The category TOF

Cockett, Robin Comfort, Cole

{robin,crcomfor}@ucalgary.ca

Department of Computer Science
University of Calgary
Alberta, Canada

We provide a complete set of identities for the symmetric monoidal category, TOF, generated by the Toffoli gate and computational ancillary bits. We do so by demonstrating that the functor which evaluates circuits on total points, is an equivalence into the full subcategory of sets and partial isomorphisms with objects finite powers of the two element set. The structure of the proof builds – and follows the proof of Cockett et al. – which provided a full set of identities for the cnot gate with computational ancillary bits. Thus, first it is shown that TOF is a discrete inverse category in which all of the identities for the cnot gate hold; and then a normal form for the restriction idempotents is constructed which corresponds precisely to subobjects of the total points of TOF. This is then used to show that TOF is equivalent to FPinj_2, the full subcategory of sets and partial isomorphisms in which objects have cardinality 2^n for some $n \in \mathbb{N}$.

1 Introduction

The Toffoli gate is a cornerstone for reversible computing: alongside the Fredkin gate, it was the first gate which was proven to be universal for classical reversible computing [6]. That is, if the values of certain wires are fixed and unchanged by computation (called "auxiliary bits") and the value of others ignored after computation (called "garbage bits"), then every reversible boolean function can be simulated using either Fredkin or Toffoli gates. The universality of the Fredkin gate relies fundamentally on the use of garbage bits. The Toffoli gate, however, is universal for classical reversible circuits even when *only* auxiliary bits are allowed. This is notable, as even the Fredkin and cnot gates combined are not universal in this sense [1, Thm. 3]. Moreover, the Toffoli gate is also used frequently in quantum computation (especially in quantum error correction [15, 9]); and has even been physically realized [13, 14].

Notably, [11] provided an infinite, complete set of identities for functions of the form $|x_1,\cdots,x_n,y\rangle \mapsto |x_1,\cdots,x_n,y+f(x_1,\cdots,x_n)\rangle$ generated by Toffoli gates with finitely many control wires, along with finitely many qubits in the state $|0\rangle$.

Auxiliary bits are a rather peculiar notion and are unnatural in the context of symmetric monoidal categories [1] ; instead, we shall take a more general and richer approach by simply allowing the inputs and outputs of wires to be fixed by components which we call "ancillary bits". Ancillary bits, in this sense, are modelled by qubit initialization and termination in [10], where the state of a circuit can degenerate to an undefined state – in finite dimensional Hilbert spaces, FHilb, this corresponds to when maps compose to a zero-matrix.

In [5], Cockett et al. provided a complete set of identities for the fragment of quantum computing generated by the controlled-not gate with ancillary bits. The paper was inspired by Lafont's work [12],

[1] An auxillary bit can be simulated by fixing the input and output of a wire using an input and output ancillary bit. However, usually, there is the added assumption that fixing bits in this manner will not cause the resulting function to degenerate or become partially defined. Thus, auxillary bits, as commonly formulated, do not provide a compositional notion.

Submitted to:
QPL 2018

but used the notion of a discrete inverse category developed in [7]. Inverse categories have now been used extensively to model the semantics of reversible computation [2, 8]. The current paper builds on [5] and provides a finite, complete set of identities for the fragment of quantum computing generated by the Toffoli gate with ancillary bits [2]. We call the symmetric monoidal category generated by the Toffoli gate and ancillary bits with these identities, TOF.

In addition to providing a complete set of identities for these circuits, we also prove a concrete equivalence into the subcategory of sets and partial isomorphisms where the objects are finite powers of the 2 element set [3]. The key step of this proof is to prove that the functor $\tilde{H}_0$, which takes an object to its (total) points, is faithful: this, in turn, relies on providing a normal form for the restriction idempotents of TOF.

Overview of the proof

We first present the symmetric monoidal category called TOF which is generated by the Toffoli gate and ancillary bits along with 17 identities. The paper culminates with a proof that TOF is isomorphic to the category, FPinj_2, of partial isomorphisms between finite powers of the two element set. The proof follows the form of the proof in [5] for the category CNOT, built from the computational ancillary bits and the cnot gate. We start by observing, Lemma 4.1, that all of the identities of the category CNOT hold in TOF. The first crucial step is to prove that some needed identities of Iwama [11] hold in this setting. The next crucial next step is to prove that TOF is a discrete inverse category. Discrete inverse categories have inverse products and, for TOF, these are essentially inherited from CNOT. Furthermore, in TOF, just as for CNOT, partial inverses are given by horizontally flipping circuits: this gives a dagger functor $(\_)^\circ : \mathsf{TOF}^{\mathsf{op}} \to \mathsf{TOF}$. In Section 8, we construct a discrete inverse functor $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ which "evaluates" maps on the points of TOF. In Section 9, we construct a normal form for the restriction idempotents of TOF using "polyforms": this is the crux of the paper. In Section 10 we prove that the functor $\tilde{H}_0$ is full faithful, borrowing results from [5] – wherein it is shown that $\tilde{H}_0$ being full and faithful on restriction idempotents implies $\tilde{H}_0$ is full and faithful in general.

2 Restriction and inverse categories

In this section, we recall the basic theory and terminology of restriction and inverse categories which will be used later.

Definition 2.1. [4, Def. 2.1.1] A **restriction structure** on a category $\mathbb{X}$ is an assignment $\overline{f} : A \to A$ for each map $f : A \to B$ in $\mathbb{X}$ satisfying the following four axioms:

[R.1] $\overline{f}f = f$ **[R.2]** $\overline{f}\,\overline{g} = \overline{g}\,\overline{f}$ **[R.3]** $\overline{\overline{g}f} = \overline{f}\,\overline{g}$ **[R.4]** $f\overline{g} = \overline{fg}f$

A **restriction category** is a category equipped with a restriction structure. A **restriction functor** is a functor which preserves the given restriction structure. An endomorphism $e : A \to A$ is called a **restriction idempotent** if $e = \overline{e}$. In particular, each $\overline{f}$ has $\overline{\overline{f}} = \overline{f}$ and is an idempotent as $\overline{f}\,\overline{f} = \overline{\overline{f}f} = \overline{f}$.

In a restriction category, a **total map** is a map f such that $\overline{f} = 1$. The total maps of a restriction category $\mathbb{X}$ form a subcategory $\mathsf{Total}(\mathbb{X})$ of $\mathbb{X}$.

[2]Although the larger fragment of quantum computing generated by the Toffoli gate, Hadamard gate and computational ancillary bits has recently been classified [16].

[3]This result implies, in particular, that TOF embeds faithfully into the categories of matrices [3], $\mathsf{Mat}(\mathbb{C})$, as FPinj_2 embeds into the category of matrices by taking partial isomorphisms to their adjacency matrices.

A basic example of a restriction category is the category of sets and partial functions, Par: the restriction of a partial function is the partial identity on the domain of definition.

Definition 2.2. [4, Sec. 2.3]. A map f is a **partial isomorphism** when there exists another map g, called the **partial inverse** of f, such that $\overline{f} = fg$ and $\overline{g} = gf$. A restriction category $\mathbb{X}$ is an **inverse category** when all its maps are partial isomorphisms.

Partial isomorphisms generalize the notion of isomorphisms to restriction categories; thus, the composition of partial isomorphisms is a partial isomorphism and partial inverses are unique. Furthermore, every restriction category $\mathbb{X}$ has a subcategory of partial isomorphisms $\mathsf{ParIso}(\mathbb{X})$ which is an inverse category. Denote the category $\mathsf{ParIso}(\mathsf{Set})$ by Pinj.

There is an important alternate characterization of an inverse category:

Theorem 2.3. [4, Thm. 2.20] A category $\mathbb{X}$ is an inverse category if and only if there exists a functor $(\_)^\circ : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$ which is the identity on objects, satisfying the following three axioms:

[INV.1] $(f^\circ)^\circ = f$ **[INV.2]** $ff^\circ f = f$ **[INV.3]** $ff^\circ gg^\circ = gg^\circ ff^\circ$

Inverse categories have restriction structure given by $\overline{c} := cc^\circ$. Every idempotent in an inverse category is necessarily a restriction idempotent.

Inverse categories can have a product-like structure:

Definition 2.4. [7, Def. 4.3.1]

Take a symmetric monoidal inverse category $\mathbb{X}$ with tensor $\_ \otimes \_ : \mathbb{X} \times \mathbb{X} \to \mathbb{X}$, symmetry c and associator a. Suppose moreover that the tensor preserves $(\_)^\circ$. We say $\mathbb{X}$ has **inverse products** if there exists a total natural diagonal transformation Δ which satisfies the following properties:

[DINV.1] Δ is cocommutative:

$$\begin{tikzcd} A \arrow[r, "\Delta_A"] \arrow[dr, "\Delta_A"'] & A \otimes A \arrow[d, "c_{A,A}"] \\ & A \otimes A \end{tikzcd}$$

[DINV.2] Δ is coassociative:

$$\begin{tikzcd} A \arrow[rr, "\Delta_A"] \arrow[d, "\Delta_A"'] & & A \otimes A \arrow[d, "1_A \otimes \Delta_A"] \\ A \otimes A \arrow[dr, "\Delta_A \otimes 1_A"'] & & A \otimes (A \otimes A) \\ & (A \otimes A) \otimes A \arrow[ur, "a_{A,A,A}"'] & \end{tikzcd}$$

[DINV.3] (Δ, Δ°) is a semi-Frobenius object:

$$\begin{tikzcd} A \otimes A \arrow[rr, "(\Delta_A \otimes 1_A) a_{A,A,A}"] \arrow[dr, "\Delta_A^\circ"] \arrow[dd, "(1_A \otimes \Delta_A) a^\circ_{A,A,A}"'] & & A \otimes (A \otimes A) \arrow[dd, "1_A \otimes \Delta_A^\circ"] \\ & A \arrow[dr, "\Delta_A"] & \\ (A \otimes A) \otimes A \arrow[rr, "\Delta_A^\circ \otimes 1_A"] & & A \otimes A \end{tikzcd}$$

[DINV.4] Δ is uniform-copying:

$$\begin{tikzcd} A \otimes B \arrow[r, "\Delta_A \otimes \Delta_B"] \arrow[dr, "\Delta_{A \otimes B}"'] & (A \otimes A) \otimes (B \otimes B) \arrow[d, "{a_{A,A,B\otimes B}(1_A \otimes a^\circ_{A,B,B})(1_A \otimes (c_{A,B} \otimes 1_B))((1_A \otimes a_{B,A,B}) a^\circ_{A,B,A\otimes B})}"] \\ & (A \otimes B) \otimes (A \otimes B) \end{tikzcd}$$

A **discrete inverse category** is a category with inverse products. Note that Δ is required to be total, so that $\Delta\Delta^\circ = 1$: making the semi-Frobenius structure separable (or special).

3 The category CNOT

In [5] the category CNOT was presented as a symmetric monoidal category with objects natural numbers generated by the 1 ancillary bits $|1\rangle \equiv$, and $\langle 1| \equiv$ [4], and the controlled not gate cnot $\equiv$, where these gates satisfy the identities in Figure 1:

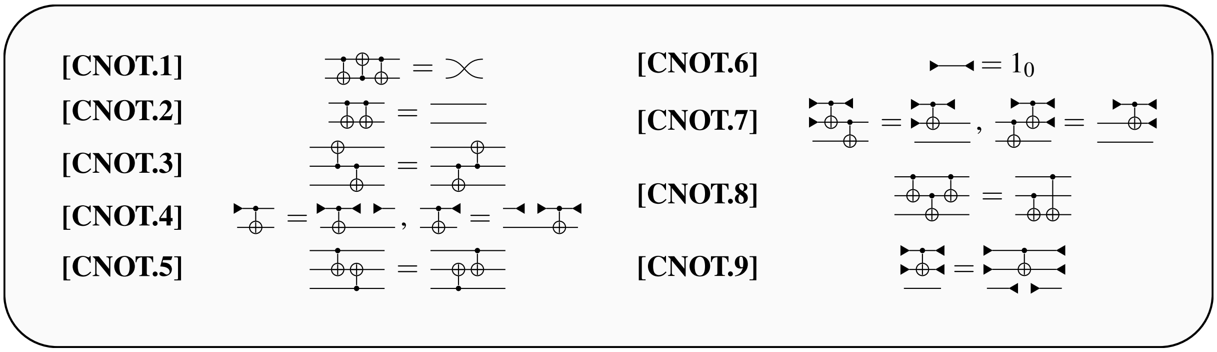
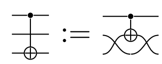


Figure 1: The identities of CNOT

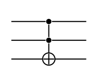
Notice that there are "gaps" in some of the cnot gates, and others are flipped. This is just shorthand to suppress burdensome symmetry maps. There is an obvious interpretation of this notation, for example:



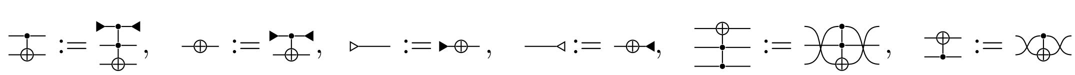
It was shown that these identities were complete; and moreover, it was shown that CNOT is equivalent to the category of affine partial isomorphisms between finite $\mathbb{Z}_2$-vector spaces. We shall use these observations to obtain a similar equivalence for the category, TOF, generated by the Toffoli gate and 1 ancillary bits.

4 The category TOF

Define the category TOF to be the symmetric monoidal category, with objects the natural numbers, generated by the 1 ancillary bits $|1\rangle$ and $\langle 1|$ (depicted graphically as in CNOT) as well as the Toffoli gate:

tof :=


The Toffoli gate and the 1-ancillary bits allow the cnot gate, not gate, $|0\rangle$ gate, $\langle 0|$ gate, flipped tof gate and flipped cnot gate to be succinctly defined:



We also allow for "gaps" in tof and cnot gates, as in CNOT.

[4] Here, the bra-ket notation is slightly deceptive because the diagrammatic order of composition makes the inner product look like the outer product, and vice versa.

These gates must satisfy the identities given in Figure 2:

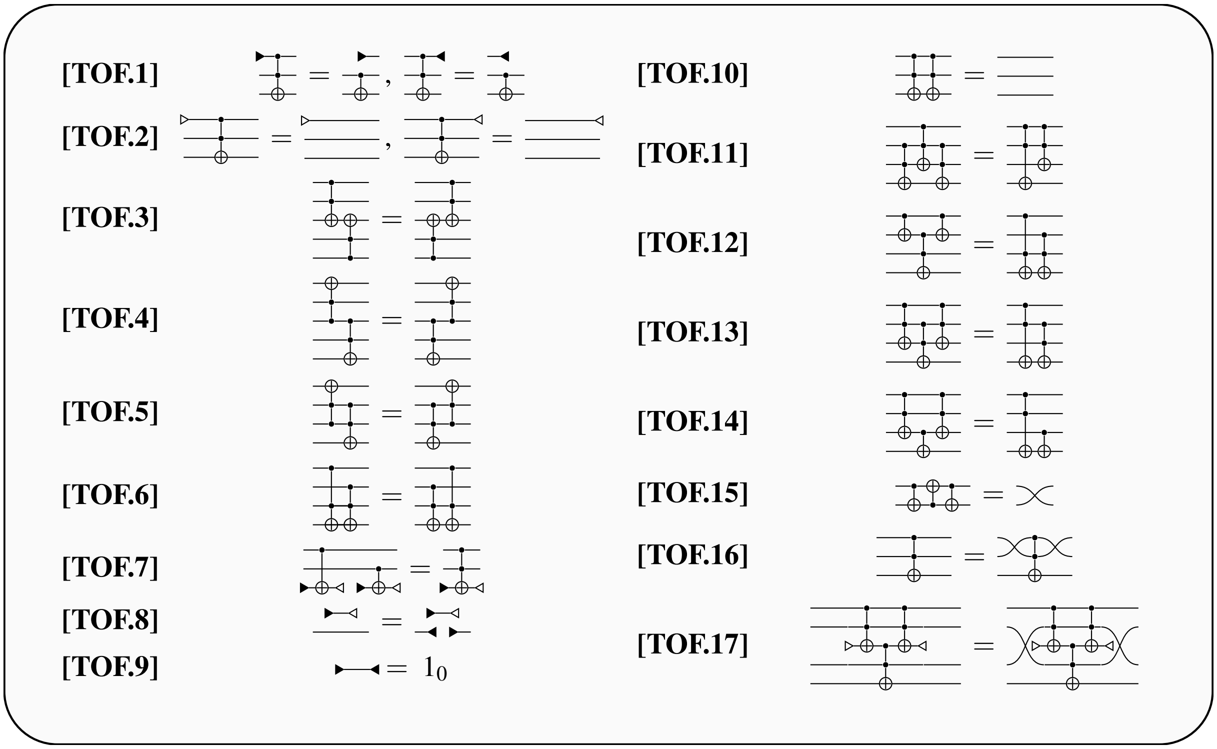
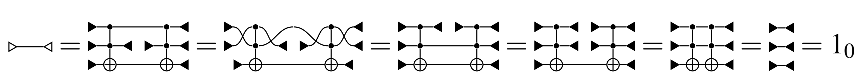


Figure 2: The identities of TOF

Axioms **[TOF.1]**-**[TOF.6]**, **[TOF.9]**-**[TOF.10]** are relatively intuitive. **[TOF.8]** corresponds to tensoring a matrix with the 1×1 zero matrix: this is useful for establishing the restriction structure of TOF. **[TOF.7]** is used for establishing a normal form for the restriction idempotents. Any of Axioms **[TOF.11]**-**[TOF.14]** combined with **[TOF.10]** are used to push $\mathsf{cnot}/\mathsf{tof}$ gates past each other thereby generating another trailing $\mathsf{cnot}/\mathsf{tof}$ gate: this will be discussed in more detail in Lemma 5.5 *(v)* . **[TOF.15]** is inherited from CNOT and is used to establish the inverse products of TOF. **[TOF.16]** expresses the commutativity of multiplication for the Toffoli gate. **[TOF.17]** is similar to **[TOF.16]**, except for the 3-bit-controlled-not gate.

As an exercise, we first show that $|0\rangle\langle 0| = 1_0$ (just as $|1\rangle\langle 1| = 1_0$ in **[TOF.9]**):



Since we build on the work done in [5], we start by establishing that there is a canonical functor from the category CNOT into TOF. The proof is contained in Appendix A.

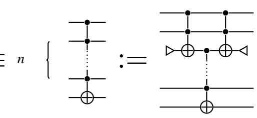
Lemma 4.1. The canonical interpretation of CNOT in TOF is functorial.

5 Controlled not gates and the Iwama identities

In reversible and quantum computing it is usual to regard the Toffoli gate and cnot as the not gate "controlled", respectively, by one and two control wires. In TOF one can define cnot_n the not gate controlled by n wires for any $n \in \mathbb{N}$:

Definition 5.1. For every $n \in \mathbb{N}$, inductively define the controlled not gate, $\mathsf{cnot}_n : n+1 \to n+1$ inductively by:

- For the base cases, let $\mathsf{cnot}_0 := \mathsf{not}$, $\mathsf{cnot}_1 := \mathsf{cnot}$ and $\mathsf{cnot}_2 := \mathsf{tof}$.
- For all $n \in \mathbb{N}$ such that $n \geq 2$:

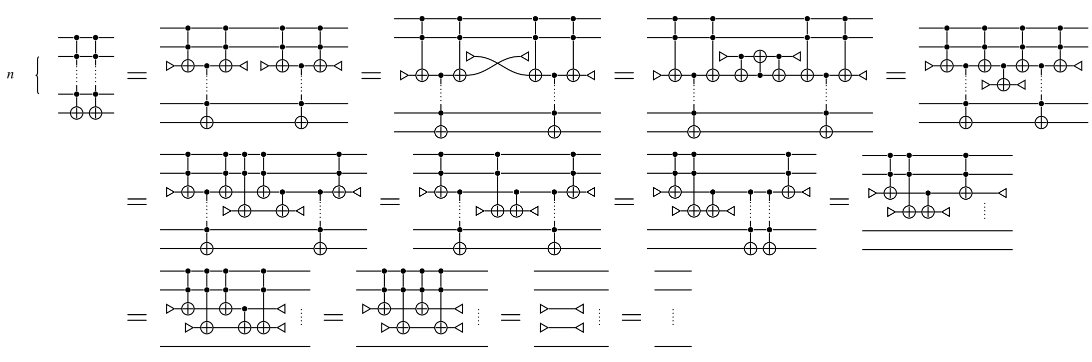
$\mathsf{cnot}_{n+1} \equiv$ 

The first n wires of cnot_n are the **control wires** while the last wire is the **target wire**. As for the cnot and tof gates, allow for cnot_n gates to haves "gaps" in between the control wires (and the target wire).

Notice that cnot_n gates are self inverse:

Lemma 5.2. Every cnot_n gate is self-inverse.

Proof. The base cases are trivial. For the inductive step, suppose that cnot_n gates are self-inverse, then:

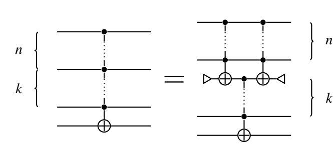


□

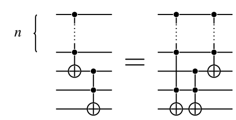
Next we show how we can "unzip" cnot_n gates; and simultaneously, we generalize Lemma B.1 to show how a cnot_n gate can be "pushed" past a Toffoli gate. This is a crucial observation in establishing the Iwama identities. The proof is contained in Appendix B.

Proposition 5.3. Given some $n \geq 1$ and $k \geq 1$:

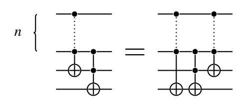
(i) cnot_{n+k} gates can be zipped and unzipped:



(ii) cnot_n gates can be pushed past Toffoli gates in the following sense:

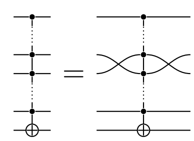


(iii) And likewise:



We can use the ability to zip and unzip controlled not gates to show that we can transpose control wires:

Corollary 5.4.



Proof. The claim follows vacuously for $n < 2$. The base case when $n = 2$ follows immediately from **[TOF.16]**. Suppose that the claim holds for some cnot_n. Consider a cnot_{n+1} gate and unzip this gate one level down. We can transpose the top two control wires by the base case and we can transpose the bottom $n-1$ control wires by the inductive hypothesis. Finally, to transpose the second and third wire from the top, either unzip the cnot_{n+1} gate down by one more step. If this cannot be done – because there is nothing more to unzip – it means one can directly apply **[TOF.17]**. □

Since transpositions generate the symmetric group, the control wires of a cnot_n gate can, therefore, be freely permuted.

We use the notation $\oplus_x^X$ to denote a $\mathsf{cnot}_{|X|}$ gate operating on the control wires in the set X and targeting the wire x. Similarly let $\rhd_x$ and $\lhd_x$ be, respectively, the $|0\rangle$ and $\langle 0|$ gates on the wire x.

The following identities are due to Iwama et al. [11]. They show how to push generalized control not gates past each other in certain key situations. The proof is contained in Appendix C.

Lemma 5.5 (Iwama's Identities)**.**

(i) $\oplus_x^X \oplus_x^X = 1$

(ii) When $x \in X$ then $\rhd_x \oplus_y^X = \rhd_x$

(iii) When the target wire are the same $\oplus_x^X \oplus_x^Y = \oplus_x^Y \oplus_x^X$

(iv) When $x \notin Y$ and $y \notin X$ then $\oplus_x^X \oplus_y^Y = \oplus_y^Y \oplus_x^X$

(v) $\oplus_x^X \oplus_y^{\{x\} \sqcup Y} = \oplus_y^{X \cup Y} \oplus_y^{\{x\} \sqcup Y} \oplus_x^X$

(vi) $\rhd_z \oplus_z^{\{x\}} \oplus_y^{\{x\} \sqcup X} = \rhd_z \oplus_z^{\{x\}} \oplus_y^{\{z\} \sqcup X}$

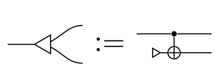
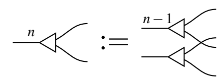
6 TOF is a discrete inverse category

Next we prove that TOF is a discrete inverse category.

Define $(\_)^\circ : \mathsf{TOF}^{\mathsf{op}} \to \mathsf{TOF}$ to be the contravariant functor which flips circuits horizontally, mapping $|1\rangle \mapsto \langle 1|$, $\langle 1| \mapsto |1\rangle$ and $\mathsf{tof} \mapsto \mathsf{tof}$. Clearly $(\_)^\circ$ is an involution (and thus, a dagger functor) as all of the axioms are horizontally symmetric and $(f^\circ)^\circ = f$.

The diagonal map in TOF is the image of the diagonal map, $\Delta_n : n \to n \otimes n$, in CNOT under the canonical functor $\mathsf{CNOT} \to \mathsf{TOF}$:

Definition 6.1. Define a family of maps $\Delta := \{\Delta_n\}_{n\in\mathbb{N}}$ with the cnot gate and 1-ancillary wires inductively, as in [5], such that $\Delta_0 = 1_0$,

$\Delta_1 :=$  and for all $n > 1$: $\Delta_n :=$ 

This yields the following result; the proof is contained in Appendix D:

Proposition 6.2. TOF is a discrete inverse category with this structure.

7 The points of TOF

The (total) points of TOF are iterated tensors of the input ancillary bits ($|0\rangle$ and $|1\rangle$) and can be denoted using the "ket" notation. We start by observing that the Toffoli gate in TOF behaves as expected on these points; the proof is contained in Appendix E:

Lemma 7.1. $\mathsf{tof}(|x_1,x_2,x_3\rangle) = |x_1,x_2,x_1\cdot x_2 + x_3\rangle$

The points above which are expressed in bra notation are clearly total. However, not all maps with domain 0 are total: in particular, as in CNOT, the maps $\Omega_{0,m}$ for $m \in \mathbb{N}$ are not total:

Definition 7.2. Define $\Omega := |1\rangle\langle 0|$, and $\Omega_{n,m} := \langle 1|^{\otimes^n}\Omega|1\rangle^{\otimes^m}$.

When any map is tensored with such a map it becomes one of them:

Lemma 7.3. For all circuits $f \in \mathsf{TOF}(n,m)$, $f \otimes \Omega = \Omega_{n,m}$.

Proof. By the functionality of the interpretation of CNOT into TOF and [5, Lemma A.2] note that Ω is idempotent. Therefore, use **[TOF.8]** to cut all of the wires around all Toffoli gates. Notice that when the wires round a Toffoli gate is cut this results in the map:

$$|111\rangle\mathsf{tof}\langle 111| = |11\rangle\mathsf{cnot}\langle 11| = |1\rangle\mathsf{not}\langle 1| = |0\rangle\langle 1| =: \Omega$$

When all wires of a circuit are cut it will therefore take the form:

$$\langle 1|^{\otimes^n}(\Omega)^{\otimes^k}(|1\rangle\langle 1|)^{\otimes^\ell}|1\rangle^{\otimes^m} = \langle 1|^{\otimes^n}(\Omega)^{\otimes^k}(1_0)^{\otimes^\ell}|1\rangle^{\otimes^m} = \langle 1|^{\otimes^n}\Omega|1\rangle^{\otimes^m} =: \Omega_{n,m}$$

□

In fact, there are only two sorts of points, those that are expressible as kets—and maps of the form $\Omega_{0,n}$ for some $n \in \mathbb{N}$:

Lemma 7.4. For all $n \in \mathbb{N}$ and $f \in \mathsf{TOF}(0,n)$ implies $f = \Omega_{0,n}$ or $f = |b_1,\cdots,b_n\rangle$ for some $b_1,\cdots,b_n \in \mathbb{Z}_2$.

Proof. Given any circuit $f \in \mathsf{TOF}(0,n)$, pull all of the $|1\rangle$ gates to the left of the circuit and all of the $\langle 1|$ gates to the right. In the middle, there will only be tof gates; thus, apply the $|1\rangle$ gates to the tof gates using Lemma 7.1. This will result in a series of $|1\rangle$ and $|0\rangle$ gates on the left. Repeatedly apply these $|1\rangle$ and $|0\rangle$ gates to the tof gates using Lemma 7.1 until there are only a series of $|1\rangle$ and $|0\rangle$ gates on the left and a series of $\langle 1|$ gates on the right, and nothing in the middle. If a $|1\rangle$ and $\langle 1|$ gate meet, they compose to form the identity and disappear. If this process can eliminate all of the $\langle 1|$ gates, then we are done. Otherwise, if $|0\rangle$ and $\langle 1|$ gate meet, they compose to form Ω; therefore, by Lemma 7.3, $f = \Omega_{0,n}$. □

8 Partial injective functions and TOF

For any restriction category $\mathbb{X}$ and any object $X \in \mathbb{X}$, we may define a restriction-preserving hom-functor $h_X : \mathbb{X} \to \mathsf{Par}$ by:

On Objects: $h_X(Y) := \{f \in \mathbb{X}(X,Y) | \overline{f} = 1_X\}$

On Maps: For each map $f : Y \to Z$, for all $g \in h_X(Y)$:

$$(h_X(f))(g) := \begin{cases} gf & \text{if } \overline{gf} = 1_X \\ \uparrow & \text{otherwise} \end{cases}$$

As TOF is a restriction category, we may consider the functor $h_0 : \mathsf{TOF} \to \mathsf{Par}$ which evaluates circuits on the total points of TOF. As TOF is an inverse category and this functor preserves restriction, we can lift $h_0 : \mathsf{TOF} \to \mathsf{Par}$ to a restriction-preserving functor $H_0 : \mathsf{TOF} \to \mathsf{Pinj}$. Clearly the nature of the total points of TOF ensures that the discrete inverse structure is preserved by H_0:

Lemma 8.1. $H_0 : \mathsf{TOF} \to \mathsf{Pinj}$ preserves discrete products.

Proof. $H_0(n) = \{|b_1 ... b_n\rangle | b_i \in \{0,1\}\}$ so that $H_0(n+m) \simeq H_0(n) \times H_0(m)$ and $H_0(\Delta) = \Delta$. □

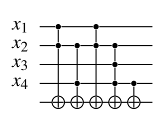
Define FPinj_2 to be the full subcategory of Pinj (sets and partial isomorphisms) with objects finite powers of the two element set. By Lemma 7.4, the object $n \in \mathsf{TOF}$ under H_0 corresponds to the set $\{|0\rangle, |1\rangle\}^n$ in FPinj_2; therefore, by restricting the co-domain of H_0 we obtain a bijective on objects functor $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$. We will prove that this functor is an equivalence of categories.

9 A normal form for the idempotents of TOF

As in [5], our objective is to reduce the fullness and faithfulness of $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ to its fullness and faithfulness on restriction idempotents. cnot_n gates will be used to define a class of circuits which will allow a normal form for the idempotents of TOF to be established. It is also worth noting that the following class of circuits corresponds to the canonical form of [11, Def. 4]:

Definition 9.1. A circuit $f : n \to n$ is said to be in **polynomial form** when it is the composition of circuits $f = c_1 \cdots c_k$ where each c_i is a cnot_j gate with control any of the first $n-1$ wires and target the last wire.

For example, the following circuit corresponding to the polynomial $x_1x_2 + x_2x_4 + x_1x_2 + x_1x_2 + x_2x_3x_4 + x_4$ is in polynomial form:

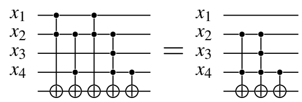


Clearly all polynomials (in normal form) can be represented by a circuit in polynomial form, where each monomial corresponds to a cnot_n gate. Moreover, this correspondence is bijective, as cnot_n gates targeting the same wire obviously commute, and cnot_n gates are self-inverse by Lemma 5.2.

For example, the following identity holds in $\mathbb{Z}_2[x_1, x_2, x_3, x_4]$

$$x_1x_2 + x_2x_4 + x_1x_2 + x_2x_3x_4 + x_4 = x_2x_4 + x_2x_3x_4 + x_4$$

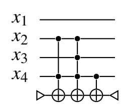
and this corresponds to the following identity in TOF:

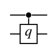


Since the restriction idempotents in FPinj are determined by boolean equations or, equivalently, by the zeros of multivariate polynomials over $\mathbb{Z}_2$, we use polynomial form circuits to provide a normal form for the restriction idempotents of TOF. By restricting the value of the bottom wire to be 0, the evaluation of this circuit on total points is defined if and only if the corresponding tuple of bits is in the kernel of the function corresponding to polynomial evaluation:

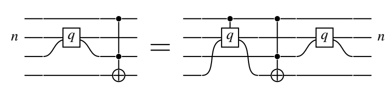
Definition 9.2. A circuit $e : n \to n$ in TOF is a **polyform** if $e = (1_n \otimes |0\rangle)q(1_n \otimes \langle 0|)$ for some $q : n+1 \to n+1$ in polynomial form.

For example the following circuit corresponding to the equation $x_2x_4 + x_2x_3x_4 + x_4 = 0$ is a polyform:



Given a polynomial form circuit q, let the circuit  denote the circuit where every cnot_n gate of q is additionally controlled by wire with the black dot.

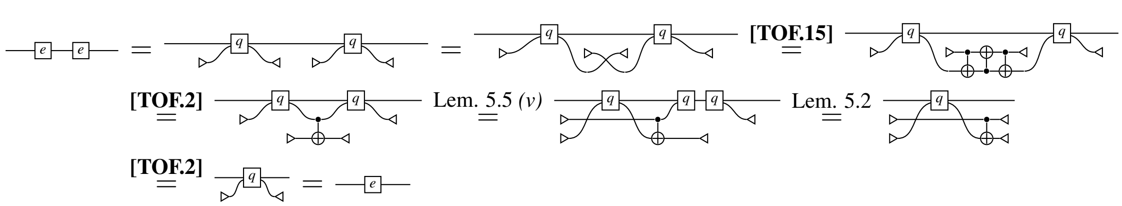
In fact given a polynomial form circuit $q : n+1 \to n+1$, by the repeated application of Lemma 5.5 *(v)* for each constituent cnot_n gate, it is useful to observe:



Our aim is now to show that the idempotents of TOF are always equivalent to a polyform so that these circuits provide a normal form for the idempotents. Because some of the steps are subtle, we annotate certain equalities with the corresponding identities used.

Lemma 9.3. Polyforms are idempotents (and therefore restriction idempotents).

Proof. Consider some map $e := (1_n \otimes |0\rangle)q(1_n \otimes \langle 0|)$ a polyform, as above, then:



$\square$

We prove that the converse also holds using 3 lemmas:

Proposition 9.4. All idempotents in TOF are equivalent to a circuit which is a polyform.

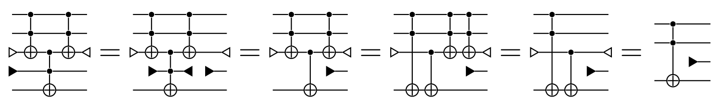
Given a polyform, f, by structural induction, it suffices to show that sandwiching f with a generating gate, g, to obtain $(1\otimes g\otimes 1)f(1\otimes g^\circ\otimes 1)$, always results in a circuit which has a polyform. There are 3 cases, one for each generating circuit:

Lemma 9.5. If $f : n \to n$ is a polyform then sandwiching f by a tof gate results in a circuit with a polyform.

Proof. By Lemma 5.5 *(v)*, push g through f until it meets the other $g^\circ = g$ and then annihilate both generalized controlled not gates by Lemma 5.2. This circuit is still a polyform. □

Lemma 9.6. If $f : n \to n$ is a polyform then sandwiching f by a $|1\rangle$ gate results in a circuit equivalent to a polyform.

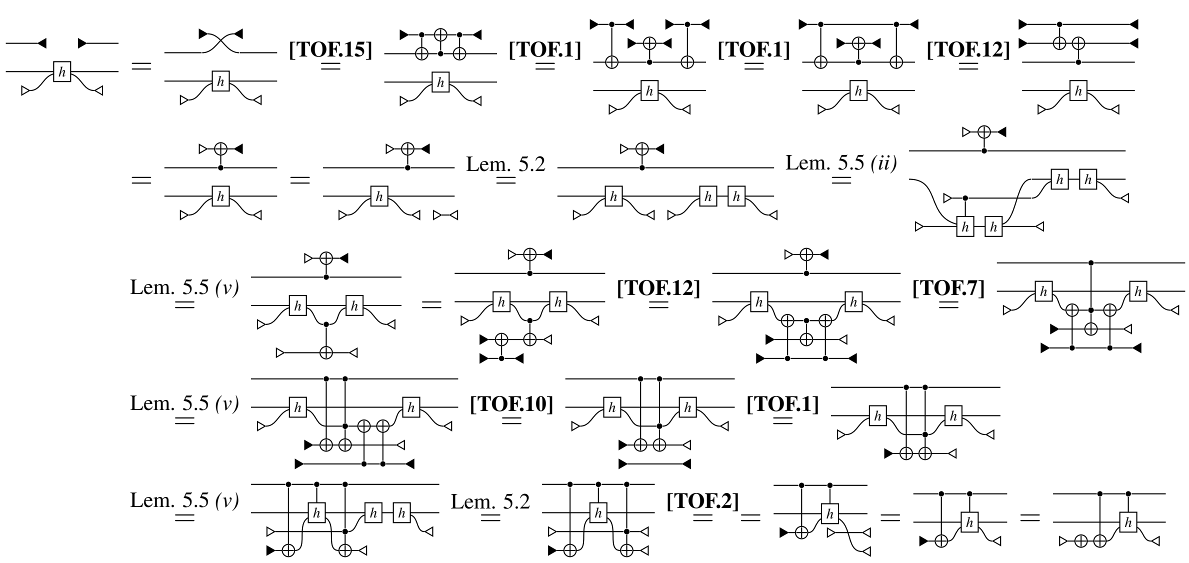
Proof. It suffices to observe for the inductive step that:



□

Lemma 9.7. If $f : n \to n$ is a polyform then sandwiching f by a $|1\rangle$ and $\langle 1|$ gate results in a circuit with a polyform.

Proof. Suppose $f : n \to n$ is a polyform $(1_n \otimes |0\rangle \otimes 1_m)h(1_n \otimes \langle 0| \otimes 1_m)$, then:



□

We have now established with Lemma 9.3 and Proposition 9.4:

Proposition 9.8. Polyforms are a normal form for the idempotents in TOF.

This implies the desired result:

Corollary 9.9. $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ is full and faithful on restriction idempotents.

10 Full and faithfullness of $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$

We follow the approach of [5] to prove the fullness of $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$. First we show that we can "simulate" all the total maps in FPinj_2 with extra outputs:

Lemma 10.1. For every total map $f \in \mathsf{FPinj}_2(n,m)$, there is some $g \in \mathsf{TOF}$ such that $\tilde{H}_0(g) = \langle 1_{\mathbb{Z}_2^n}, f \rangle$.

Proof. Consider a total $f \in \mathsf{FPinj}_2(n,m)$. For any i such that $1 \leq i \leq m$, observe that $f\pi_i$ corresponds to a polynomial in $\mathbb{Z}[x_1, \cdots, x_n]$ and thus, there is a circuit $g_i : n+1 \to n+1$ in polynomial form such that $\tilde{H}_0(h_i) = \langle 1_{\mathbb{Z}_2^n}, f\pi_i \rangle$ where $h_i := (1_n \otimes |0\rangle)g_i$.

Now, inductively define the circuit P_i for all i such that $0 \leq i \leq m$, such that: $P_0 = 1_n$ and for every i such that $0 \leq i < m$, $P_{i+1} := h_{i+1}(P_i \otimes 1_1)$.

Then $\tilde{H}_0(P_m) = \langle 1_{\mathbb{Z}_2^n}, f\pi_1, \cdots, f\pi_m \rangle = \langle 1_n, f \rangle$. □

Then we recall a technical observation from [5]:

Lemma 10.2 ([5, Lemma C.21]). Let $F : \mathbb{X} \to \mathbb{Y}$ be an inverse product preserving functor between discrete inverse categories. Let f be a partial isomorphism in $\mathbb{Y}$. If $\langle \overline{f}, f \rangle := \Delta(\overline{f} \otimes f)$ and $\langle \overline{f^\circ}, f^\circ \rangle := \Delta(\overline{f^\circ} \otimes f^\circ)$ are in the image of F, then f and f° are also in the image of F.

This allows us to show:

Proposition 10.3. $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ is full.

Proof. Consider a map $f \in \mathsf{FPinj}_2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$ for arbitrary $n, m \in \mathbb{Z}$. By Lemma 10.2, if we can simulate $\langle \overline{f}, f \rangle$ and $\langle \overline{f^\circ}, f^\circ \rangle$, we can simulate f. However, partial maps of the form $\langle \overline{g}, g \rangle : X \to X \times Y$ are restrictions of a total map, unless Y is empty,. The case of Y being empty does not occur in FPinj_2 as the empty set is not an object. Thus, all such maps are restrictions of total maps. Therefore, by Lemma 10.1 there is some $h \in \mathsf{TOF}$ such that $\tilde{H}_0(h) \geq \langle 1, g \rangle$ for any g. However, by Proposition 9.9 $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ is full on restriction idempotents, so there is some $e = \overline{e}$ such that $H_0(e) = \overline{g}$ and so $H_0(eh) = \langle \overline{g}, g \rangle$ which completes the proof. □

The faithfulness of $\tilde{H}_0$ is reduced to its faithfulness on restriction idempotents. This uses another technical result from [5] which we recall:

Lemma 10.4 ([5, Lemma C.25]). A restriction functor $F : \mathbb{X} \to \mathbb{Y}$ between discrete inverse categories, which preserves inverse products, is faithful if and only if it is faithful on restriction idempotents.

As $\tilde{H}_0$ is faithful on idempotents and preserves inverse products, this gives:

Proposition 10.5. $\tilde{H}_0 : \mathsf{TOF} \to \mathsf{FPinj}_2$ is faithful.

By Propositions 10.3 and 10.5, we may conclude:

Theorem 10.6. TOF is discrete-inverse-equivalent to FPinj_2.

References

[1] Scott Aaronson, Daniel Grier & Luke Schaeffer (2017): *The Classification of Reversible Bit Operations*. In: *LIPIcs-Leibniz International Proceedings in Informatics*, 67, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[2] Holger Bock Axelsen & Robin Kaarsgaard (2016): *Join inverse categories as models of reversible recursion*. In: *International Conference on Foundations of Software Science and Computation Structures*, Springer, pp. 73–90.

[3] Michael Barr (1992): *Algebraically compact functors*. Journal of Pure and Applied Algebra 82(3), pp. 211–231.

[4] J Robin B Cockett & Stephen Lack (2002): *Restriction categories I: categories of partial maps*. Theoretical computer science 270(1-2), pp. 223–259.

[5] Robin Cockett, Cole Comfort & Priyaa Srinivasan (2018): *The Category CNOT*. Electronic Proceedings in Theoretical Computer Science 266, pp. 258–293, doi:10.4204/eptcs.266.18. Available at `https://doi.org/10.4204/eptcs.266.18`.

[6] Edward Fredkin & Tommaso Toffoli (2002): *Conservative logic*. In: Collision-based computing, Springer, pp. 47–81.

[7] Brett Giles (2014): *An investigation of some theoretical aspects of reversible computing*. Ph.D. thesis, University of Calgary.

[8] Robert Glück & Robin Kaarsgaard (2017): *A categorical foundation for structured reversible flowchart languages*. In: Proceedings of the 33rd Conference on the Mathematical Foundations of Programming Semantics (MFPS XXXIII).

[9] Daniel Gottesman (1997): *Stabilizer codes and quantum error correction*. arXiv preprint quant-ph/9705052.

[10] Alexander S Green, Peter LeFanu Lumsdaine, Neil J Ross, Peter Selinger & Benoît Valiron (2013): *An introduction to quantum programming in quipper*. In: International Conference on Reversible Computation, Springer, pp. 110–124.

[11] Kazuo Iwama, Yahiko Kambayashi & Shigeru Yamashita (2002): *Transformation rules for designing CNOT-based quantum circuits*. In: Proceedings of the 39th annual Design Automation Conference, ACM, pp. 419–424.

[12] Yves Lafont (2003): *Towards an algebraic theory of boolean circuits*. Journal of Pure and Applied Algebra 184(2-3), pp. 257–310.

[13] T Monz, K Kim, W Hänsel, M Riebe, AS Villar, P Schindler, M Chwalla, M Hennrich & R Blatt (2009): *Realization of the quantum Toffoli gate with trapped ions*. Physical review letters 102(4), p. 040501.

[14] Matthew D Reed, Leonardo DiCarlo, Simon E Nigg, Luyan Sun, Luigi Frunzio, Steven M Girvin & Robert J Schoelkopf (2012): *Realization of three-qubit quantum error correction with superconducting circuits*. Nature 482(7385), p. 382.

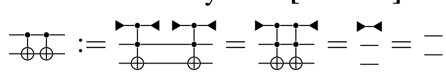
[15] Peter W Shor (1996): *Fault-tolerant quantum computation*. In: Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on, IEEE, pp. 56–65.

[16] Renaud Vilmart (2018): *A ZX-Calculus with Triangles for Toffoli-Hadamard, Clifford+ T, and Beyond*. arXiv preprint arXiv:1804.03084.

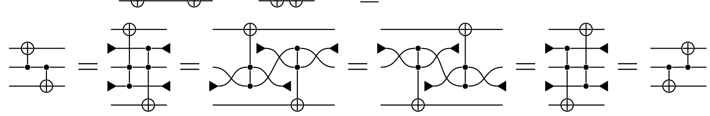
A Proof of Lemma 4.1

[CNOT.1]: This follows immediately from **[TOF.15]**.

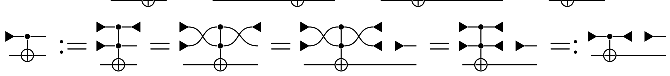
[CNOT.2]:



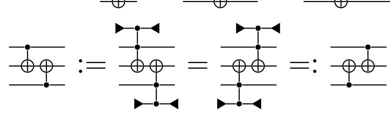
[CNOT.3]:



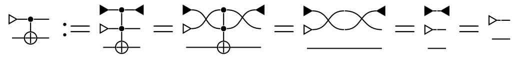
[CNOT.4]:

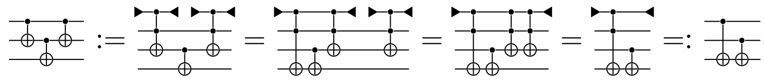


[CNOT.5]:



[CNOT.6]: This follows immediately from **[TOF.9]**.

[CNOT.7]: 

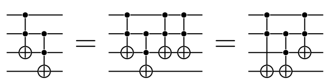
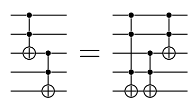
[CNOT.8]: 

[CNOT.9]: This follows immediately from **[TOF.10]**.

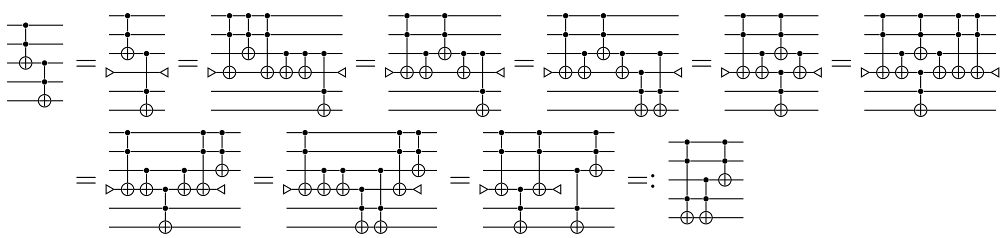
B Proof of Proposition 5.3

First, we show how tof gates can be “pushed past” each other with a “trailing” side-effect:

Lemma B.1.

(i)  *(ii)* 

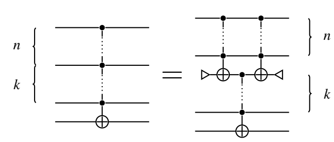
Proof. Of part *(ii)*:



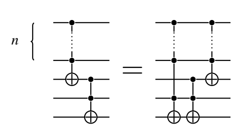
□

Recall the statement of Proposition 5.3:
Given some $n \geq 1$ and $k \geq 1$:

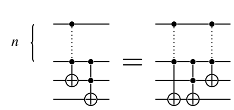
(i) cnot_{n+k} gates can be zipped and unzipped:



(ii) cnot_n gates can be pushed past Toffoli gates in the following sense:



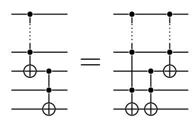
(iii) And likewise:



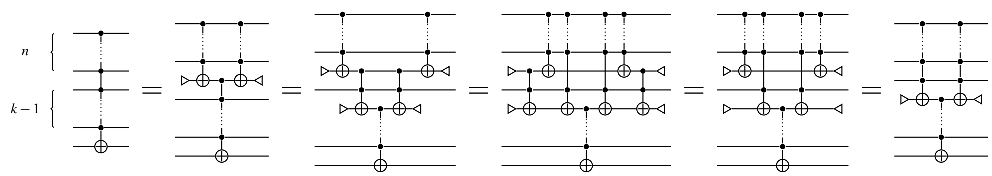
The proof is by a simultaneous induction for claims *(i)* and *(ii)* on the number of control wires, n, to unzip and the number of control wires being pushed past a Toffoli gate. Claim *(iii)* follows as a consequence.

Proof. For the induction, suppose that $n,k \geq 2$. The cases when $n = 1$ or $n = 2$ follow as a consequence.

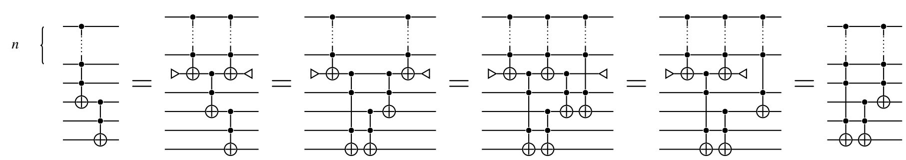
- The base cases of claim *(i)* follows by the definition of the cnot_n gate. The base cases of claim *(ii)* Lemma is precisely Lemma B.1*(ii)*.
- For $n \geq 2$: assume that for any $m > n$ and all $k \leq n$, we can unzip a cnot_m gate k levels down that and we can push a cnot_n gate past a tof gate as follows:



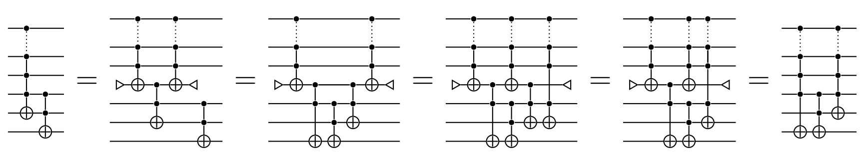
Consider the two identities for $n+1$; first for the zipper:



For the second inductive step, observe:



Observe that the claim holds when not both $k \geq 2$ and $n \geq 2$, as a consequence of the induction. For claim *(iii)*, we use claims *(i)* and *(ii)* to observe:



□

C Proof of Lemma 5.5

Recall the statement of Lemma 5.5:

(i) $\oplus_x^X \oplus_x^X = 1$

(ii) When $x \in X$ then $\triangleright_x \oplus_y^X = \triangleright_x$

(iii) When the target wire are the same $\oplus_x^X \oplus_x^Y = \oplus_x^Y \oplus_x^X$

(iv) When $x \notin Y$ and $y \notin X$ then $\oplus_x^X \oplus_y^Y = \oplus_y^Y \oplus_x^X$

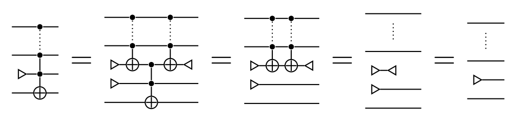
(v) $\oplus_x^X \oplus_y^{\{x\}\sqcup Y} = \oplus_y^{X\cup Y} \oplus_y^{\{x\}\sqcup Y} \oplus_x^X$

(vi) $\rhd_z \oplus_z^{\{x\}} \oplus_y^{\{x\}\sqcup X} = \rhd_z \oplus_z^{\{x\}} \oplus_y^{\{z\}\sqcup X}$

We prove each case separately:

(i) This is Lemma 5.2.

(ii) Using Corollary 5.4 it suffices to consider the case where x is the bottom control wire. Using Proposition 5.3 *(i)* and Lemma 5.2, observe:



(iii) The proof follows easily from Axioms **[TOF.3]**, **[TOF.4]**, **[TOF.5]** and **[TOF.6]**.

(iv) The proof follows easily from Axioms **[TOF.4]** and **[TOF.5]**.

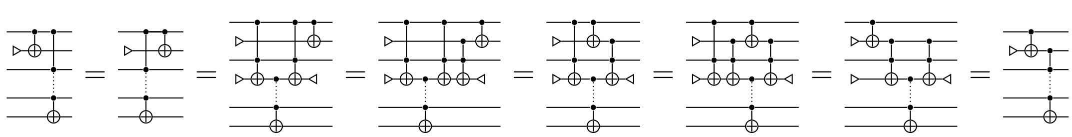
(v) The proof is by induction on the number of control wires of the second gate.

The base cases are provided by Proposition 5.3 *(ii)* and *(iii)*.

Suppose now that the claim holds for all cases in which the second gate has no more than n control wires. Consider when the second gate has $n+1$ control wires. Using Corollary 5.4 it suffices to consider the case where y is the bottom wire and x is the second bottom wire:

$$
\begin{aligned}
\oplus_x^X \oplus_y^{Y\sqcup\{x\}} &= \oplus_x^X \rhd_z \oplus_z^Y \oplus_y^{\{z,x\}} \oplus_z^Y \lhd_z && \text{Use Prop. 5.3 } (i) \text{ to unzip } \oplus_y^{Y\sqcup\{x\}} \text{ to the bottom}\\
&= \rhd_z \oplus_z^Y \oplus_x^X \oplus_y^{\{z,x\}} \oplus_z^Y \lhd_z &&\\
&= \rhd_z \oplus_z^Y \oplus_y^{X\sqcup\{z\}} \oplus_y^{\{z,x\}} \oplus_x^X \oplus_z^Y \lhd_z && \text{Prop. 5.3 } (ii), (iii)\\
&= \rhd_z \oplus_z^Y \oplus_y^{X\sqcup\{z\}} \oplus_y^{\{z,x\}} \oplus_z^Y \oplus_x^X \lhd_z &&\\
&= \rhd_z \oplus_z^Y \oplus_y^{X\sqcup\{z\}} \oplus_z^Y \oplus_y^{\{z,x\}} \oplus_y^{Y\sqcup\{x\}} \oplus_x^X \lhd_z && \text{Prop. 5.3 } (ii), (iii)\\
&= \rhd_z \oplus_z^Y \oplus_z^Y \oplus_y^{X\sqcup\{z\}} \oplus_y^{X\cup Y} \oplus_y^{\{z,x\}} \oplus_y^{Y\sqcup\{x\}} \oplus_x^X \lhd_z && \text{Ind. Hyp.}\\
&= \rhd_z \oplus_y^{X\sqcup\{z\}} \oplus_y^{X\cup Y} \oplus_y^{\{z,x\}} \oplus_y^{Y\sqcup\{x\}} \oplus_x^X \lhd_z &&\\
&= \rhd_z \oplus_y^{X\sqcup\{z\}} \oplus_y^{X\cup Y} \oplus_y^{\{z,x\}} \lhd_z \oplus_y^{Y\sqcup\{x\}} \oplus_x^X &&\\
&= \rhd_z \oplus_y^{X\cup Y} \lhd_z \oplus_y^{Y\sqcup\{x\}} \oplus_x^X && \text{Lem. 5.5 } (ii)\\
&= \rhd_z \lhd_z \oplus_y^{X\cup Y} \oplus_y^{Y\sqcup\{x\}} \oplus_x^X &&\\
&= \oplus_y^{X\cup Y} \oplus_y^{Y\sqcup\{x\}} \oplus_x^X &&
\end{aligned}
$$

(vi) Using Corollary 5.4, it suffices to observe:



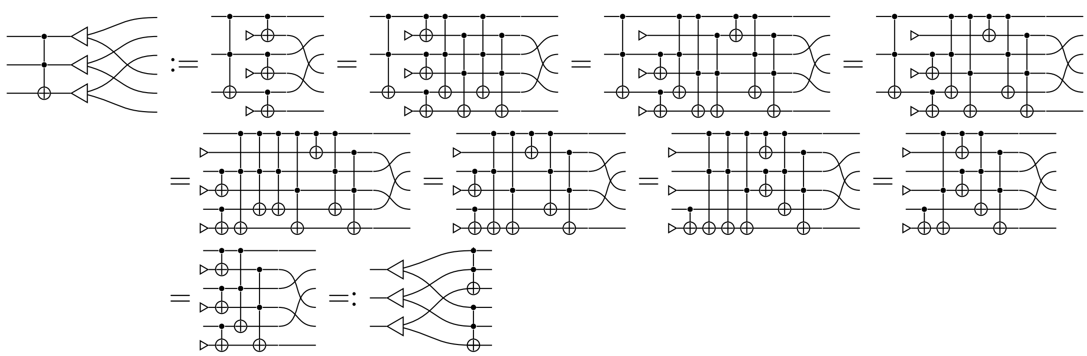
D Proof of Proposition 6.2

Most of the proof is inherited from [5] using Lemma 4.1.

We first show that Δ is a natural transformation:

Lemma D.1. Δ is a natural transformation in TOF.

Proof. We prove that Δ is a natural transformation by structural induction. We have only to prove the inductive case for tof as the cases for the 1-ancillary bits are proven in [5, Lemma B.3]:

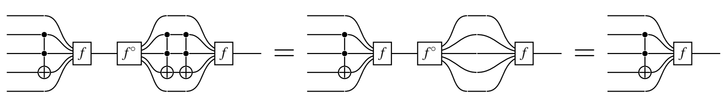


$\square$

To prove that TOF is a discrete inverse category with respect to $(\_)^\circ : \mathsf{TOF}^{\mathsf{op}} \to \mathsf{TOF}$ it must also be shown that **[INV.1]**, **[INV.2]** and **[INV.3]** hold. As **[INV.1]** is immediate it remains to prove **[INV.2]** and **[INV.3]**:

Lemma D.2. For all maps f in TOF **[INV.2]** holds, that is $ff^\circ f = f$.

Proof. We prove that **[INV.2]** holds by structural induction. Again we have only to prove the inductive case for tof as the cases for the ancillary bits are proven in [5, Lemma B.14]. Suppose inductively that $ff^\circ f = f$ for some circuit f, then we need to show that we can extend f by a tof gate and preserve the property. This is almost immediate as:



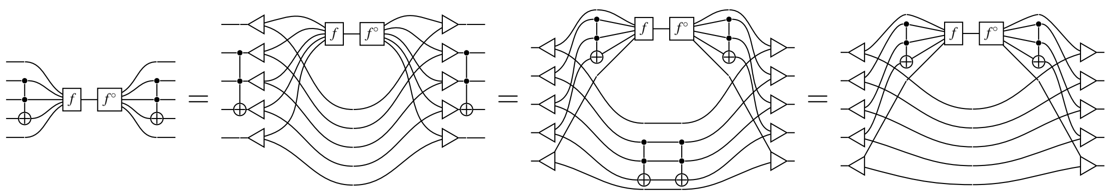
$\square$

To prove that **[INV.3]** holds, we identify the restriction idempotents of TOF with what are called latchable circuits. A map f in a discrete, symmetric monoidal category is called **latchable** when $\Delta(f \otimes 1)\Delta^\circ$ [5, Definition B.9]. We already know that latchable circuits commute with each other [5, Lemma B.10]; therefore, to prove that all circuits of the form ff° are latchable is to prove that **[INV.3]** holds.

Lemma D.3. Circuits of the form ff° in TOF are latchable and, thus, **[INV.3]** holds.

Proof. We prove that circuits of the form ff° in TOF are latchable by structural induction. We have only to prove the inductive case for tof as the cases for the 1-ancillary bits are proven in [5, Proposition

B.12]: Suppose that some circuit f is latchable, then we must show inductively that adjoining a Toffoli gate will result in a latchable circuit:



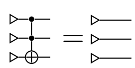
$\square$

This allows us to Proposition 6.2:

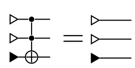
Proof. Lemmas D.2 and D.3 show that TOF is an inverse category. Lemma D.1 and the fact that the semi-Frobenius identities hold in CNOT imply that $(n, \Delta_n, \Delta_n^\circ)$ forms a natural separable, commutative, semi-Frobenius algebra for all $n \in \mathbb{N}$. Thus, TOF is a discrete inverse category. $\square$

E Proof of Lemma 7.1

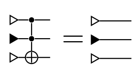
$\mathsf{tof}(|000\rangle) = |000\rangle$:



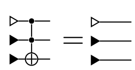
$\mathsf{tof}(|001\rangle) = |001\rangle$:



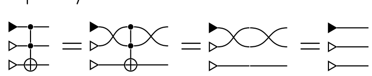
$\mathsf{tof}(|010\rangle) = |010\rangle$:



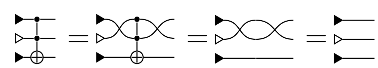
$\mathsf{tof}(|011\rangle) = |011\rangle$:



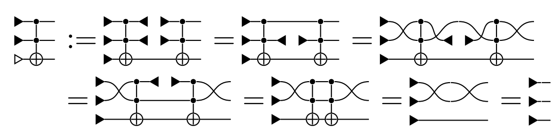
$\mathsf{tof}(|100\rangle) = |100\rangle$:



$\mathsf{tof}(|101\rangle) = |101\rangle$:



$\mathsf{tof}(|110\rangle) = |111\rangle$:



$\mathsf{tof}(|111\rangle) = |110\rangle$: