respectively. In the previous section we saw that  $\blacktriangle$ ,  $\circ$  can moreover be used to copy controlled diagrams. In this section, we explain this connection by demonstrating that controlled states are in fact isomorphic to multilinear polynomials. Firstly, we describe how to interpret certain ZXW diagrams as polynomials. Consider the following diagrams:



If we treat the bottom wires as an indeterminate  $x$ , we can read these bottom-up as computing  $x - 1$  and  $2x + 3$ , respectively. Moreover, since these diagrams are both controlled states, they can be added to yield a diagram resembling  $3x + 2$ :



When trying to multiply these diagrams, rather than getting  $(x-1)(2x+3) = 2x^2 + x - 3$ , we instead get  $x - 3$ .



The reason for the missing  $2x^2$  term is that  $(??)$  implies  $x^2 = 0$ . Other than that, controlled state arithmetic appears to faithfully reflect polynomial arithmetic. To help formalise this correspondence, we introduce the following definition.

**Definition 5.1.** A ZXW diagram with a single input on top is **arithmetic** if it contains only  $|$ ,  $\times$  wires,  $\blacktriangle$ ,  $\circ$ ,  $\blacktriangledown$  nodes and  $\boxed{a}$  boxes.

To interpret an arithmetic ZXW diagram as an arithmetic expression, read  $\blacktriangle$  as  $+$ ,  $\circ$  as  $\times$ ,  $\boxed{a}$  as the number  $a$ ,  $\blacktriangledown$  as fanout and output/bottom wires as variables  $x_1, \dots, x_n$  numbered from left to right. The following lemma establishes that all arithmetic diagrams are controlled states:

**Lemma 5.10.** For any arithmetic diagram  $A$ ,

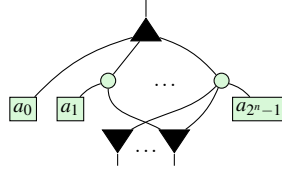
$$\boxed{A} = \text{two red dots}$$

The diagram shows a box labeled  $A$  with a single input wire at the top and multiple output wires at the bottom. This is equated to a diagram consisting of two red dots, each with a single output wire.

*Proof.* By definition, other than wires  $A$  contains only  $\blacktriangle$ ,  $\circ$ ,  $\blacktriangledown$ , and  $\boxed{a}$ . All  $\boxed{a}$ 's can be removed with  $(??)$ . Meanwhile all the spiders copy  $\bullet$  due to  $(??, ??, ??)$  respectively.  $\square$

Just as it is typical to represent a polynomial in normal form as a sum of products, it is possible to rewrite every arithmetic diagram into a normal form as a single  $\blacktriangle$ , followed by a layer of  $\circ$ , followed by a layer of  $\boxed{a}$ ,  $\blacktriangledown$ .

**Definition 5.2.** An  $n$ -output arithmetic diagram is said to be written in **polynormal form** (PNF) if it looks like:



The  $i$ th coefficient  $a_i$  is connected to the  $k$ th  $\blacktriangledown$  iff the  $k$ th bit in the binary expansion of  $i$  is 1.

This normal form is very closely related to the completeness normal form (CoNF, see Definition ??). Simply applying (??) to the  $\blacktriangledown$ s at the bottom of a PNF and fusing the number boxes gives a CoNF diagram. The reason we introduce the definition of a PNF is that it is an arithmetic diagram and therefore has a more immediate arithmetic interpretation. The reason for the specific connectivity condition is that it enables a PNF to directly represent its own matrix.

**Proposition 3.**

$$\begin{array}{c} \text{PNF Diagram} \end{array} = \begin{bmatrix} 1 & a_0 \\ 0 & a_1 \\ \dots & \dots \\ 0 & a_{2^n-1} \end{bmatrix} \quad (14)$$

*Proof.* We prove by induction on  $n$ .

For the base case,  $n = 0$ . The only PNF with no outputs is a number so we have:

$$\boxed{a_0} = \begin{bmatrix} 1 & a_0 \end{bmatrix}$$

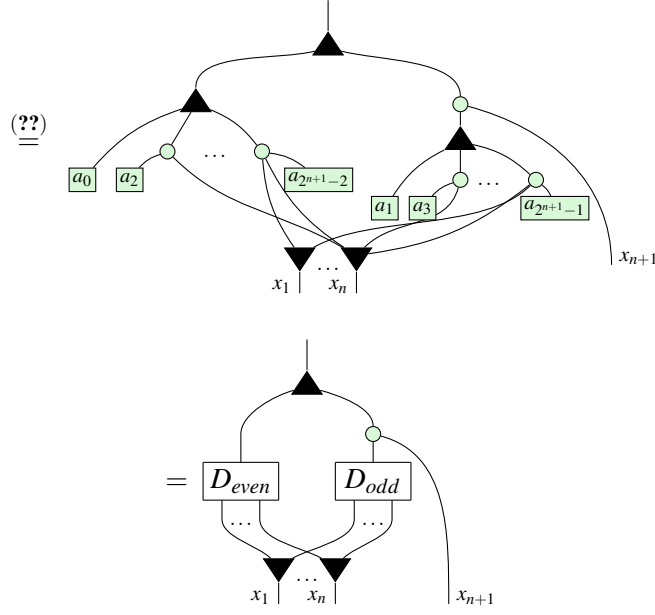
as desired.

For inductive hypothesis, we assume that (??) holds for every PNF on  $n$  outputs. We use this hypothesis to extend it to PNFs with  $n + 1$  outputs.

Let  $D$  be an arbitrary PNF with  $n + 1$  outputs. Firstly, observe that  $x_{n+1}$  is connected to only the odd coefficients  $\{a_{2k+1}\}$  since these are exactly the indices with 1 in the least significant bit. Thus we can rewrite:

$$\begin{array}{c} \boxed{D} \\ \vdots \end{array} = \begin{array}{c} \text{PNF Diagram} \\ \vdots \end{array} = \begin{array}{c} \text{Revised PNF Diagram} \end{array}$$

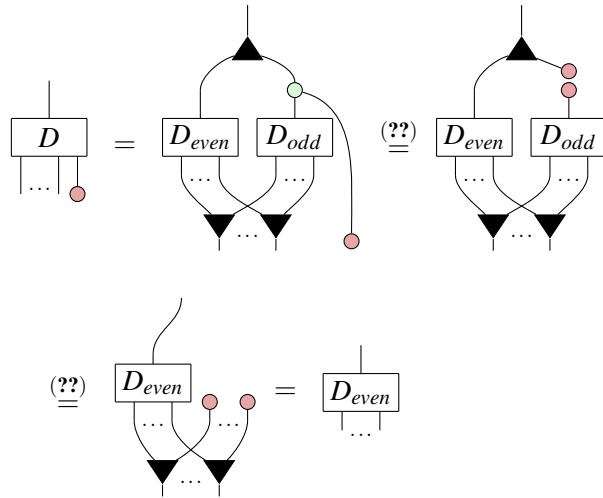
The diagram shows the decomposition of a PNF with  $n+1$  outputs into a revised PNF. The revised diagram has two sets of inputs: even-indexed coefficients  $a_0, a_2, \dots, a_{2^{n+1}-2}$  and odd-indexed coefficients  $a_1, a_3, \dots, a_{2^{n+1}-1}$ . The odd-indexed coefficients are connected to a set of nodes that produce outputs  $x_1, \dots, x_{n+1}$ . The even-indexed coefficients are connected to another set of nodes that produce outputs  $x_1, \dots, x_n$ .



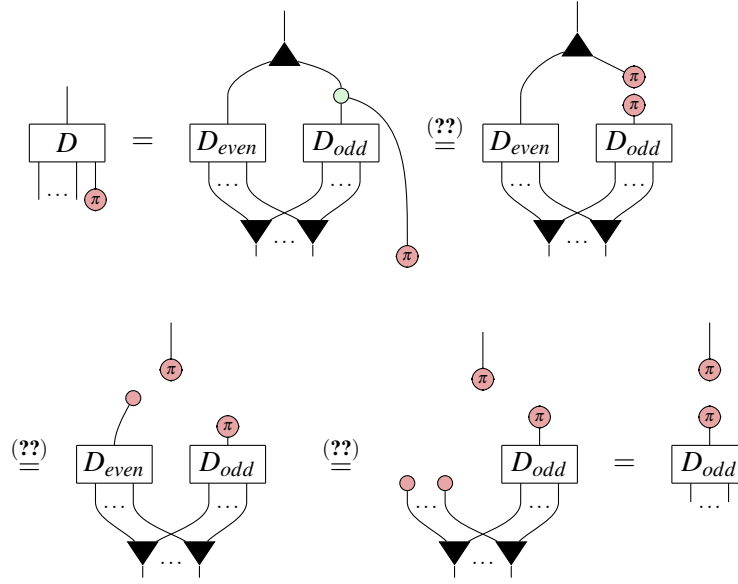
Where  $D_{even}, D_{odd}$  are PNF diagrams. Since they are over  $n$  variables, we can apply the inductive hypothesis and obtain:

$$D_{even} = \begin{bmatrix} 1 & a_0 \\ 0 & a_2 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \end{bmatrix}, D_{odd} = \begin{bmatrix} 1 & a_1 \\ 0 & a_3 \\ \dots & \dots \\ 0 & a_{2^{n+1}-1} \end{bmatrix} \quad (*)$$

Next, plugging red we observe:



Meanwhile,



Summing these together,

$$\begin{aligned}
 D &= D + D = D_{\text{even}} + D_{\text{odd}} \\
 &= (D_{\text{even}} \otimes |0\rangle) + (D_{\text{odd}} |1\rangle \langle 1| \otimes |1\rangle) \\
 &\stackrel{(*)}{=} \begin{bmatrix} 1 & a_0 \\ 0 & a_2 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \end{bmatrix} \otimes |0\rangle + \begin{bmatrix} 0 & a_1 \\ 0 & a_3 \\ \dots & \dots \\ 0 & a_{2^{n+1}-1} \end{bmatrix} \otimes |1\rangle \\
 &= \begin{bmatrix} 1 & a_0 \\ 0 & 0 \\ 0 & a_2 \\ 0 & 0 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & a_1 \\ 0 & 0 \\ 0 & a_3 \\ \dots & \dots \\ 0 & 0 \\ 0 & a_{2^{n+1}-1} \end{bmatrix} = \begin{bmatrix} 1 & a_0 \\ 0 & a_1 \\ 0 & a_2 \\ 0 & a_3 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \\ 0 & a_{2^{n+1}-1} \end{bmatrix}
 \end{aligned}$$

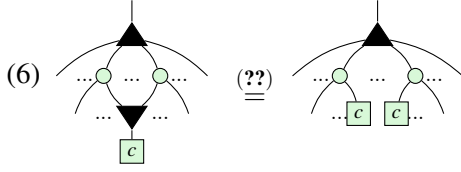
Completing the inductive step. □

Thus, every controlled state can be represented as at least one arithmetic diagram (namely, its PNF). Moreover, we now show that any other arithmetic diagram can always be rewritten to its PNF.

**Proposition 4.** All arithmetic diagrams can be written into PNF







Clearly, we can only stop applying these rules once  $A$  is a sum of products of copies. Steps (2) and (3)

ensure the top of  $A$  has such a structure and steps (4) - (6) ensure that there is nothing beneath the  $\blacktriangledown$ 's. To see that this will always terminate, observe that (2) and (3) preserve the depth of  $A$  while (4), (5), (6) all decrease it. (2) and (3) can only be applied a finite number of times before another simplification must be used. So repeatedly applying these rewrites must eventually shrink the depth down to 3, as desired. Finally, to put  $A$  in PNF we must:

(7) Collect terms: whenever there are two boxes connected to exactly the same set of  $\blacktriangledown$ 's, use (??) to fuse them together.

(8) Pad: use (??) to insert  $\boxed{0}$  for any connectivities that do not exist in  $A$ .

(9) Reorder: use (??) to reorder coefficients into the canonical order.

Step (7) ensures that every  $\blacktriangledown$  has unique connectivity. Step (8) ensures there are exactly  $2^n$  coefficients so that step (9) can order them in the appropriate way.

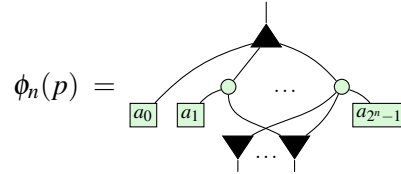
Thus  $A$  has been written in PNF, completing the proof.  $\square$

### 5.3 Isomorphism

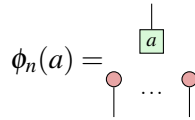
At last we can prove the isomorphism. Throughout we shall let  $\mathcal{P}_n$  denote the ring  $\mathbb{C}[x_1, \dots, x_n]/(x_1^2, \dots, x_n^2)$ .

**Theorem 5.1.** *There is an isomorphism  $\mathcal{P}_n \simeq \tilde{\mathcal{S}}_n$*

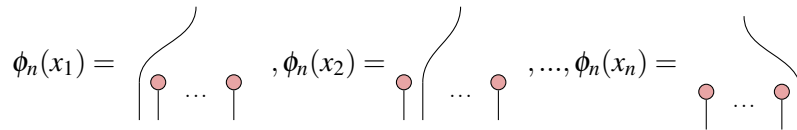
First, we shall define the map  $\phi_n : \mathcal{P}_n \rightarrow \tilde{\mathcal{S}}_n$  before proving it induces an isomorphism.  $\phi_n$  is defined to map an arbitrary polynomial  $p(x_1, \dots, x_n) = a_0 + a_1x_1 + \dots + a_{2^n-1}x_1x_2\dots x_n$  to the following PNF:



Some important special cases are mapping scalars  $a \in \mathbb{C}$ :



And mapping indeterminates  $x_i$ :



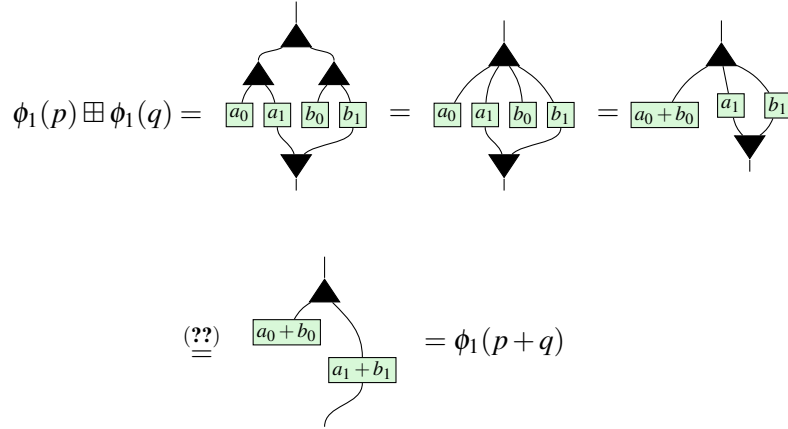
We can now prove this yields an isomorphism.

*Proof.* First, we show  $\phi_n$  is a homomorphism, i.e.

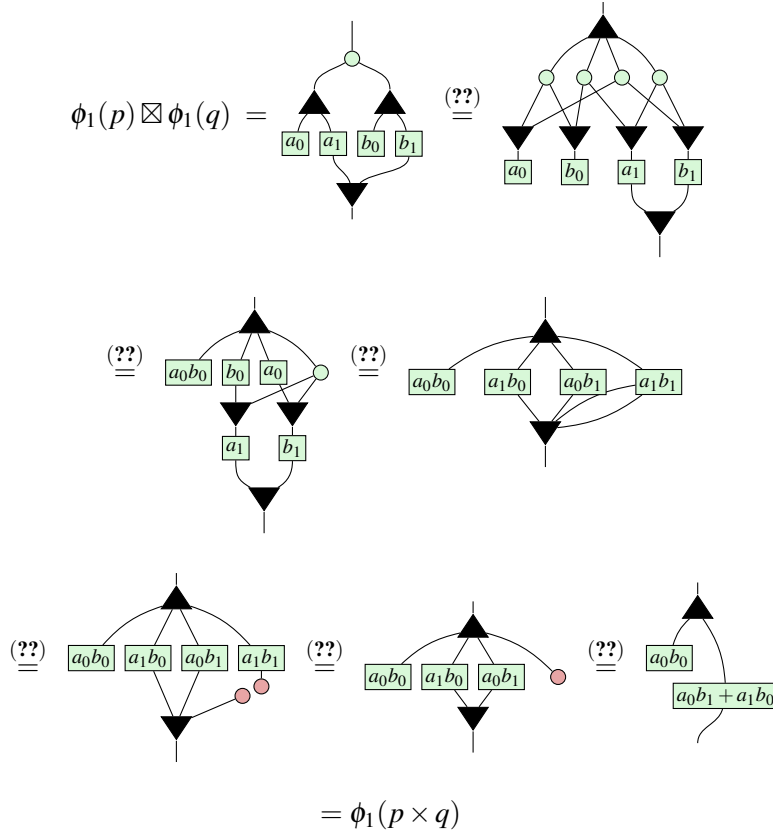
$$\forall p, q \in \mathcal{P}_n, \phi_n(p + q) = \phi_n(p) \boxplus \phi_n(q), \quad \phi_n(p \times q) = \phi_n(p) \boxtimes \phi_n(q)$$

The strategy for the proof will be an induction on  $n$ .

**Base case:** We have not defined controlled states for  $n = 0$ , so the base case begins with  $n = 1$ . Let  $p, q \in \mathcal{P}_1$ . Write as  $p(x_1) = a_0 + a_1x_1, q(x_1) = b_0 + b_1x_1$ , where  $a_0, a_1, b_0, b_1 \in \mathbb{C}$ . Then since  $p + q = a_0 + b_0 + (a_1 + b_1)x_1$ ,



Meanwhile, since  $p \times q = a_0a_1 + (a_0b_1 + a_1b_0)x_1$ ,



Completing the base case.

**Inductive step:**

Let  $\text{Hom}(n)$  assert that  $\phi_n$  is a homomorphism. Then for the inductive step we wish to prove that  $\forall n, \text{Hom}(n) \implies \text{Hom}(n+1)$ .

The proof relies on the recursive definition of  $R[x_1, x_2] = R[x_1][x_2]$ , for any ring  $R$ , to rewrite an arbitrary polynomial  $p(x_1, \dots, x_{n+1}) = a_0 + a_1x_{n+1} + \dots + a_{2^{n+1}-1}x_1x_2\dots x_{n+1} \in \mathcal{P}_{n+1}$  as  $p(x_{n+1}) = p_0 + p_1x_{n+1}$ , where  $p_0, p_1 \in \mathcal{P}_n$ . This allows the  $p_i$  to be treated similarly to the scalars in the base case. To emphasise this, they will be drawn in green boxes. To help distinguish when an operation is covered by the inductive hypothesis, the wires for variables  $x_1, \dots, x_n$  will be drawn in light blue, while the  $x_{n+1}$  wires will be drawn in black. Thus the inductive hypothesis states that:

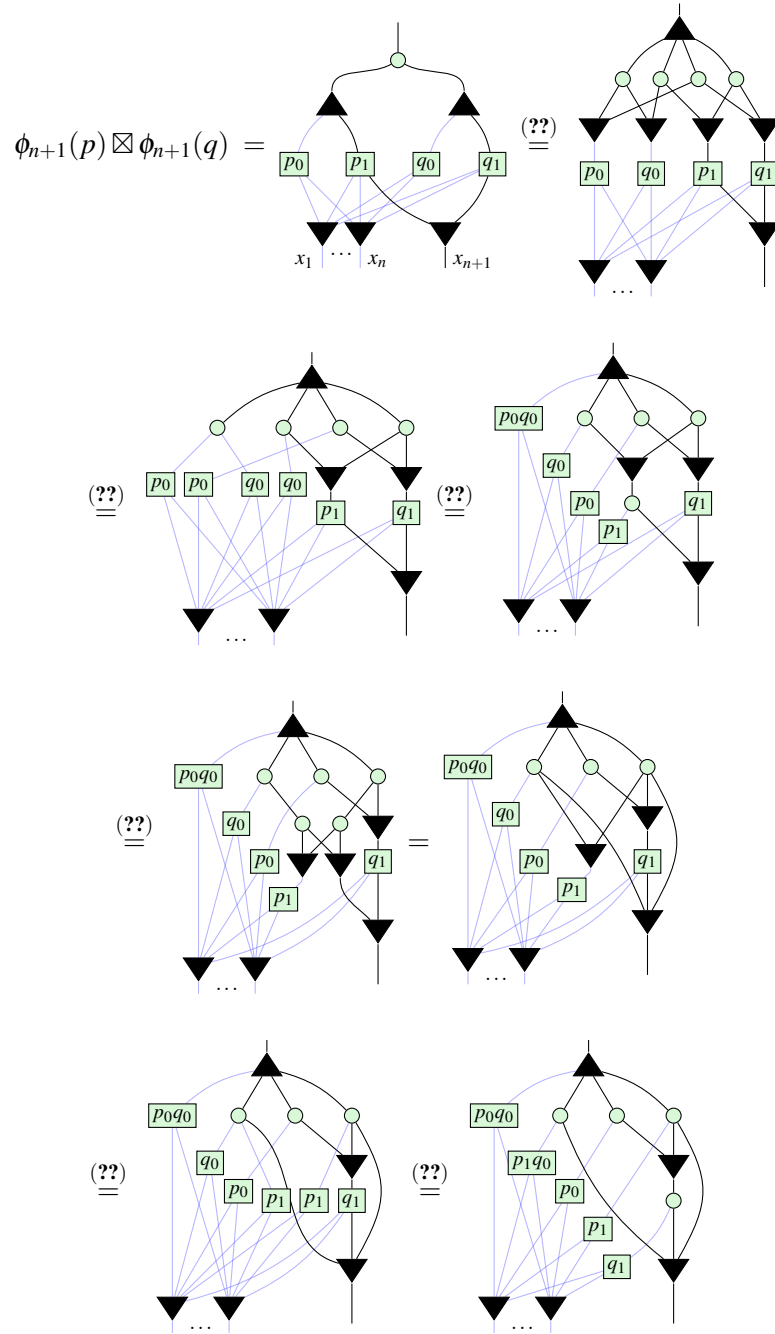
$$\begin{array}{c} \text{Diagram 1: A triangle with a black triangle at the top. Two green boxes labeled 'a' and 'b' are below it. Wires from 'a' and 'b' go to two black triangles. These two black triangles have wires going to a single black triangle at the bottom. The wires from 'a' and 'b' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'. To the right of the diagram is an equals sign followed by a green box labeled 'a+b'. Wires from 'a+b' go to two black triangles, which then have wires going to a single black triangle at the bottom. The wires from 'a+b' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'.$$
(IH1)

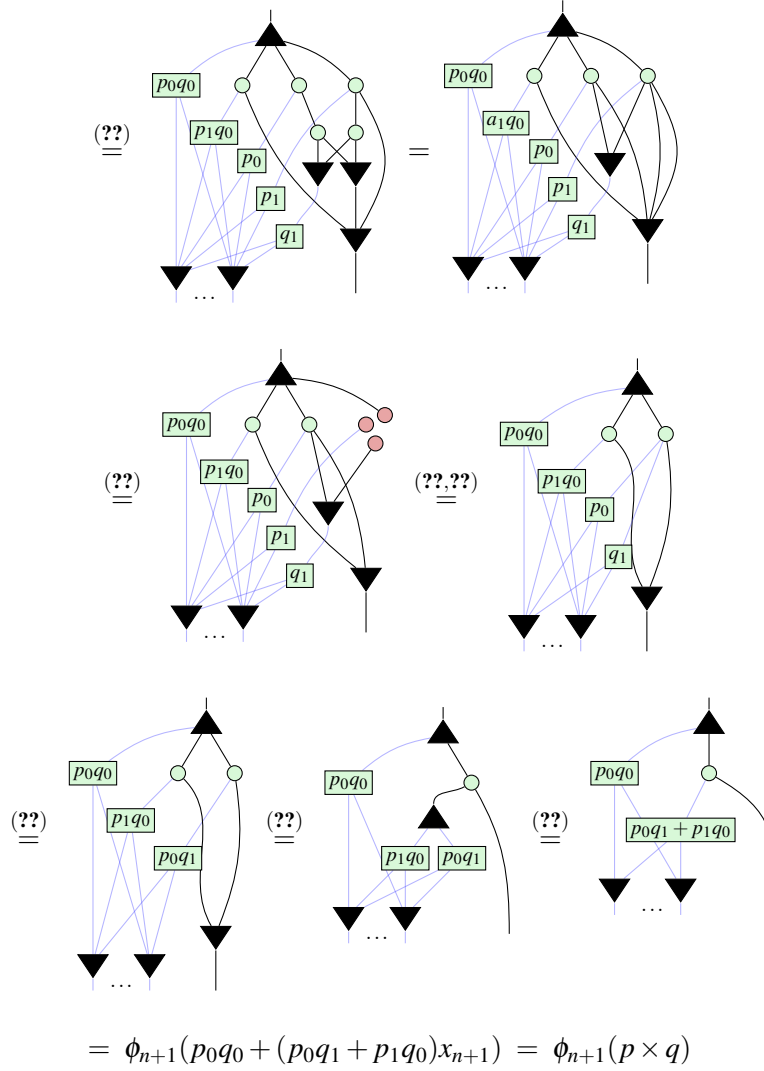
$$\begin{array}{c} \text{Diagram 2: A green circle at the top. Two green boxes labeled 'a' and 'b' are below it. Wires from 'a' and 'b' go to two black triangles. These two black triangles have wires going to a single black triangle at the bottom. The wires from 'a' and 'b' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'. To the right of the diagram is an equals sign followed by a green box labeled 'a \times b'. Wires from 'a \times b' go to two black triangles, which then have wires going to a single black triangle at the bottom. The wires from 'a \times b' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'.$$
(IH2)

Let  $p(x_{n+1}) = p_0 + p_1x_{n+1}$ ,  $q(x_{n+1}) = q_0 + q_1x_{n+1}$ , where  $p_0, p_1, q_0, q_1 \in \mathcal{P}_n$ . Then for addition:

$$\begin{aligned} \phi_{n+1}(p) \boxplus \phi_{n+1}(q) &= \begin{array}{c} \text{Diagram 3: A triangle with a black triangle at the top. Four green boxes labeled 'p_0', 'p_1', 'q_0', 'q_1' are below it. Wires from 'p_0' and 'q_0' go to a black triangle. Wires from 'p_1' and 'q_1' go to another black triangle. These two black triangles have wires going to a single black triangle at the bottom. The wires from 'p_0' and 'q_0' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'. To the right of the diagram is an equals sign followed by a green box labeled 'p_0 + q_0'. Wires from 'p_0 + q_0' go to two black triangles, which then have wires going to a single black triangle at the bottom. The wires from 'p_0 + q_0' to the bottom black triangle are light blue. Below the bottom black triangle are labels 'x_1 \dots x_n'.$$

Similarly, for multiplication:

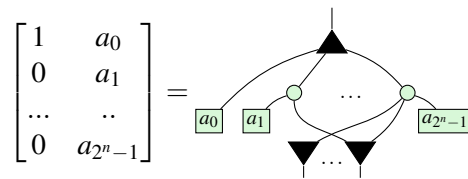




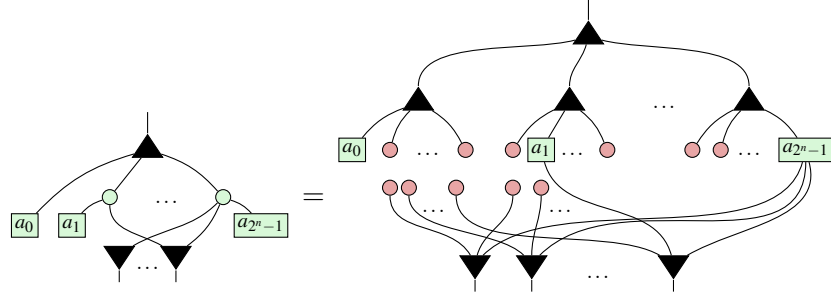
$$= \phi_{n+1}(p_0q_0 + (p_0q_1 + p_1q_0)x_{n+1}) = \phi_{n+1}(p \times q)$$

This completes the inductive step, proving that  $\forall n > 1$ ,  $\phi_n$  is a homomorphism.

Finally, to see  $\phi_n$  is an isomorphism, we use proposition ?? to write an arbitrary controlled state in PNF:



Then all we have to do is interpret it as the image of a polynomial:



$$\begin{aligned}
 &= \phi_n(a_0) + \phi_n(a_1 x_n) + \dots + \phi_n(a_{2^n-1} x_1 x_2 \dots x_n) \\
 &= \phi_n(a_0 + a_1 x_n + \dots + a_{2^n-1} x_1 x_2 \dots x_n)
 \end{aligned}$$

□

## 6 Applications