ARITHMETIC ZXW DIAGRAMS ARE POLYNOMIALS

how to: equational reasoning with controlled diagrams

Edwin Agnew[1], Lia Yeh[1,2], Razin Shaikh[1,2], Richie Yeung[1,2]

[1]Department of Computer Science, University of Oxford, [2]Quantinuum, 17 Beaumont Street, Oxford

Quantum Graphical Calculi

Quantum graphical languages such as the ZX-, ZW-, and ZH-calculus reason about processes in quantum information, agnostic to the model of quantum computation (e.g. circuit-, measurement-, or fusion-based). Each diagram is identified with a linear map, and the calculus serves as an equational theory to derive proofs of mathematically equality entirely by rules equating diagrams.

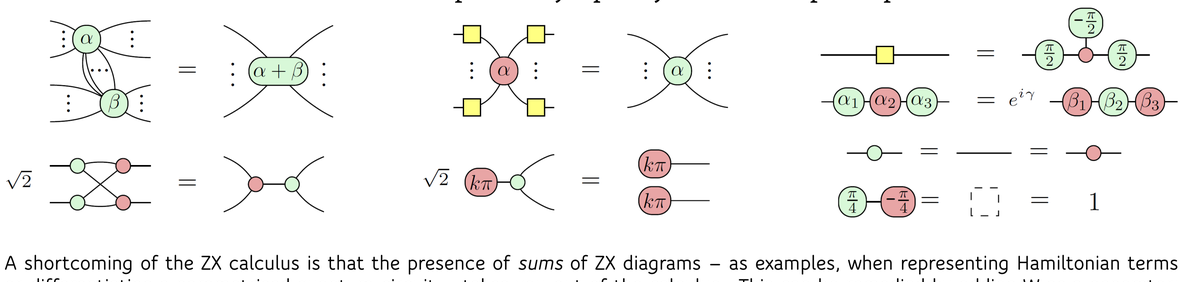
Capable of proving any equality of linear maps on any number of qubits (and as of 2023, any linear map in finite-dimensional Hilbert space!), these techniques have been applied to research topics across quantum computing – To list a few: quantum circuit optimisation (poster #571) and compilation (#575), photonic quantum computing (#681), and quantum error correction (#823).

The qubit ZX Calculus

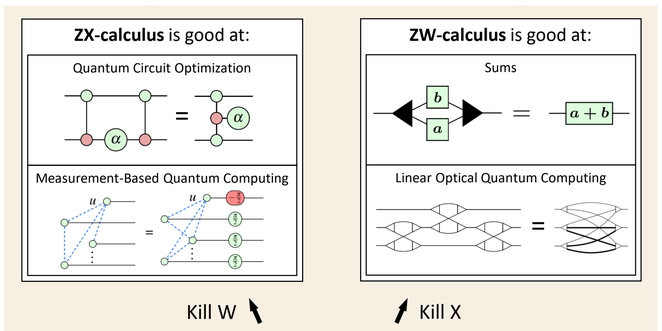
$$m\left\{ \vdots\ \alpha\ \vdots \right\}n \ :=\ |0\rangle^{\otimes n}\langle 0|^{\otimes m} \ +\ e^{i\alpha}\,|1\rangle^{\otimes n}\langle 1|^{\otimes m}$$

$$m\left\{ \vdots\ \alpha\ \vdots \right\}n \ :=\ |+\rangle^{\otimes n}\langle +|^{\otimes m} \ +\ e^{i\alpha}\,|-\rangle^{\otimes n}\langle -|^{\otimes m}$$

Its 8 rules suffice to prove any equality of linear maps on qubits:



A shortcoming of the ZX calculus is that the presence of *sums* of ZX diagrams – as examples, when representing Hamiltonian terms or differentiating a parametrised quantum circuit – takes you out of the calculus. This can be remedied by adding W as a generator:

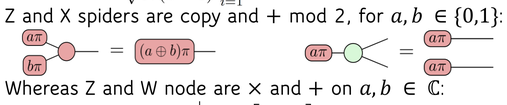


$$\llbracket\cdot\rrbracket \quad |00\rangle\langle 0| + \sum_{i=1}^{d-1}(|0i\rangle + |i0\rangle)\langle i|$$

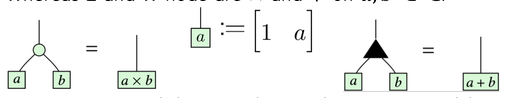
This generalises the qudit (d-dimensional) W state:

$$\left|W_N^d\right\rangle = \frac{1}{\sqrt{N(d-1)}}\sum_{i=1}^{d-1}(|i0\cdots 00\rangle + \cdots + |00\cdots 0i\rangle)$$

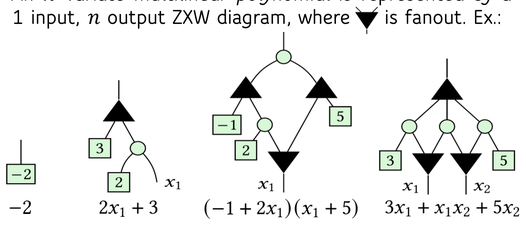
Z and X spiders are copy and + mod 2, for $a, b \in \{0,1\}$:



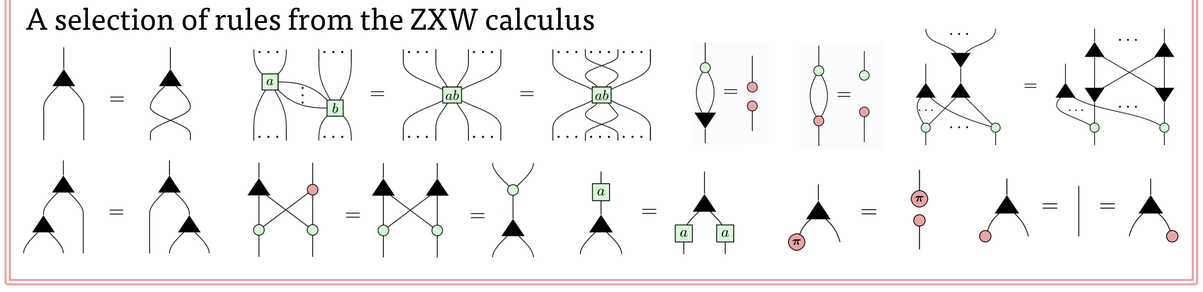
Whereas Z and W node are × and + on $a, b \in \mathbb{C}$:



An n-variate *multilinear polynomial* is represented by a 1 input, n output ZXW diagram, where ▼ is fanout. Ex.:



A selection of rules from the ZXW calculus

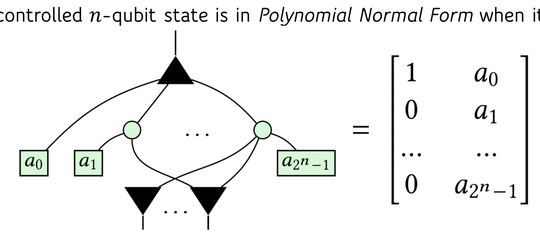


While it was known that $\left(\widetilde{\ a\ },\ \widetilde{\ \blacktriangle\ },\ \widetilde{\ \curlyvee\ }\right) \simeq (\mathbb{C}, +, \times)$, we show that the arithmetic structure is far richer through identifying the mathematical properties enabling the ZXW calculus completeness result for proving all equalities in finite-dimensional Hilbert space.

A ZXW diagram with a single input on top is **arithmetic** if it contains only $|$, ✕ wires, $\widetilde{\ \blacktriangle\ }$, $\widetilde{\ \curlyvee\ }$, $\widetilde{\ \blacktriangledown\ }$ nodes and $\widetilde{\ a\ }$ boxes.

Polynomial Normal Form

A ZXW diagram for an arbitrary controlled n-qubit state is in *Polynomial Normal Form* when it is of the form

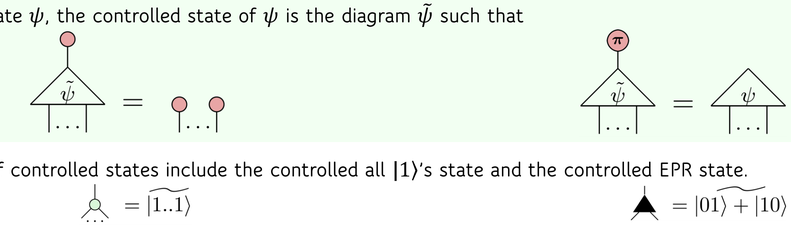


It is representable as the polynomial $a_0 + a_1x_n + \ldots + a_{2^n-1}x_1x_2\ldots x_n$; these are studied in multipartite entanglement.

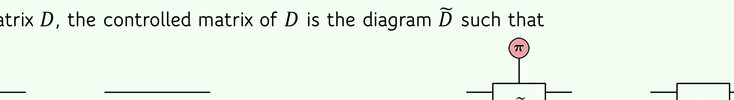
We provide an algorithm over rules of the ZXW calculus to write any arithmetic ZXW diagram into Polynomial Normal Form.

Controlled diagrams in the qubit ZXW calculus

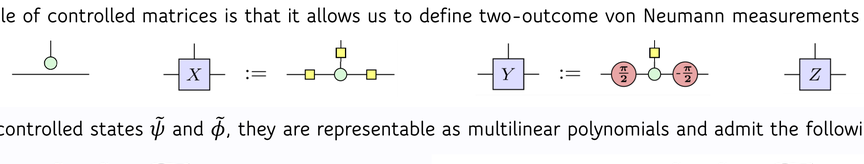
For an arbitrary state ψ, the controlled state of ψ is the diagram ψ such that



Notable examples of controlled states include the controlled all $|1\rangle$'s state and the controlled EPR state.



For an arbitrary square matrix D, the controlled matrix of D is the diagram $\widetilde{D}$ such that



A notable example of controlled matrices is that it allows us to define two-outcome von Neumann measurements for Pauli gadgets:

Given any two controlled states $\tilde{\psi}$ and $\tilde{\phi}$, they are representable as multilinear polynomials and admit the following operations:

The controlled state $\tilde{\psi} \boxplus \tilde{\phi} = \widetilde{\psi + \phi}$ is given by

and the controlled state $\tilde{\psi} \boxtimes \tilde{\phi} = \widetilde{\psi \times \phi}$ is given by

Given controlled matrices $\widetilde{M_1}$, ..., $\widetilde{M_k}$ and complex numbers c_1, ..., c_k, the controlled matrix $\widetilde{\sum_i c_i M_i}$ is given by

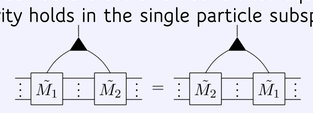
Main Results

Let $\widetilde{S^n}$ be the set of all controlled n-partite states. ($\widetilde{S^n}$,⊞,⊠) defines a commutative ring, i.e.:

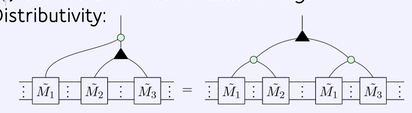
- ⊞ defines an Abelian group
- ⊠ defines a commutative monoid
- ⊠ distributes over ⊞

Likewise, let $\widetilde{M^n}$ be the set of all controlled square matrices on n qubits. ($\widetilde{M^n}$, $\widetilde{\ \blacktriangle\ }$, $\widetilde{\ \curlyvee\ }$) defines a non-commutative ring.

Commutativity holds in the single particle subspace setting:



Distributivity:

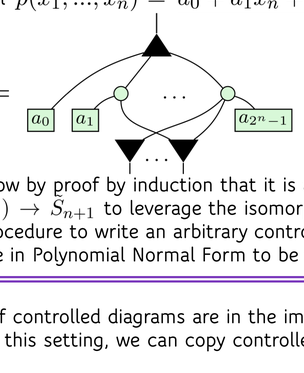


Polynomial Isomorphism Theorem of ZXW Controlled Diagrams

There is an isomorphism $\mathcal{P}_n = \widetilde{S_n}$, of multilinear polynomials $\mathcal{P}_n := \mathbb{C}[x_1, ..., x_n]/(x_1^2, ..., x_n^2)$ to the commutative ring ($\widetilde{S^n}$,⊞,⊠).

Proof idea: For an arbitrary multilinear polynomial $p(x_1, ..., x_n) = a_0 + a_1x_n + \ldots + a_{2^n-1}x_1x_2\ldots x_n$,

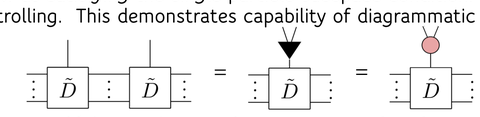
$$\phi_n(p) \ =$$



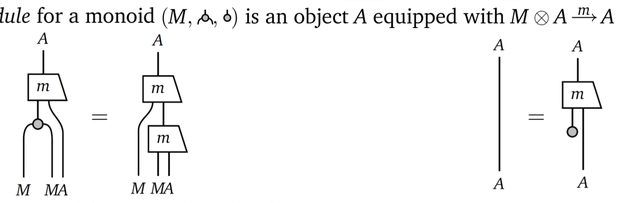
We first define the map $\phi_n : \mathcal{P}_n \to \tilde{S}_n$ and show by proof by induction that it is a homomorphism.
The inductive step extends it to $\mathcal{P}_n[x_{n+1}]/(x_{n+1}^2) \to \tilde{S}_{n+1}$ to leverage the isomorphism $\mathcal{P}_n[x_{n+1}]/(x_{n+1}^2) \simeq \mathcal{P}_{n+1}$.
Finally, ϕ_n defines an isomorphism: We give a procedure to write an arbitrary controlled state to Polynomial Normal Form, and conversely can interpret any controlled state in Polynomial Normal Form to be the image of ϕ_n for some polynomial.

In an arithmetic ZXW diagram, when all control wires of controlled diagrams are in the image of the same W node, these controls are collectively restricted to a single particle subspace. In this setting, we can copy controlled diagrams without violating no-cloning!

Consider the two controlled wires below as satisfying the single particle subspace condition. Then, the controlled matrix is copyable, irrespective of which diagram it is controlling. This demonstrates capability of diagrammatic equational reasoning with black boxes.



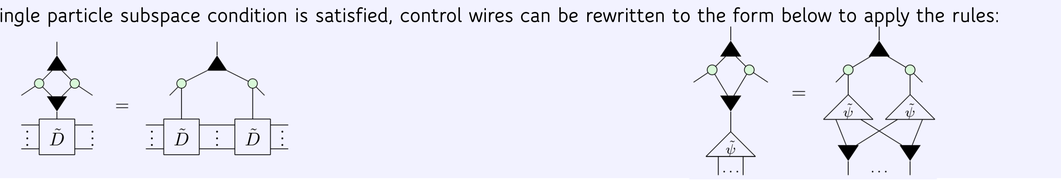
In a monoidal category, a *module* for a monoid $(M, \blacktriangle, \circ)$ is an object A equipped with $M \otimes A \xrightarrow{m} A$ satisfying:



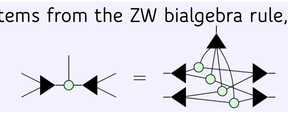
The morphism m is called an *action* of the monoid on the object A.

We remark that each controlled square matrix in $\widetilde{M^n}$ satisfies these relations as to be an action of the monoid $(M, \blacktriangle, \circ) = (\mathbb{C}^2, \blacktriangle, \bullet)$ but for one caveat: Instead of the usual tensor product, the monoidal product must preserve the single particle subspace condition.

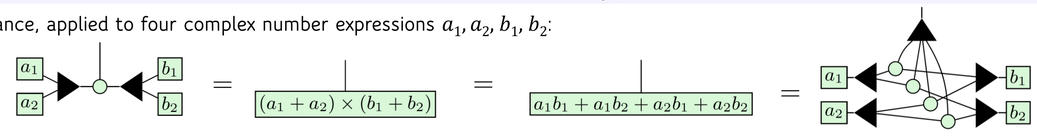
When the single particle subspace condition is satisfied, control wires can be rewritten to the form below to apply the rules:



The ability to copy arbitrary controlled diagrams stems from the ZW bialgebra rule, which captures distributivity of ⊠ over ⊞.



For instance, applied to four complex number expressions a_1, a_2, b_1, b_2:

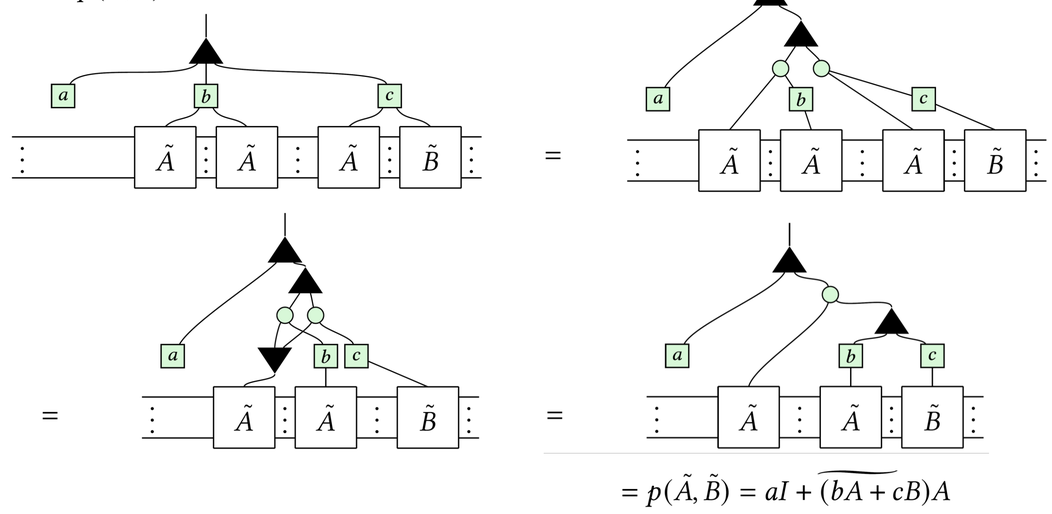


Moreover, an arithmetic ZXW diagram controlling a sequence of controlled matrices gives a *multivariate polynomial over matrices*.

We can thus leverage our graphical rewrite rules for both arithmetic ZXW diagrams and controlled diagrams, to factor them. This may aid Hamiltonian circuit optimisation and compilation; see poster #681 for Hamiltonian exponentiation applied to nonlinear optics.

To show a factorisation example of a multivariate polynomial over matrices, for same size square matrices I, A, B and $a, b, c \in \mathbb{C}$:

$$p(\tilde{A}, \tilde{B}) = aI + \widetilde{bA^2 + cBA} =$$



$$= p(\tilde{A}, \tilde{B}) = aI + \widetilde{(bA + cB)A}$$

Applications

Algebraic complexity

VP (the class of polynomially sized polynomials) is considered the algebraic analogue of P, while VNP (the class of polynomials such that the coefficient of any monomial is efficiently computable) is considered the algebraic analogue of NP. Clearly, VP ⊆ VNP.

We define an algebraic analogue of BQP, the class of polynomials corresponding to polynomially sized quantum circuits:

A family of polynomials f_n is in VQP iff for every n there exists a polynomially sized quantum circuit Q_n on n qubits such that $f_n = pQn|0\ldots0\rangle$.

We further prove that VNP ⊆ VQP ⇒ P#P ⊆ BQP. As P#P ⊆ BQP seems highly implausible, we conjecture that VNP ⊈ VQP.

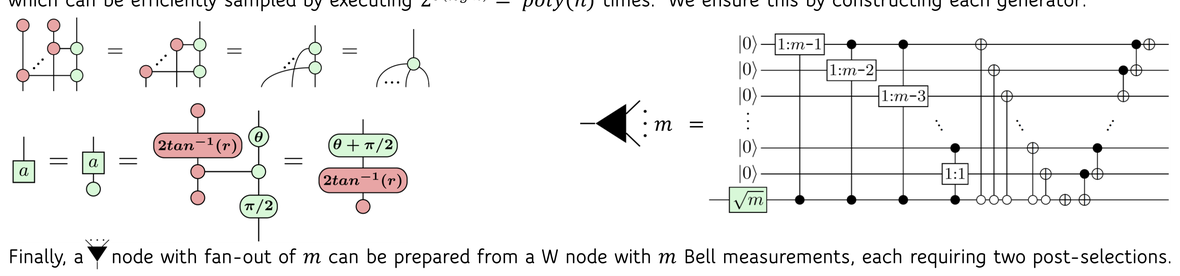
Entanglement detection

Let $A = \mathbb{C}^{2^{\otimes n}}, B = \mathbb{C}^{2^{\otimes m}}$. Let $X = \{x_1, ..., x_n\}, Y = \{y_1, ..., y_m\}$ be the corresponding indeterminates. Let $|\psi\rangle_{AB}$ be a bipartite pure state. Then $|\psi\rangle$ is separable iff each irreducible factor of p_ψ (over $\mathbb{C}[x_1, ..., x_n, y_1, ..., y_m]$) is an X-poly or Y-poly.

Therefore, whether a bipartite pure state is entangled or separable is computable through polynomial factorisation.

Quantum circuit sampling of arithmetic ZXW diagrams

Consider an arbitrary polysize arithmetic ZXW diagram with at most $O(\log n)$ W nodes, $O(\log n)$ Z phases of non-unit magnitude, and $O(\log n)$ ▼ nodes with $O(\log n)$ bounded fan-out. Then it is synthesisable as a quantum circuit with $O(\log n)$ post-selections, which can be efficiently sampled by executing $2^{O(\log n)} = poly(n)$ times. We ensure this by constructing each generator:



Finally, a ▼ node with fan-out of m can be prepared from a W node with m Bell measurements, each requiring two post-selections.

References

E Agnew (2023). Quantum Polynomials in the ZXW Calculus. Master's thesis at the University of Oxford.
B Poor, Q Wang, R Shaikh, L Yeh, R Yeung, B Coecke (2023). Completeness for arbitrary finite dimensions of ZXW-calculus, a unifying calculus. In 38th Annual ACM/IEEE Symposium on Logic in Computer Science.
R Shaikh, Q Wang, R Yeung (2022). How to Sum and Exponentiate Hamiltonians in ZXW Calculus. In 19th International Conference on Quantum Physics and Logic.
R Vilmart (2019). A near-minimal axiomatisation of zx-calculus for pure qubit quantum mechanics. In 34th Annual ACM/IEEE Symposium on Logic in Computer Science.
L Yeh (2023). Scaling W State Circuits in the qudit Clifford Hierarchy. In 1st International Workshop on the Art, Science, and Engineering of Quantum Programming.