Equational Reasoning with Controlled ZXW Diagrams

Edwin Agnew   Lia Yeh   Richie Yeung   Matthew Wilson

1 Abstract

asdf

2 Introduction

asdf

3 ZXW Calculus

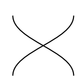
3.1 Generators

The (qubit) ZXW calculus is build from the following generators:

- **Identity wire**:

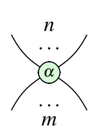
$$:= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- **Swap**:



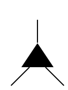
$$:= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- **Z box**:



$$:= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|, \alpha \in \mathbb{C}$$

- **W node**:



$$:= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1|$$

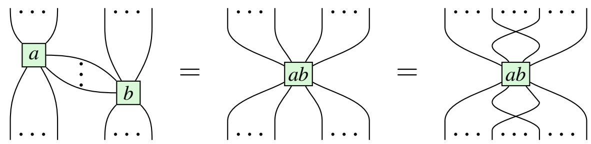
- **H box**:

$$:= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

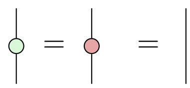
To appear in EPTCS.

3.2 Rules

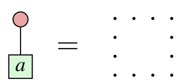
ZX Rules:



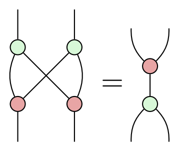
(S1)



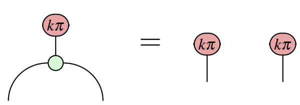
(S2)



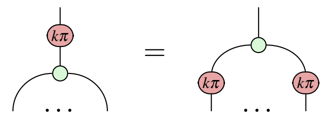
(Ept)



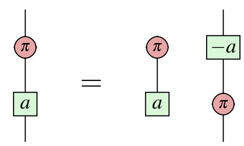
(B2)



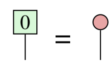
(K0)



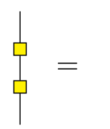
(K1)



(K2)



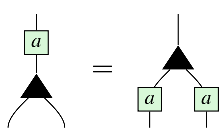
(Zer)



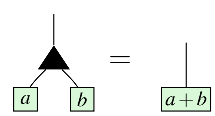
(H)

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

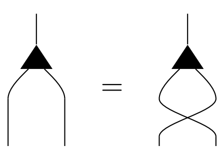
ZW Rules:



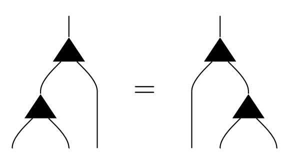
(Pcy)



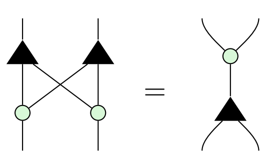
(ADD)



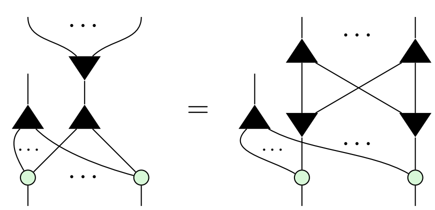
(Sym)



(Aso)

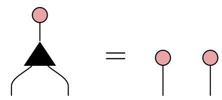


(BZW)

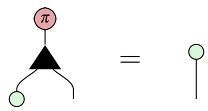


(WW)

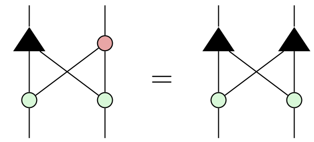
ZXW Rules:



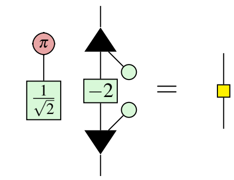
(Bs0)



(Bsj)



(TA)



(HD)

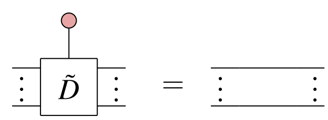
A number of basic lemmas are found in appendix A.

4 Controlled Diagrams

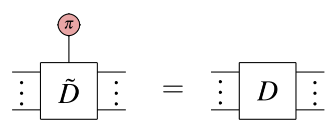
4.1 Definitions

As defined in [4],

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



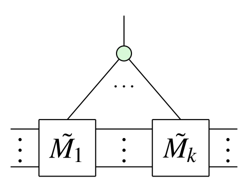
(4.1)



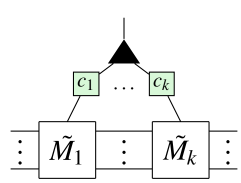
(4.2)

It is possible to perform matrix arithmetic with controlled diagrams.

Proposition 1. Given controlled matrices $\tilde{M}_1,\ldots,\tilde{M}_k$, the controlled matrix $\widetilde{\Pi_i M_i}$ is given by



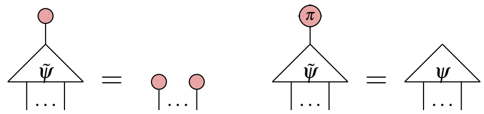
Given controlled matrices $\tilde{M}_1,\ldots,\tilde{M}_k$ and complex numbers $c_1,\ldots,c_k$, the controlled matrix $\widetilde{\Sigma_i c_i M_i}$ is given by



Proof. See propositions 3.3 and 3.4 in [4] □

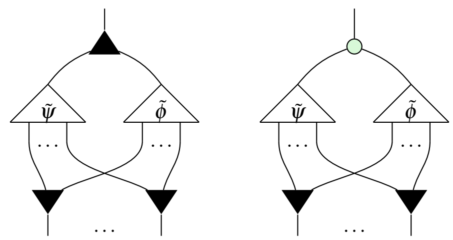
We can also defined the analogue for states

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



(4.3)

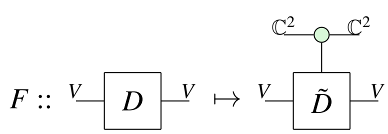
The addition and multiplication of controlled states are defined similarly to controlled matrix arithmetic, except that a layer of  s are appended at the bottom to preserve the number of outputs.



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

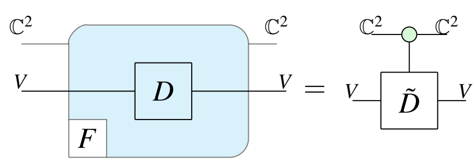
4.2 Functor

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



(4.4)

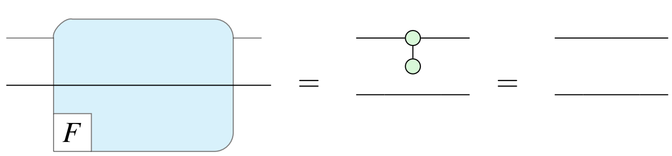
In the functorial box notation of [2], this would be:



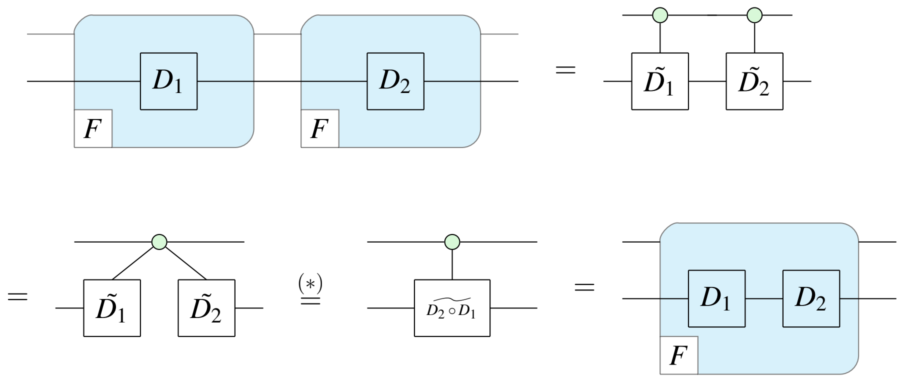
(4.5)

Proposition 2. The map F defined in (4.4) is a lax monoidal funtor.

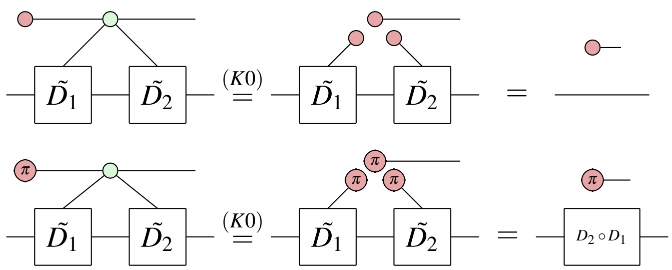
Proof. On $id_V : V \to V$:

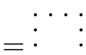


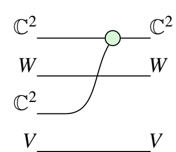
Composing $F(D_2) \circ F(D_1)$:



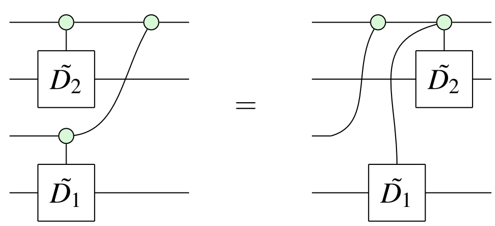
Where $(*)$ follows from



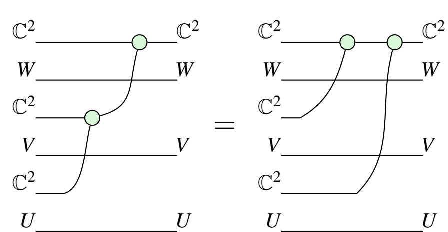
F preserves the monoidal unit since $\mathbf{1_{EndVect}} = \mathbf{1_{Vect}} =$ 
F is lax thanks to the following structure morphism: $\phi_{V,W} : F(V) \otimes F(W) \to F(V \otimes W)$:

$\phi_{V,W} =$ 

ϕ is natural since for any $D_1 : V \to V, D_2 : W \to W$, we have:



Finally, ϕ satisfies the coherence condition since for any U, V, W:



□

4.3 Monad?

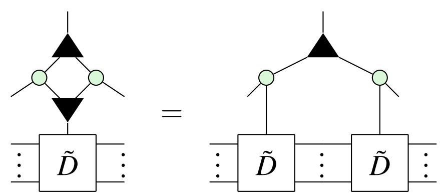
5 Polynomials

5.1 Rings

Most of this will be moved to the appendix

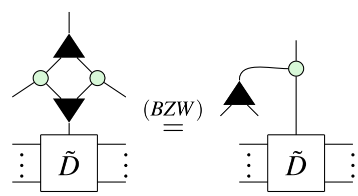
Let $\tilde{E}_n$ be the set of controlled square matrices on n qubits. The goal of this section is to prove that the addition and multiplication operations introduced above induce a ring on $\tilde{E}_n$. Before doing so, we prove a few important lemmas. The first lemma enables us to copy controlled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

Lemma 5.1. *For any square matrix D,*

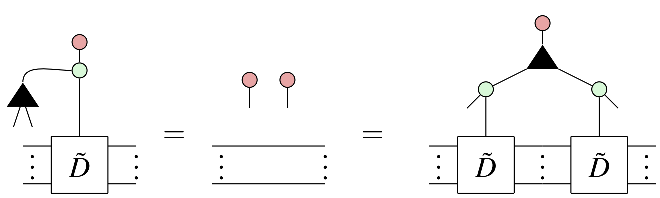


(5.1)

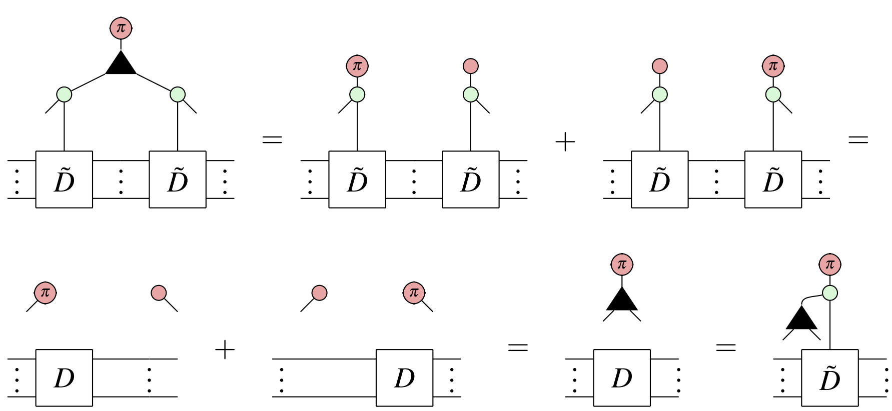
Proof. First of all, using (BZW) we can rewrite the LHS to



Then clearly



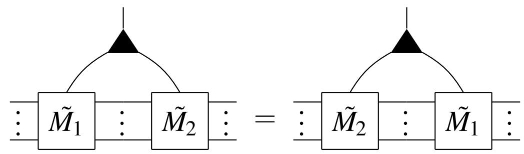
Meanwhile,



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

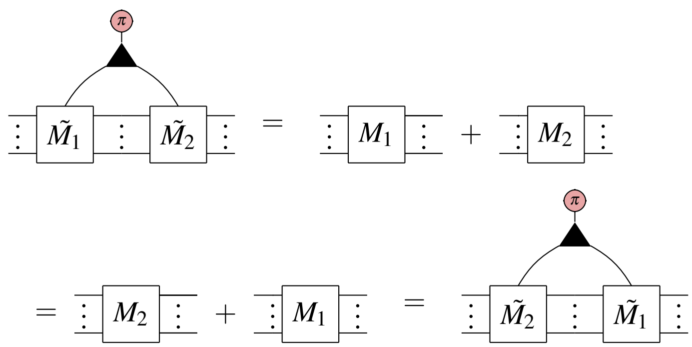
Now we show that controlled matrix addition and multiplication satisfy the ring axioms. Associativity of $+, \times$ follow immediately from (Aso, S1), respectively. Commutativity of addition follows from the commutativity of matrix addition.

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



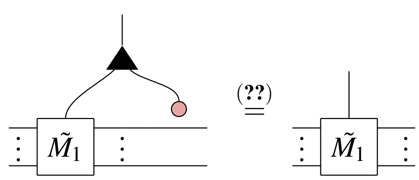
(5.2)

Proof. We prove by plugging red and commutativity of matrix addition. By definition of controlled matrices, plugging gives I_n on both sides. Meanwhile, plugging gives:



□

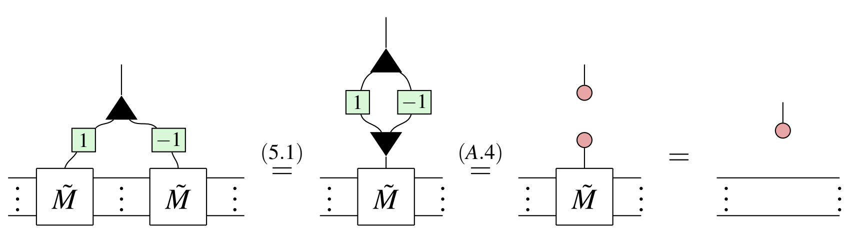
The additive identity is defined as $\otimes I_n$:



The multiplicative identity is defined very similarly as $\otimes I_n$. The existence of additive inverses relies on the copying lemma from before.

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

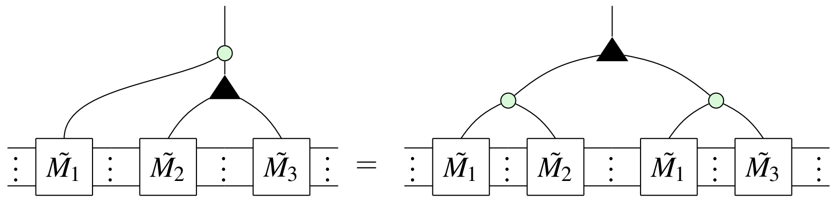
Proof.



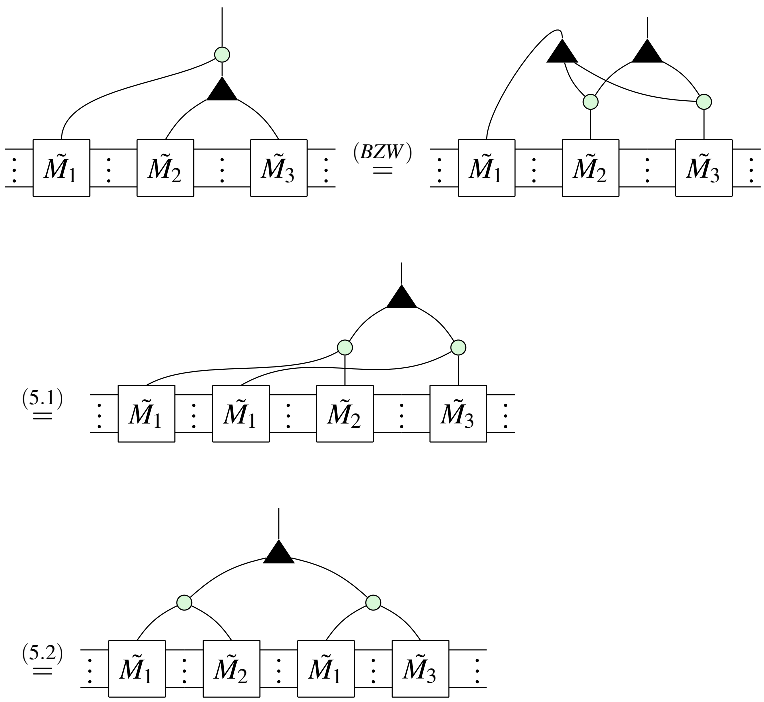
□

Finally, we prove distributivity.

Lemma 5.4.



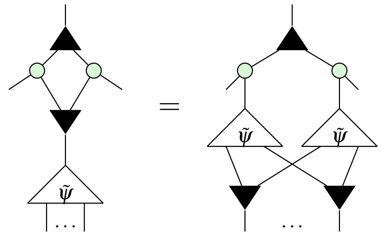
Proof.



□

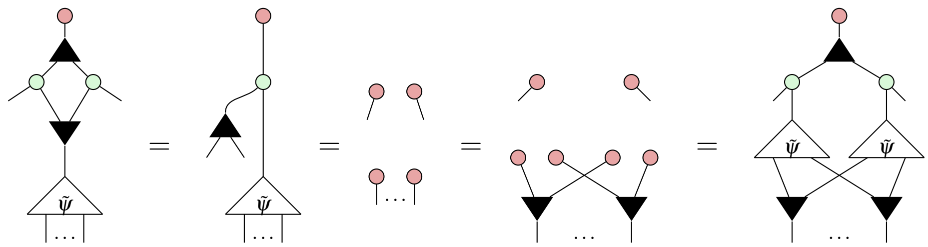
Combining the lemmas of this section shows that controlled matrices form a ring. A similar result can be shown for controlled states. Once again, we start with the ability to copy controlled states.

Lemma 5.5. *For any state ψ,*

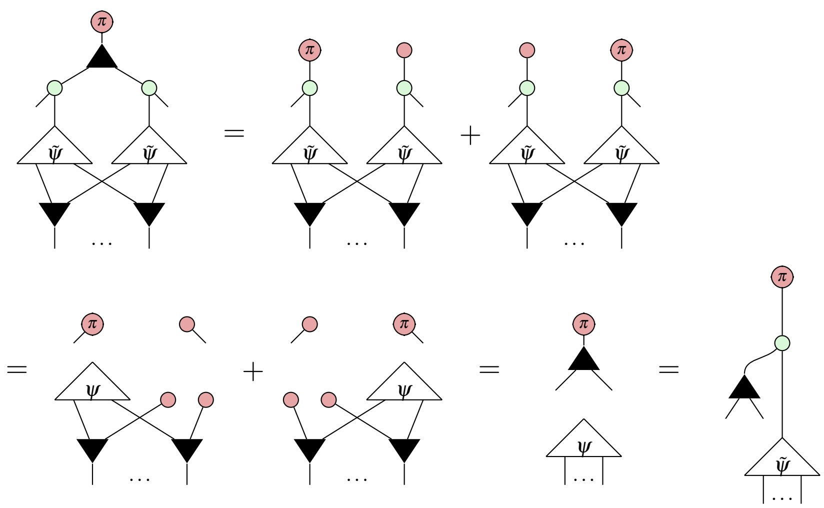


(5.3)

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



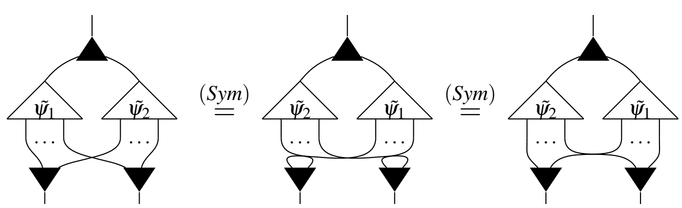
Meanwhile, plugging $|1\rangle$ gives



Completing the proof □

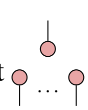
Many of the ring axioms follow directly from basic ZXW rules. For example we can show commutativity of addition as follows:

Lemma 5.6. *For n-partite states* ψ_1, ψ_2, $\tilde{\psi}_1 \boxplus \tilde{\psi}_2 = \tilde{\psi}_2 \boxplus \tilde{\psi}_1$

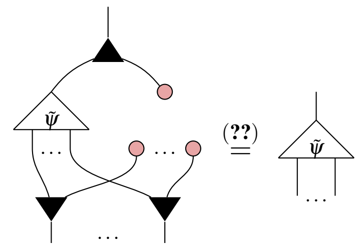
Proof.  □

Associativity of $\boxplus$ follows similarly, using (Aso). 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:

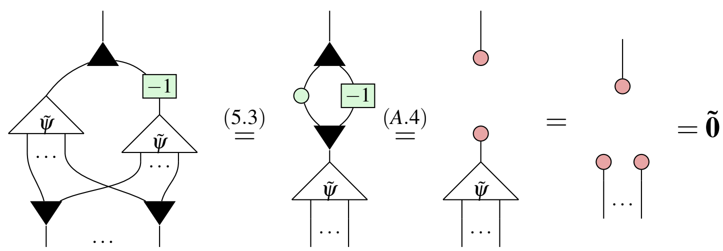


□

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 . Then $\tilde{\psi} \circ \boxed{-1}$ inverts $\tilde{\psi}$ since:



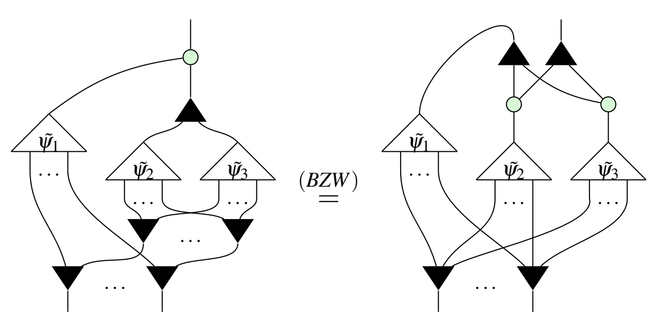
□

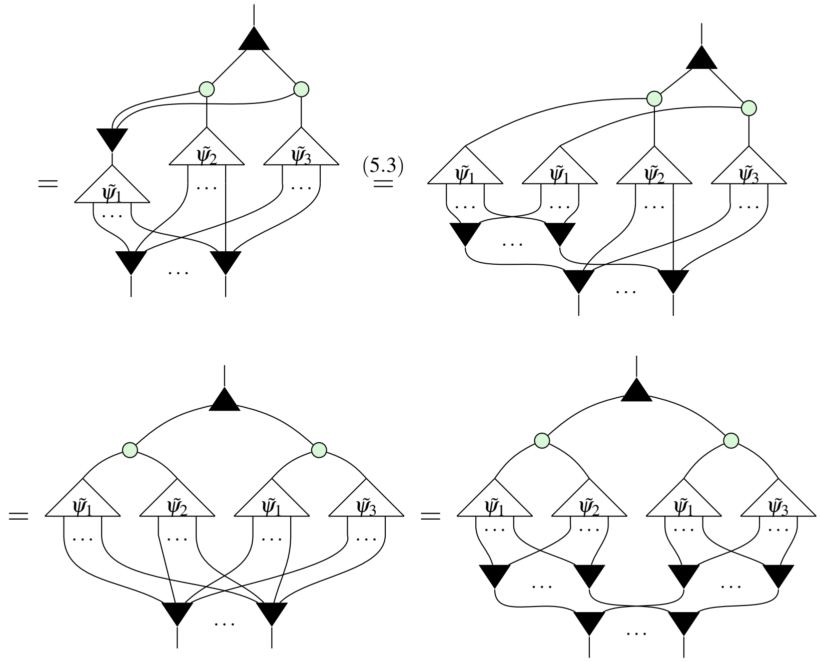
Associativity and commutativity of $\boxtimes$ follow as before, using (S1) for . Finally, we must prove distributivity.

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.

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

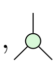
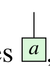
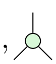




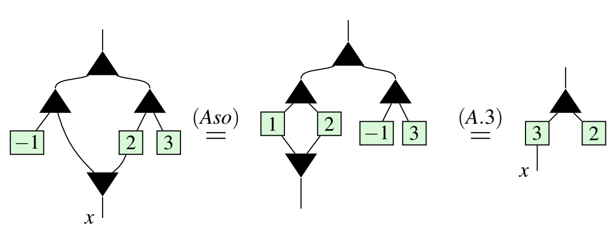
$$= \ (\tilde{\psi}_1 \boxtimes \tilde{\psi}_2) \boxplus (\tilde{\psi}_1 \boxtimes \tilde{\psi}_3)$$

□

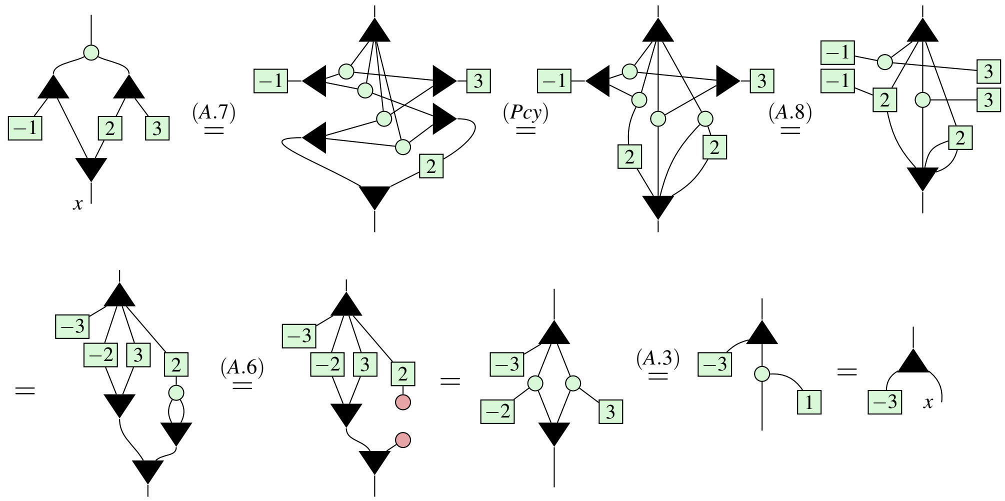
5.2 Arithmetic

Its been known since 2011 that  ,  can be used to add and multiply numberstates , respectively [1]. In the previous section we saw that  ,  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 together, 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 $x-3$.

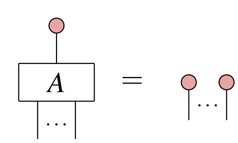


The reason for the missing $2x^2$ term is that (A.6) implies $x^2 = 0$. Other than that, controlled state arithmetic appears to faithfully reflect polynomial arithmetic. To help formalise this correspondence, we introduce the following definition.

Definition 5.1. A ZXW diagram with a single input on top is **arithmetic** if it contains only $|$, wires, , , nodes and boxes.

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

Lemma 5.10. *For any arithmetic diagram A,*

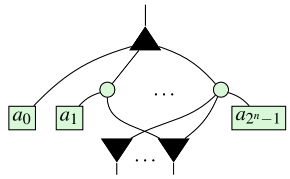


(5.4)

Proof. By definition, other than wires A contains only , , , and . All 's can be removed with (Ept). Meanwhile all the spiders copy due to (Bs0, K0, **??**) 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 , followed by a layer of , followed by a layer of , .

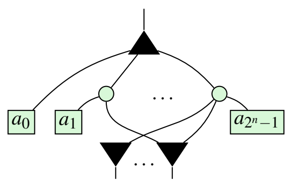
Definition 5.2. An n-output arithmetic diagram is said to be written in **polynormal form** (PNF) if it looks like:



The ith coefficient a_i is connected to the kth iff the kth bit in the binary expansion of i is 1.

This normal form is very closely related to the completeness normal form (see [3]). Simply applying (TA) to the 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.



$$= \begin{bmatrix} 1 & a_0 \\ 0 & a_1 \\ \dots & \dots \\ 0 & a_{2^n-1} \end{bmatrix} \tag{5.5}$$

Proof. See appendix B □

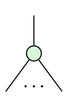
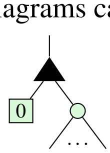
Thus, every controlled state can be represented as at least one arithmetic diagram (namely, its PNF). Moreover, we now show that any other arithmetic diagram can always be rewritten to its PNF.

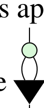
Proposition 4. All arithmetic diagrams can be written into PNF

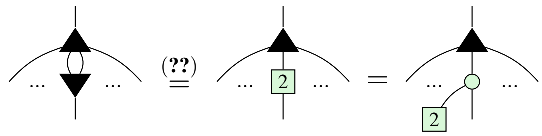
Proof. Let A be an arithmetic diagram. If $A =$, we are done.

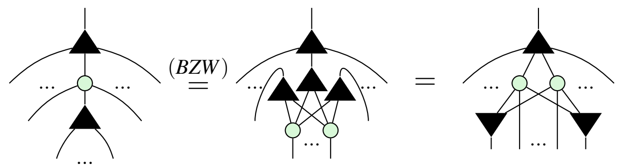
Otherwise, A has at least one output. First, we shall rewrite A into three layers, consisting of: (1) a single W at the top, (2) a layer of and (3) a layer of 's and 's. Then we shall collect terms and order the boxes to produce a PNF.

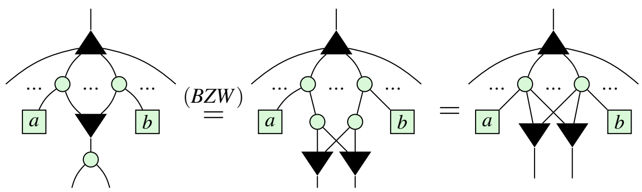
If the top of A is not already , it must be . It cannot be since the remaining arithmetic diagram would then have no inputs which is impossible. It cannot be since there is only one input and arithmetic diagrams cannot contain . Thus we can rewrite:

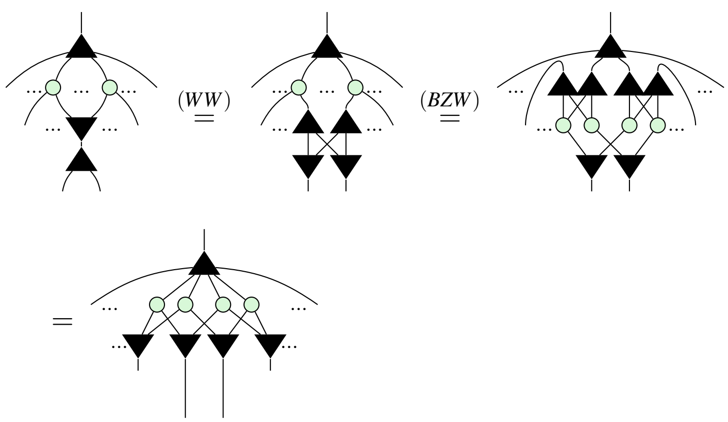
(1)  $\overset{(??)}{=}$ 

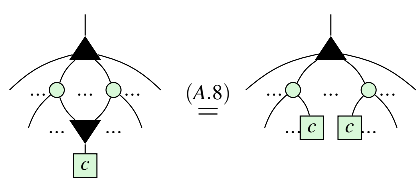
(1) guarantees there is a W at the top. We shall now repeatedly apply rewrites underneath the W until there are exactly three layers. Assume that fusion is applied as much as possible between each stage and (A.6) is applied and simplified with (K0) to remove  whenever possible. Then for as long as there are at least 4 layers, we can apply one of the following rewrites:

(2) 

(3) 

(4) 

(5) 

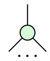
(6) 

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 ’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 ’s, use (A.5) to fuse them together.

(8) Pad: use (A.2) to insert $\boxed{0}$ for any connectivities that do not exist in A.

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

Step (7) ensures that every  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.

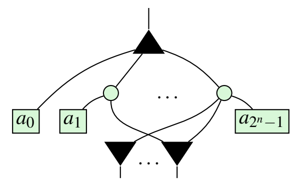
□

5.3 Isomorphism

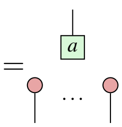
At last we can prove the isomorphism. Throughout we shall let $\mathscr{P}_n$ denote the ring $\mathbb{C}[x_1,\ldots,x_n]/(x_1^2,\ldots,x_n^2)$.

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

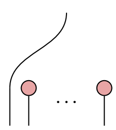
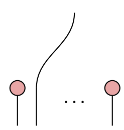
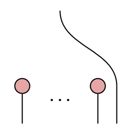
First, we shall define the map $\phi_n : \mathscr{P}_n \to \tilde{S}_n$ before proving it induces an isomorphism. ϕ_n is defined to map an arbitrary polynomial $p(x_1,\ldots,x_n) = a_0 + a_1 x_n + \ldots + a_{2^n-1} x_1 x_2 \ldots x_n$ to the following PNF:

$\phi_n(p) =$ 

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

$\phi_n(a) =$ 

And mapping indeterminates x_i:

$\phi_n(x_1) =$  $, \phi_n(x_2) =$  $, \ldots, \phi_n(x_n) =$ 

The full proof is found in appendix B.

6 Applications

References

[1] Coecke, B., Kissinger, A., Merry, A., and Roy, S. The ghz/w-calculus contains rational arithmetic. *arXiv preprint arXiv:1103.2812* (2011).

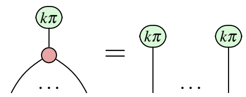
[2] Melliès, P.-A. Functorial boxes in string diagrams. In *International Workshop on Computer Science Logic* (2006), Springer, pp. 1–30.

[3] Poór, B., Wang, Q., Shaikh, R. A., Yeh, L., Yeung, R., and Coecke, B. Completeness for arbitrary finite dimensions of zxw-calculus, a unifying calculus. *arXiv preprint arXiv:2302.12135* (2023).

[4] Shaikh, R. A., Wang, Q., and Yeung, R. How to sum and exponentiate hamiltonians in zxw calculus. *arXiv preprint arXiv:2212.04462* (2022).

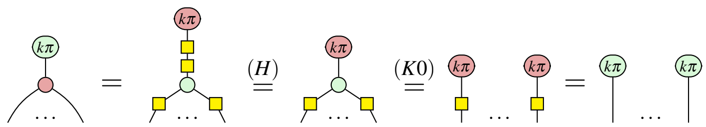
Appendix A Basic Lemmas

Lemma A.1.



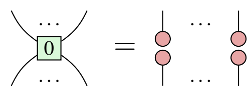
(A.1)

Proof.



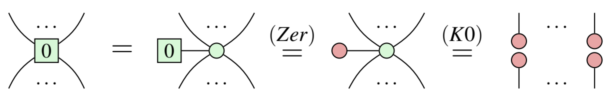
□

Lemma A.2.



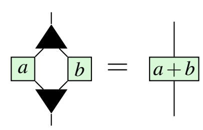
(A.2)

Proof.



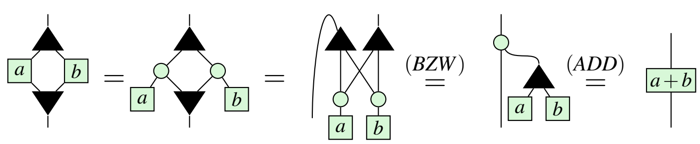
□

Lemma A.3.



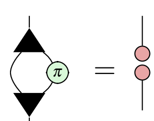
(A.3)

Proof.



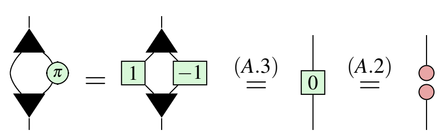
□

Lemma A.4.



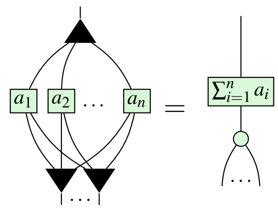
(A.4)

Proof.



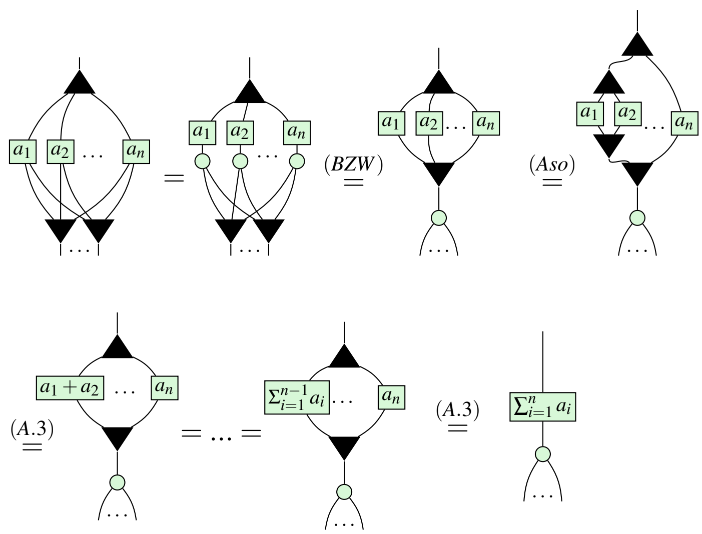
□

Lemma A.5.



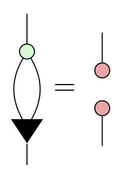
(A.5)

Proof.



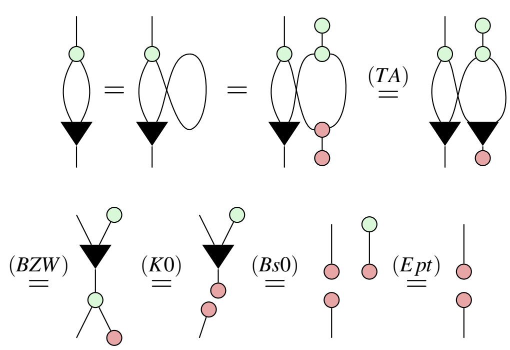
□

Lemma A.6.



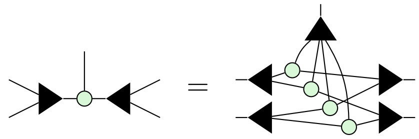
(A.6)

Proof.



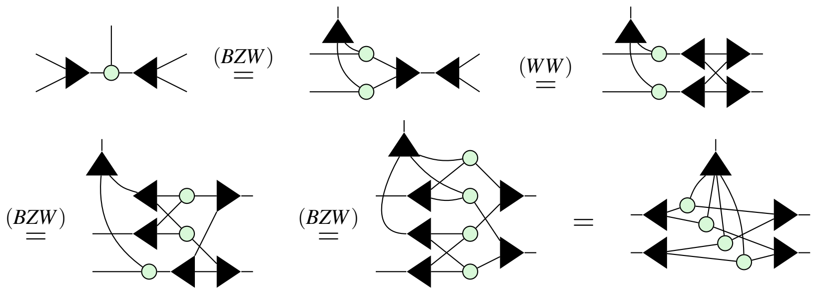
□

Lemma A.7.



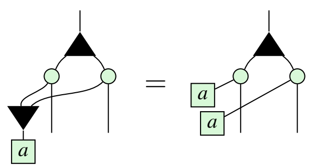
(A.7)

Proof.



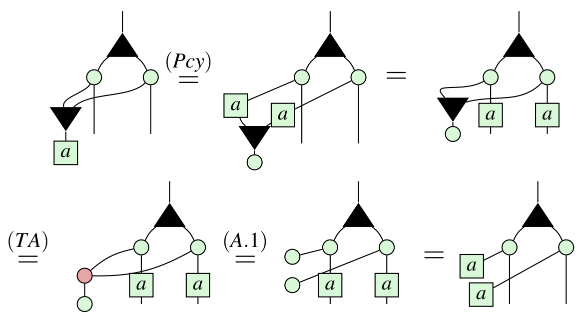
□

Lemma A.8.



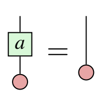
(A.8)

Proof.



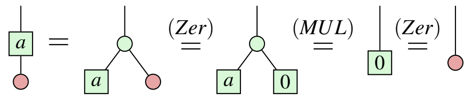
□

Lemma A.9.



(A.9)

Proof.



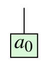
□

Appendix B Proofs

Proof of proposition 3

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:

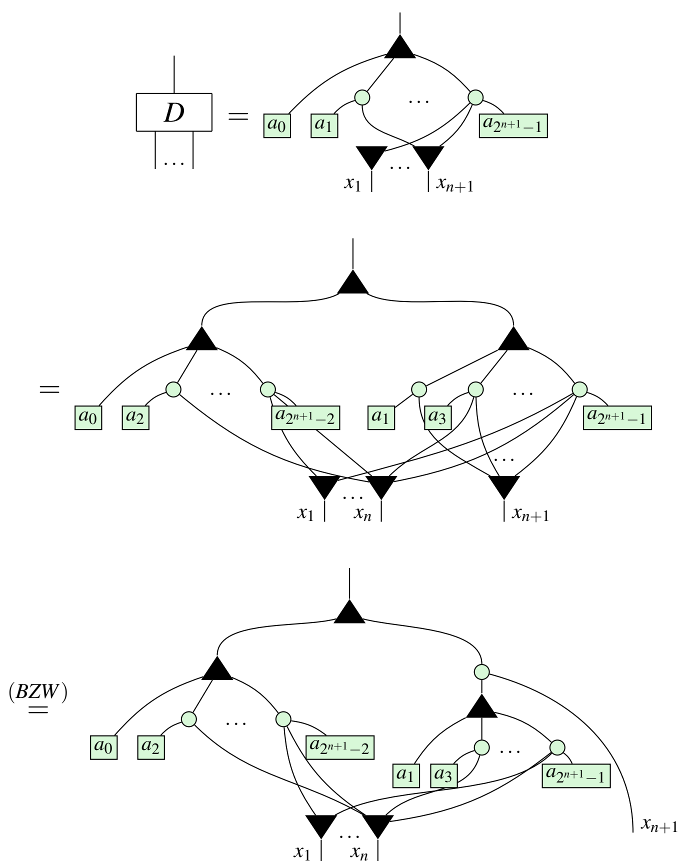


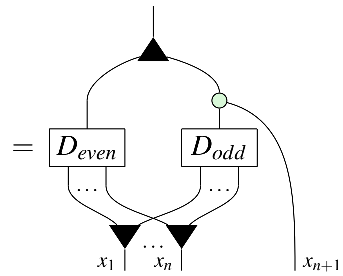
$$= \begin{bmatrix} 1 & a_0 \end{bmatrix}$$

as desired.

For inductive hypothesis, we assume that (5.5) 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:

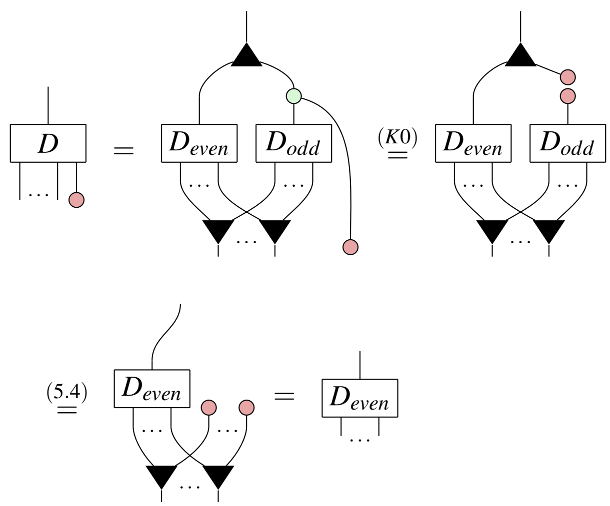




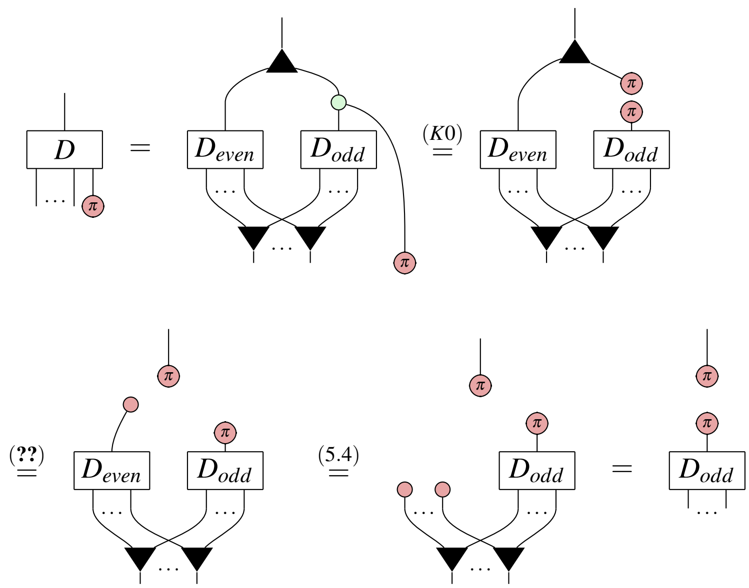
Where D_{even}, D_{odd} are PNF diagrams. Since they are over n variables, we can apply the inductive hypothesis and obtain:

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

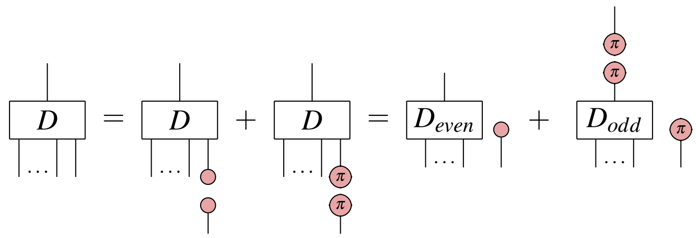
Next, plugging red we observe:



Meanwhile,



Summing these together,



$$= \ (D_{even} \otimes |0\rangle) + (D_{odd}|1\rangle\langle 1| \otimes |1\rangle)$$

$$\overset{(*)}{=} \begin{bmatrix} 1 & a_0 \\ 0 & a_2 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \end{bmatrix} \otimes |0\rangle + \begin{bmatrix} 0 & a_1 \\ 0 & a_3 \\ \dots & \dots \\ 0 & a_{2^{n+1}-1} \end{bmatrix} \otimes |1\rangle$$

$$= \begin{bmatrix} 1 & a_0 \\ 0 & 0 \\ 0 & a_2 \\ 0 & 0 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & a_1 \\ 0 & 0 \\ 0 & a_3 \\ \dots & \dots \\ 0 & 0 \\ 0 & a_{2^{n+1}-1} \end{bmatrix} = \begin{bmatrix} 1 & a_0 \\ 0 & a_1 \\ 0 & a_2 \\ 0 & a_3 \\ \dots & \dots \\ 0 & a_{2^{n+1}-2} \\ 0 & a_{2^{n+1}-1} \end{bmatrix}$$

Completing the inductive step. □

B.1 Isomorphism

Proof of Theorem 5.1

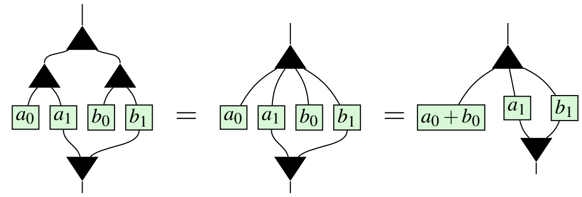
Proof. First, we show ϕ_n is a homomorphism, i.e.

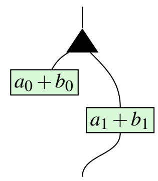
$$\forall p, q \in \mathscr{P}_n, \phi_n(p+q) = \phi_n(p) \boxplus \phi_n(q), \quad \phi_n(p \times q) = \phi_n(p) \boxtimes \phi_n(q)$$

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

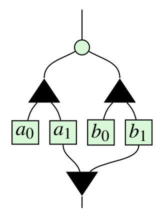
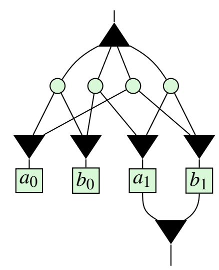
Base case: We have not defined controlled states for $n = 0$, so the base case begins with $n = 1$. Let $p, q \in \mathscr{P}_1$. Write as $p(x_1) = a_0 + a_1 x_1, q(x_1) = b_0 + b_1 x_1$, where $a_0, a_1, b_0, b_1 \in \mathbb{C}$. Then since

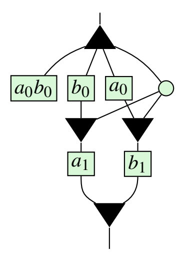
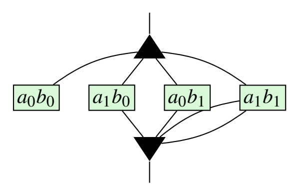
$p+q = a_0 + b_0 + (a_1+b_1)x_1$,

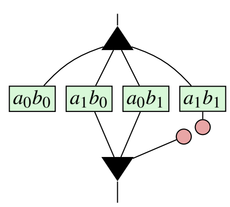
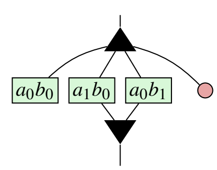
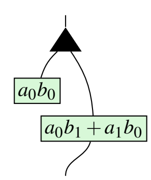
$\phi_1(p) \boxplus \phi_1(q) =$ 

$\overset{(A.3)}{=}$  $= \phi_1(p+q)$

Meanwhile, since $p \times q = a_0 a_1 + (a_0 b_1 + a_1 b_0)x_1$,

$\phi_1(p) \boxtimes \phi_1(q) =$  $\overset{(A.7)}{=}$ 

$\overset{(A.8)}{=}$  $\overset{(Pcy)}{=}$ 

$\overset{(A.6)}{=}$  $\overset{(A.9)}{=}$  $\overset{(A.3)}{=}$ 

$= \phi_1(p \times q)$

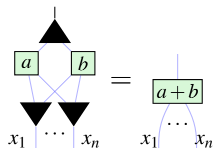
Completing the base case.

Inductive step:

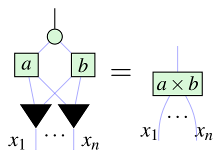
Let $Hom(n)$ assert than ϕ_n is a homomorphism. Then for the inductive step we wish to prove that $\forall n, Hom(n) \implies Hom(n+1)$.

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 $p(x_1,...,x_{n+1}) = a_0 + a_1 x_{n+1} + ... + a_{2^{n+1}-1} x_1 x_2 ... x_{n+1} \in \mathscr{P}_{n+1}$ as $p(x_{n+1}) = p_0 +$

$p_1 x_{n+1}$, where $p_0, p_1 \in \mathscr{P}_n$. 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 $x_1, \ldots, x_n$ will be drawn in light blue, while the x_{n+1} wires will be drawn in black. Thus the inductive hypothesis states that:



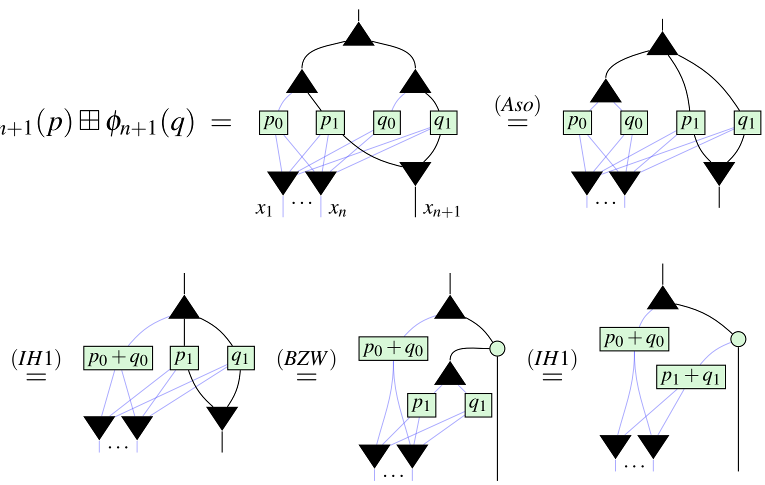
(IH1)



(IH2)

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

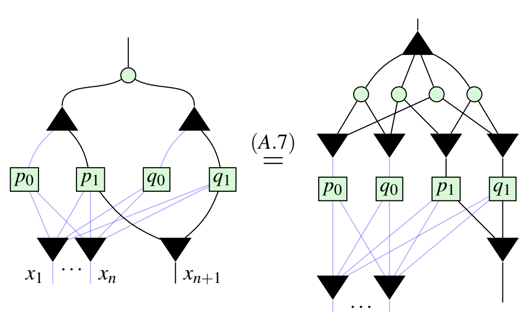
$\phi_{n+1}(p) \boxplus \phi_{n+1}(q) \;=$

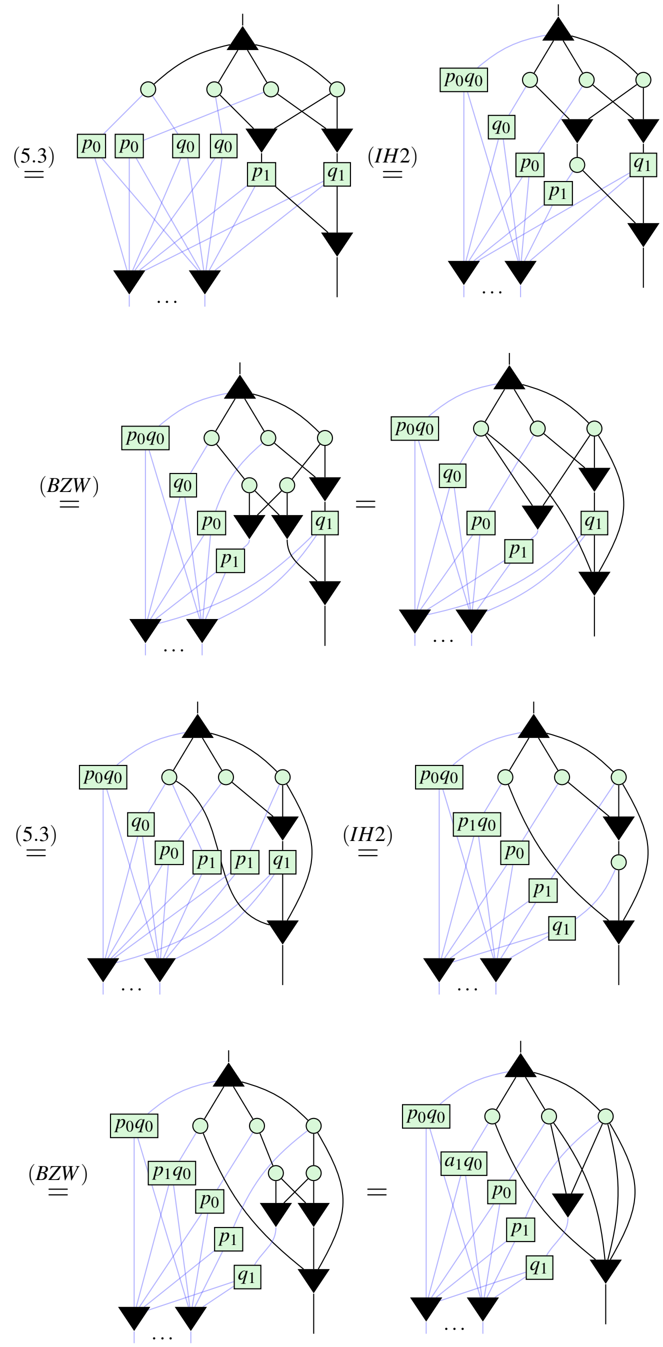


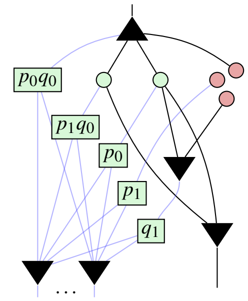
$$= \;\phi_{n+1}(p_0 + q_0 + (p_1 + q_1)x_{n+1}) \;=\; \phi_{n+1}(p+q)$$

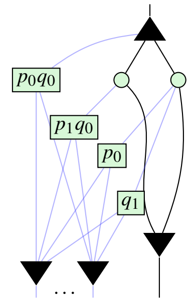
Similarly, for multiplication:

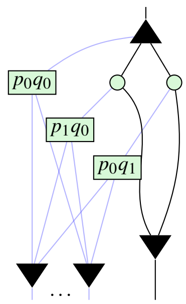
$\phi_{n+1}(p) \boxtimes \phi_{n+1}(q) \;=$

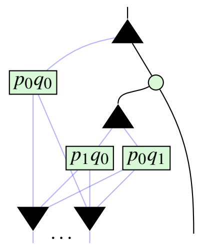


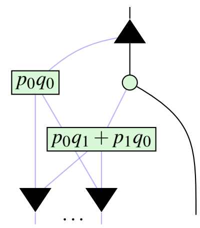

(5.3)
=
(IH2)
=
(BZW)
=
=
(5.3)
=
(IH2)
=
(BZW)
=
=

$\overset{(A.6)}{=}$ 

$\overset{(5.4,\textbf{??})}{=}$ 

$\overset{(IH2)}{=}$ 

$\overset{(BZW)}{=}$ 

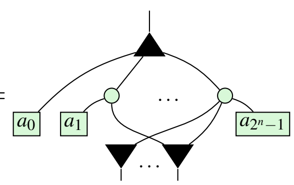
$\overset{(IH1)}{=}$ 

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

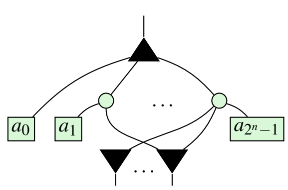
This completes the inductive step, proving that $\forall n > 1$, ϕ_n is a homomorphism.

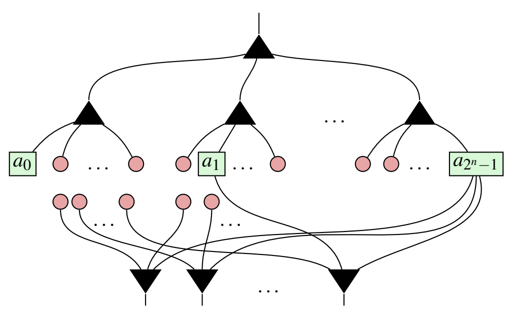
Finally, to see ϕ_n is an isomorphism, we use proposition 4 to write an arbitrary controlled state in PNF:

$$\begin{bmatrix} 1 & a_0 \\ 0 & a_1 \\ \dots & .. \\ 0 & a_{2^n-1} \end{bmatrix} =$$



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



$=$


$$= \ \phi_n(a_0) + \phi_n(a_1x_n) + \dots + \phi_n(a_{2^n-1 x_1 x_2 \dots x_n})$$

$$= \ \phi_n(a_0 + a_1x_n + \dots + a_{2^n-1}x_1x_2\dots x_n)$$

$\square$