REASONING ABOUT ERRORS USING $\sqrt{\Pi}$

This paper represents a simple quantum error correction circuit in $\sqrt{\Pi}$. The language provides a sound and complete equational theory and is universal for quantum *computation*. However, it lacks much of the functionality needed to handle errors. We investigate the required additional structure and extend the language accordingly.

1. Introduction

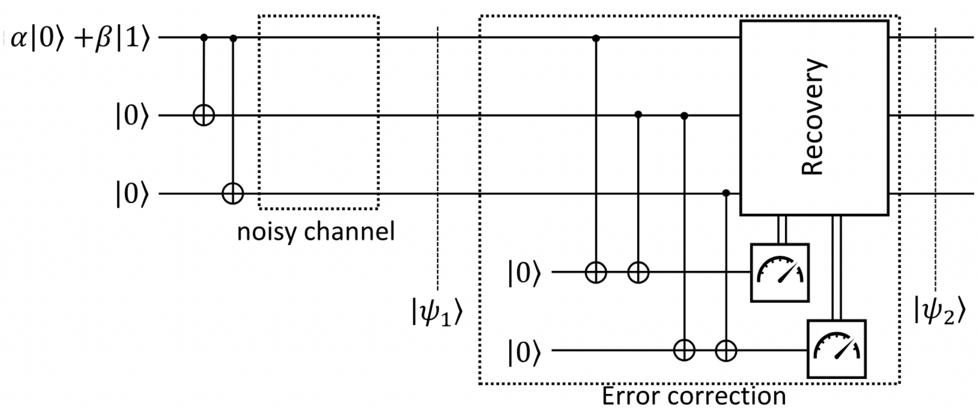
Previous work [2] in categorical quantum theory establishes that the category **Unitary**, which includes finite-dimensional Hilbert spaces as objects and unitary transformations as morphisms, captures the categorical semantics for pure state quantum *computing*. **Unitary** forms a canonical model for the language $\sqrt{\Pi}$ as it is a rig category equipped with morphisms $\omega : I \to I$ representing scalars and $V : I \oplus I \to I \oplus I$ as square root of X gate such that following equations are satisfied:

$$(E1) \quad \omega^8 = \mathrm{id}$$

$$(E2) \quad V^2 = \sigma_{\oplus} = X$$

$$(E3) \quad V \circ S \circ V = \omega^2 \cdot S \circ V \circ S, \text{ where } S : I \oplus I \to I \oplus I \text{ is given by } S = \mathrm{id} \oplus \omega^2$$

The above three equations and the existence of scalars as $I \to I$ satisfying certain coherence conditions is enough to extend the classical reversible language Π to a universal quantum language $\sqrt{\Pi}$ developed in [3]. This extension alters the semantics from a rig groupoid of finite sets and bijections to a unitary rig groupoid. In $\sqrt{\Pi}$, the two-dimensional additive structure $[\![I \oplus I]\!]$ is interpreted as qubits, whereas in *Pi*, it was interpreted as bits or booleans. This distinction is significant and will be referenced later. Quantum circuits over qubits are represented as compositions of morphisms defined by the rig structure. For example, consider the circuit for a 3-qubit flip code.



The base language of $\sqrt{\Pi}$ imposes that the number of wires must remain constant throughout the entire circuit, i.e. it is impossible to temporarily allocate an ancilla, use it during a sub-expression, and discard it afterward. This shortcoming is a problem for encoding part of the circuit. Since, in the encoding part, one needs to tensor an arbitrary incoming quantum state with two ancilli qubits initialized to $|0\rangle$.

We fix this by extending the language to account for state preparation and effects using techniques in [2]. All ancilla systems are generated by a single object $I \oplus I$; therefore, there is a subcategory $\mathrm{Gen}_{I\oplus I}(\mathbf{Unitary})$ generated by taking arbitrary monoidal products of a single generating object $I \oplus I$ with itself, with only monoidal coherence isomorphisms between them.

This gives a strict monoidal embedding $\mathfrak{F}_{I\oplus I} : \mathrm{Gen}_{I\oplus I}(\mathbf{Unitary}) \to \mathbf{Unitary}$ given by the identity of objects and morphisms. From this, we construct a category $\mathbf{Unitary}_{I\oplus I}$ such that its:

- objects are same as in **Unitary**.
- morphisms $A \to B$ are equivalence classes of triples $[U, f, V]$ consisting of two objects U and V of $\mathrm{Gen}_{I\oplus I}(\mathbf{Unitary})$ and a morphism $A \otimes \mathfrak{F}_{I\oplus I}(U) \to B \otimes \mathfrak{F}_{I\oplus I}(V)$ under the equivalence $\sim$ below.
- the identity $A \to A$ is the equivalence class of $\mathrm{id}_{A\otimes I}$.
- the composite of $[U, f, V]$ and $[W, g, X]$ with $f : A \otimes \mathfrak{F}_{I\oplus I}(U) \to \mathfrak{F}_{I\oplus I}$ and $g : B \otimes \mathfrak{F}_{I\oplus I} \to C \otimes \mathfrak{F}_{I\oplus I}(X)$ is the equivalence class of representative $A \otimes \mathfrak{F}_{I\oplus I}(U \otimes W) \to C \otimes \mathfrak{F}_{I\oplus I}(V \otimes X)$ in **Unitary** given by,

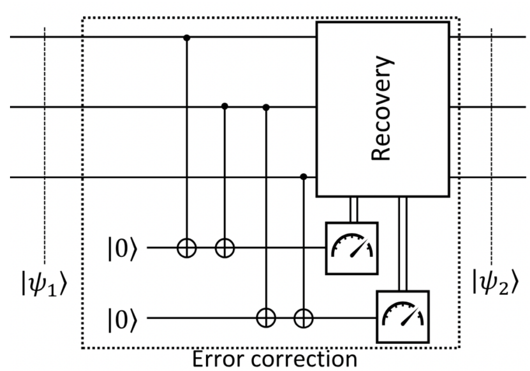
$$[U \otimes W, \alpha_{\otimes} \circ g \otimes \mathrm{id}_{\mathfrak{F}_{I\oplus I}(V)} \circ \alpha_{\otimes}^{-1} \circ \mathrm{id}_B \otimes \sigma_{\otimes} \circ \alpha_{\otimes} \circ f \otimes \mathrm{id}_{\mathfrak{F}_{I\oplus I}(V)} \circ \alpha_{\otimes}^{-1}, X \otimes V]$$

Now we can choose $|0\rangle$ as the distinguished state $I \to I \oplus I$ and $\langle 0|$ as the distinguished effects $I \oplus I \to I$. This gives us an interpretation functor $[\![\_]\!] : \mathbf{Unitary}_{I\oplus I} \to \mathbf{Contraction}$ by Prop. 23 in [2] which gives semantics of $\sqrt{\Pi}$ in **Contraction** where **Contraction** is the category of finite-dimensional Hilbert spaces and contractions. This category contains all states as morphisms $I \to A$ (isometries), all effects as morphisms $A \to I$ (coisometries). Therefore, the model $\mathbf{Unitary}_{I\oplus I}$ and **Unitary** of $\sqrt{\Pi}$ embeds in **Contraction**, the universal dagger rig category containing all unitaries, states, effects [1]. We can now prepare states as primitive $|0\rangle : I \to \mathbb{2}$ and derived $|1\rangle = |0\rangle \odot X$. With the ability to manipulate ancilli systems, the encoding can be expressed as follows.

```
encode-qubits : 𝟚 ↔ 𝟚ᴸ
encode-qubits = uniti★r ⊙ uniti★r ⊙
                ((id↔ ⊗ zero) ⊗ zero) ⊙
                (CX ⊗ id↔) ⊙
                assocr★ ⊙
                (id↔ ⊗ CX)
```

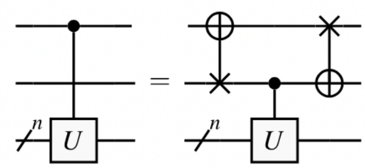
Here, $\mathbb{2}^L$ denotes the logical qubit. We have added redundancy by using controlled X gates by making three copies of the initial state. Conceptually, $(\alpha|0\rangle + \beta|1\rangle) \otimes (|0\rangle \otimes |0\rangle) \mapsto \alpha|000\rangle + \beta|111\rangle$. This logical qubit is sent through some noisy channel before we can compute syndrome using two ancilli initialized to $|0\rangle$. The following function applies as a series of controlled X gates to ancilli.

```
compute-syndrome : 𝟚ᴸ ×ᵤ I ×ᵤ I ↔ 𝟚ᴸ ×ᵤ I ×ᵤ I
compute-syndrome =
id↔ ⊗ zero ⊗ zero ⊙
(id↔ ⊗ id↔ ⊗ id↔) ⊗ id↔ ⊙
assocl★ ⊗ id↔ ⊙
(cnot-swap ⊗ id↔) ⊗ id↔ ⊙
```



```
assocr⋆ ⊗ id↔ ⊙
(id↔ ⊗ cnot-swap) ⊗ id↔ ⊙
assocr⋆ ⊙
id↔ ⊗ (id↔ ⊗ id↔) ⊙
id↔ ⊗ assocr⋆ ⊙
id↔ ⊗ id↔ ⊗ assocl⋆ ⊙
id↔ ⊗ id↔ ⊗ cnot-swap ⊗ id↔ ⊙
id↔ ⊗ id↔ ⊗ assocr⋆ ⊙
id↔ ⊗ id↔ ⊗ id↔ ⊗ CX ⊙
reassociate ⊙
id↔ ⊗ id↔ ⊗ uncnot-swap ⊗ id↔ ⊙
id↔ ⊗ assocl⋆ ⊙ {!!}
```

We could do the encoding part easily because we only needed the ability to manipulate ancillary systems. However, computing syndrome poses multiple problems. Firstly, the above program is very long. This is so because $\sqrt{\Pi}$ only provides combinators to apply controlled gates to adjacent qubits. To apply CX gate to non-adjacent qubits we use a series of controlled SWAP gates to make the wires adjacent, apply CX and reverse the swapping to get to the original state. This trick ensures that the long-range CNOT gate decomposition produces both the lowest number of CNOT gates and circuit depth, in this sequential order, in the literature [5]. We can also use SWAP gates to make wires adjacent, but it does not reduce the size of the program.



From above, we can introduce ancilla and apply the series of controlled gates, but to compute syndrome and apply corrections at the end $\sqrt{\Pi}$ lacks three important features:

- $\sqrt{\Pi}$ should have a distinction between classical bits and qubits.
- There is no way to do a *non-destructive measurement* to get the syndrome values.
- There is no way to apply the corrections based on syndrome values.

Measuring the ancilli should yield a classical bit. This is essential since we need to work with these bits to correct the error accordingly and get back to the original state. Moreover, to use the classical measured values and correct a logical quantum state, we need a notion of non-destructive measurement in a *hybrid* language that allows us to manipulate classical bits and qubits together.

There are at least two ways in the literature of ZX calculus to tackle these problems.

The first one [13] is based on extending GHZ/W calculus, which uses interactions between three-partite entangled states instead of two complementary states with Selinger's CPM construction [12]. Although the document seems incomplete, the author claims that this combination results in a purely graphical verification of quantum error-correcting codes.

Secondly, we have [7] where the authors use ZX calculus and Quantomatic to verify the correctness of the 3-qubit flip circuit. All steps performed until the syndrome measurement are similar to ours. After measurement, the authors use tagged Z, X nodes to denote which gate needs to be applied to which *qubit* according to measured *bits* and use ZX reductions to show that the composition of encoder, corrector and decoder is reduces to identity thus, verifying correctness.

ZX calculus is a graphical language for quantum theory it deals with *linear maps* between Hilbert spaces whereas $\sqrt{\Pi}$ is a language for quantum computing as it works with *unitaries* between Hilbert spaces. To fix the these problems, we will use techniques from [1, 8, 2] to step by step build a hybrid quantum-classical language on top of $\sqrt{\Pi}$. We will start with adding partiality to our model of $\sqrt{\Pi}$ using the two-step arrow construction [8] associated with information effects of *allocation* and *hiding*. This gives us a combination of classical cloning and discarding using which we can define a measurement combinator `measure: 𝟚 ⇝ 𝟚` defined as `measure = clone ⋙ fst` as in [2, 8]. Semantically $[\![\texttt{measure}]\!]$ is described in **CPTP** of finite dimensional Hilbert spaces and completely positive trace preserving maps between them. Measurement is an inherently *irreversible* operation therefore, we consider mixed states given by density matrices. A density matrix corresponds to the morphism $\rho : H \to H$ such that for all $0 \leq \langle \rho(\psi)|\psi\rangle \leq 1$. Thus any pure state $|\psi\rangle$ is also a mixed state $|\psi\rangle\langle\psi| : H \to H$. We interpret using the measurement instrument channel w.r.t. classical states $\{|b\rangle_i\}_{i\in I}$ [8]

$$\rho \mapsto \Sigma_{i\in I} |b_i\rangle\langle b_i|\,\rho\,|b_i\rangle\langle b_i|$$

sending quantum states to mixed states. Consider an arbitrary qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, and the associated density matrix:

$$|\phi\rangle\langle\phi| = (\alpha|0\rangle + \beta|1\rangle)(\alpha\langle 0| + \beta\langle 1|).$$

Conjugating by $[\![\text{clone}]\!]$ yields matrix:

$$\begin{aligned}[\![\text{clone}]\!]\,|\phi\rangle\langle\phi|\,[\![\text{clone}]\!]^\dagger &= \alpha|00\rangle + \beta|11\rangle)(\alpha\langle 00| + \beta\langle 11|)\\ &= |\alpha|^2|00\rangle\langle 00| + \alpha\bar{\beta}|00\rangle\langle 11| + \beta\bar{\alpha}|11\rangle\langle 00| + |\beta|^2|11\rangle\langle 11|\end{aligned}$$

$[\![\text{fst}]\!]$ is given by the partial trace of density matrices:

$$\begin{aligned}&[\![\text{fst}]\!]\big(|\alpha|^2|00\rangle\langle 00| + \alpha\bar{\beta}|00\rangle\langle 11| + \beta\bar{\alpha}|11\rangle\langle 00| + |\beta|^2|11\rangle\langle 11|\big)\\ &= |\alpha|^2\,\text{tr}(|0\rangle\langle 0|)\,|0\rangle\langle 0| + \alpha\bar{\beta}\,\text{tr}(|0\rangle\langle 1|)\,|0\rangle\langle 1|\\ &\quad + \beta\bar{\alpha}\,\text{tr}(|1\rangle\langle 0|)\,|1\rangle\langle 0| + |\beta|^2\,\text{tr}(|1\rangle\langle 1|)\,|1\rangle\langle 1|\\ &= |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|.\end{aligned}$$

As pointed out by the authors the problem here is that although the language now has a notion of irreversibility it is still quantum and thus there is not way to describe $[\![\texttt{Bit}]\!]$. Moreover, measurement should have type `QBit` $\to$ `Bit` but here it is `Qbit` $\to$ `QBit`. This interpretation takes the second road to classicality [4] that of *decoherence* since `measure` is a causal operation that sets all off-diagonal entries of a density matrix to 0. We can use the $\textbf{Split}^{\perp}_{=}$ construction from [4, 6] as described in [1] to *classicise* our language by adding classical types interpreted as C* algebras since there is an equivalence $\textbf{Split}^{\perp}_{=}(\textbf{FHilb}_{\text{CPTN}}) \simeq \textbf{FCStar}_{\text{CPTN}}$. I think having this type level distinction between type of bits and type of qubits as in QPL [11] would allow manipulation of bits which is needed to express the error correction circuit we started with.

2. Construction

$\sqrt{\Pi}$ is a universal language for quantum computing and has its semantics in **Unitary** as mentioned before. **Unitary** has a rig structure, i.e., it is symmetric monoidal in two different ways such that the monoidal product distributes over the other satisfying 24 coherence conditions [10]. In context of Hilbert spaces this corresponds to $(\otimes, I)$ and $(\oplus, O)$ i.e. the tensor product and direct sum such that

$\otimes$ distributes over $\oplus$ (upto natural isomorphism) via distributors $\delta^L : A \otimes (B \oplus C) \to (A \otimes B) \oplus (A \otimes C)$ and $\delta^R : (A \oplus B) \otimes C \to (A \otimes C) \oplus (B \otimes C)$ and annihilators $\delta_0^L : O \otimes A \to O$ and $\delta_0^R : A \otimes O \to O$. It is also a dagger structure ($f^{-1} = f^{\dagger}$) such that all coherence isomorphisms are unitary. We will use affine completions for two monoidal structures of this dagger rig category to introduce notions of partiality and discarding [1]. If there is a unique morphism $A \to I$ for any object A, the monoidal category is called *affine*, and if there is a unique morphism $I \to A$ for any object A, it is called coaffine.

2.1. **Additive Affine Completion of Unitary.** We can think of a partial map as $A \to B \oplus E$ as a usual map $A \to B$ extended with extra part E. Moreover, it does not matter how one represents this extra part. For example, consider $f : A \to B \oplus E$ some maps $m : E \to E'$ then, $(\mathrm{id} \oplus m) \circ f$ describes the same map as f. Therefore, there is a preorder for maps $f : A \to B \oplus E$ and $f' : A \to B \oplus E'$ as $f \leq_L f'$ iff there exists some mediator $m : E \to E'$ such that the diagram commutes.

$$\begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "f'"] & \\ B \oplus E \arrow[rr, "id \oplus m"'] & & B \oplus E' \end{tikzcd}$$

We will be considering the equivalence closure (lease equivalence relation) $\sim_{L_\oplus}$ of this partial order. For **Unitary** its additive affine completion $L_\oplus(\textbf{Unitary})$ is the category whose

- objects are same as **Unitary** (Hilbert Spaces);
- morphisms are pairs $[f, E] : A \to B$ of an equiv. class of morphisms $f : A \to B \oplus E$ under $\sim_{L_\oplus}$;
- identities $A \to A$ are pairs $[\rho_\oplus^{-1}, O]$ (where $\rho_\oplus$ is the right unitor $A \oplus O \to A$);
- composition of $[f, E] : A \to B$, $[g, E'] : B \to C$ is $[\alpha_\oplus \circ g \otimes \mathrm{id}_E \circ f, E' \oplus E]$.

The dual construction *additive coaffine completion* $R_\oplus(\textbf{Unitary})$ is defined as $L_\oplus(\textbf{Unitary}^{\mathrm{op}})^{\mathrm{op}}$ such that morphisms in $R_\oplus(\textbf{Unitary})$ hide the part of source/input i.e. $f : A \to B$ corresponds to $f : A \oplus H \to B$ where H can be thought of as *heap* and f as a program that takes A as input and *may* use the heap H in producing B. Again, we do not care about the actual contents of the heap so we can identity f with $f \circ (\mathrm{id}_A \oplus H) : A \oplus H' \to B$ where $h : H' \to H$ preprocesses the heap. Like before, we will work with $\sim_{R_\oplus}$ generated by this diagram.

$$\begin{tikzcd} & B & \\ A \oplus H \arrow[ur, "f"] & & A \oplus H' \arrow[ul, "f'"'] \arrow[ll, "id \oplus h"] \end{tikzcd}$$

Neither $L_\oplus(\textbf{Unitary})$ nor $R_\oplus(\textbf{Unitary})$ are *dagger* rig categories. This is because, by Proposition 6 in [1], $R_\oplus(\textbf{Unitary}) \simeq \textbf{Isometry}$, which implies that $L_\oplus(\textbf{Unitary}) \simeq \textbf{coIsometry}$. Both of these structures are only rig categories. Interestingly when composed as $L_\oplus(R_\oplus(\textbf{Unitary}))$ or $R_\oplus(L_\oplus(\textbf{Unitary}))$ we recover the dagger by Prop. 9 in [1]. This composition is similar to the construction we did to facilitate ancilli manipulation before. It is the *additive biaffine completion* of **Unitary**, the category $LR_\oplus(\textbf{Unitary})$ whose

- objects are same as **Unitary**;
- morphisms are triple $[H, f, G]$ of two objects H, G and a morphism $f : A \oplus H \to B \oplus G$ of **Unitary** quotiented by $\sim_{LR_\oplus}$;
- identities $A \to A$ are triples $[O, \mathrm{id}_{A \oplus O}, O]$;
- composition of $f : A \oplus H \to B \oplus G$ and $g : B \oplus H' \to C \oplus G'$ is given by

$$A \oplus (H \oplus H') \xrightarrow{\alpha_\oplus^{-1}} (A \oplus H) \oplus H' \xrightarrow{f \oplus \mathrm{id}} (B \oplus G) \oplus H' \xrightarrow{\cong} (B \oplus H') \oplus G \xrightarrow{g \oplus \mathrm{id}} (C \oplus G') \oplus G \xrightarrow{\alpha_\oplus} C \oplus (G' \oplus G).$$

The relation $\sim_{LR_\oplus}$ used to quotient is the least equivalence relation containing the three relations $\sim_{\mathrm{id}_\oplus}$, $\sim_{L_\oplus}$, and $\sim_{R_\oplus}$ defined as follows, for all $f : A \oplus H \to B \oplus G$:

- $f \sim_{L_\oplus} (\mathrm{id} \oplus m) \circ f$ for all $m : G \to G'$;

- $f \sim_{R\oplus} f \circ (\mathrm{id} \oplus n)$ for all $n : H' \to H$;
- $f \sim_{\mathrm{id}\oplus} \alpha_{\oplus} \circ (f \oplus \mathrm{id}_X) \circ \alpha_{\oplus}^{-1}$ for all identities id_X.

2.2. **Multiplicative Affine Completion of Unitary.** We can form the multiplicative affine completion of **Unitary** as $L_{\otimes}$(**Unitary**) same as $L_{\oplus}$(**Unitary**). Here, morphisms of form $f : A \to B$ are equivalence classes of morphisms $A \to B \otimes G$ in **Unitary** with identities and composition defined as before. This construction models *discarding* by allowing any state to be hidden partially or totally. $L_{\otimes}$ captures Stinespring dilation and according to [9], $L_{\otimes}$(**Isometry**) is monoidally equivalent to category $\mathbf{FHilb}_{\mathrm{CPTP}}$ of finite dimensional Hilbert spaces and completely positive trace-preserving maps (quantum channels). $L_{\otimes}$(**Unitary**) is a monoidal category such that:

- objects are same as that of **Unitary**;
- morphisms $A \to B$ are equivalence classes of morphisms $A \to B \otimes G$ in **Unitary** under $\sim_{L_{\otimes}}$;
- composition of two morphisms $f : A \to B$ and $g : B \to C$ in $L_{\otimes}$(**Unitray**) corresponds to composition of $f' : A \to B \otimes G$ and $g' : B \to C \otimes G'$ as $A \to C \otimes (G \otimes G')$;
- identities are inverse right unitors $\rho_{\otimes}^{-1}$;
- it is monoidal w.r.t. $\otimes$ such that tensor unit & product of objects/morphisms is same in **Unitary**.

References

[1] Pablo Andrés-Martínez, Chris Heunen, and Robin Kaarsgaard. Universal Properties of Partial Quantum Maps. *Electronic Proceedings in Theoretical Computer Science*, 394:192–207, November 2023.

[2] Jacques Carette, Chris Heunen, Robin Kaarsgaard, and Amr Sabry. The Quantum Effect: A Recipe for QuantumPi. (arXiv:2302.01885), May 2023.

[3] Jacques Carette, Chris Heunen, Robin Kaarsgaard, and Amr Sabry. With a Few Square Roots, Quantum Computing Is as Easy as Pi. *Proceedings of the ACM on Programming Languages*, 8(POPL):546–574, January 2024.

[4] Bob Coecke, John Selby, and Sean Tull. Two Roads to Classicality. *Electronic Proceedings in Theoretical Computer Science*, 266:104–118, February 2018.

[5] Pedro M. Q. Cruz and Bruno Murta. Shallow unitary decompositions of quantum Fredkin and Toffoli gates for connectivity-aware equivalent circuit averaging. *APL Quantum*, 1(1):016105, March 2024.

[6] Francis Borceux Dominique Dejean. Cauchy completion in category theory.

[7] Ross Duncan and Maxime Lucas. Verifying the Steane code with Quantomatic. *Electronic Proceedings in Theoretical Computer Science*, 171:33–49, December 2014.

[8] Chris Heunen and Robin Kaarsgaard. Quantum information effects. *Proceedings of the ACM on Programming Languages*, 6(POPL):1–27, January 2022.

[9] Mathieu Huot and Sam Staton. Universal Properties in Quantum Theory. *Electronic Proceedings in Theoretical Computer Science*, 287:213–223, January 2019.

[10] Miguel L. Laplaza. Coherence for distributivity. In G. M. Kelly, M. Laplaza, G. Lewis, and Saunders Mac Lane, editors, *Coherence in Categories*, pages 29–65, Berlin, Heidelberg, 1972. Springer.

[11] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, August 2004.

[12] Peter Selinger. Dagger Compact Closed Categories and Completely Positive Maps. *Electronic Notes in Theoretical Computer Science*, 170:139–163, March 2007.

[13] Schröder De Witt. The ZX-calculus is incomplete for stablizer quantum mechanics. December 2014.