The Category TOF

Robin Cockett, Cole Comfort

University of Calgary

June 6, 2018

Outline

Background

Background

The Toffoli gate is a linear map $|x_1, x_2, x_3\rangle \mapsto |x_1, x_2, x_1 \cdot x_2 + x_3 \mod 2\rangle$.
It is given by the following matrix:

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

The Toffoli gate is universal for classical reversible computing: every reversible Boolean function can be simulated with Toffoli gates and fixed/input/output bits.

The Toffoli gate is the "most-universal" classically reversible gate, since we don't have to ignore any of the output bits.

This leads to the question: *what identities characterize this universal class of circuits?*

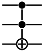
The Category TOF

The Category TOF

Define the symmetric monoidal category TOF:

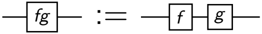
Objects: Natural numbers.

Maps: Generated by the following components:

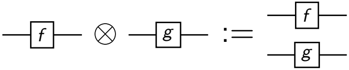
$tof \equiv$  $|1\rangle \equiv$  $\langle 1| \equiv$ 

$|1\rangle$ and $\langle 1|$ are called the 1-ancillary bits.

Composition:



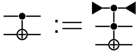
Tensor:



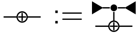
The Category TOF: Basic Components

Define some basics components with these generators:

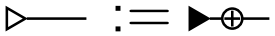
The controlled-not (*cnot*) gate :



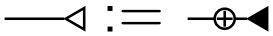
The *not* gate:



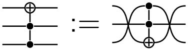
The 0 input ancillary bit:



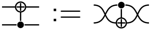
The 0 output ancillary bit:



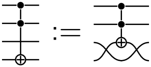
The flipped *tof* gate:



The flipped *cnot* gate:

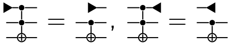


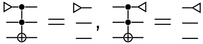
We also allow gaps in between the target/control wires:

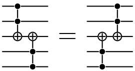


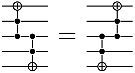
We require that these components satisfy the following identities:

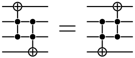
The Category TOF: Identities

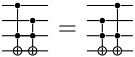
[TOF.1] 

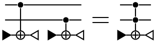
[TOF.2] 

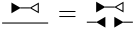
[TOF.3] 

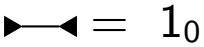
[TOF.4] 

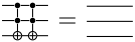
[TOF.5] 

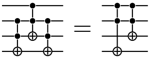
[TOF.6] 

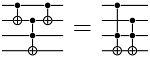
[TOF.7] 

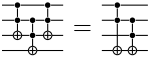
[TOF.8] 

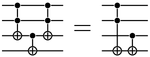
[TOF.9] 

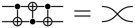
[TOF.10] 

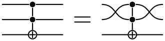
[TOF.11] 

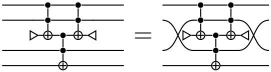
[TOF.12] 

[TOF.13] 

[TOF.14] 

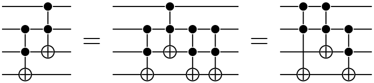
[TOF.15] 

[TOF.16] 

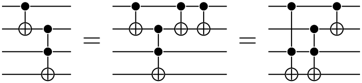
[TOF.17] 

Justification for [TOF.11]-[TOF.14]

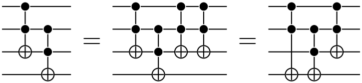
For [TOF.11]:



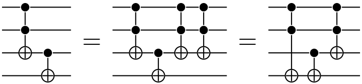
For [TOF.12]:



For [TOF.13]:



For [TOF.14]:



Proof Overview

We show:

Theorem

TOF *is discrete-inverse equivalent to* FPinj_2.

The proof follows the same general structure of CNOT, for which we proved a similar completeness result for the *cnot* gate:

1. Prove that TOF is a discrete inverse category.
2. Construct a normal form for the idempotents of TOF.
3. Construct a functor $H : \mathrm{TOF} \to \mathrm{FPinj}_2$ and use the normal form to show it is full and faithful on restriction idempotents.
4. Use the discrete inverse structure of TOF to extend the fullness and faithfulness of $H : \mathrm{TOF} \to \mathrm{FPinj}_2$ on idempotents to show $H : \mathrm{TOF} \to \mathrm{FPinj}_2$ is an equivalence.

TOF is a Discrete Inverse Category

Restriction Categories

A **restriction category** $\mathbb{X}$ is a category along with an assignment of an arrow $\overline{f} : A \to A$ for each $f : A \to B$ such that the following identities hold:

[R.1] $\overline{f} f = f$

[R.2] $\overline{g}\,\overline{f} = \overline{f}\,\overline{g}$

[R.3] $\overline{\overline{f} g} = \overline{f}\,\overline{g}$

[R.4] $f \overline{g} = \overline{fg} f$

Maps of the form $\overline{f}$ for some f are called **restriction idempotents**.
Restriction categories generalize the category of sets and partial maps, Par, where:

$$\overline{f}(x) := \begin{cases} x & \text{If } f(x) \downarrow \\ \uparrow & \text{Otherwise} \end{cases}$$

Inverses and isomorphisms are generalized in restriction categories.
Given a map $f : A \to B$, a map $g : B \to A$ is the **partial inverse** of f when $fg = \overline{f}$ and $gf = \overline{g}$.
A map is a **partial isomorphism** when it has a partial inverse.
Just like normal inverses, partial inverses are unique and the composition of two partial isomorphisms is a partial isomorphism.

Inverse Categories

A restriction category is an **inverse category** when every map is a partial isomorphism.

Alternatively, $\mathbb{X}$ is an inverse category when there is an identity-on-objects functor $(\_)^\circ : \mathbb{X}^{\mathsf{op}} \to \mathbb{X}$ such that:

(INV.1) $(f^\circ)^\circ = f$

(INV.2) $ff^\circ f = f$

(INV.3) $ff^\circ gg^\circ = gg^\circ ff^\circ$

The functor takes maps to their partial inverses, so that $\overline{f} := ff^\circ$.

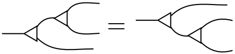
All idempotents in inverse categories are restriction idempotents.

Denote the category sets and partial isomorphisms by Pinj.

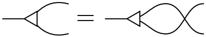
Discrete Inverse Categories

An inverse category $\mathbb{X}$ has **inverse products** when it has a symmetric tensor product which preserves restriction and there is total natural diagonal transformation Δ such that:

- Δ is coassociative:

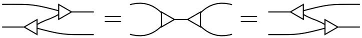


- Δ is cocommutative:

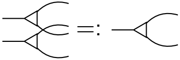


Discrete Inverse Categories

- Δ satisfies the semi-Frobenius (non-unital Frobenius) identity:



- Δ satisfies the uniform copying identity:

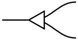
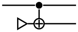
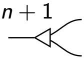
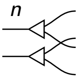


A category with inverse products is a **discrete inverse category**.

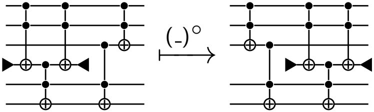
Discrete Inverse Structure of TOF

TOF is a discrete inverse category in the same way as CNOT:

- Δ is defined inductively, such that $\Delta_0 := 1_0$,

  $\Delta_1 =$  $:=$  and $\Delta_{n+1} =$  $:=$ 

- The functor $(\_)^{\circ} : \mathrm{TOF}^{op} \to \mathrm{TOF}$ is defined by horizontally flipping circuits, taking $|1\rangle \mapsto \langle 1|$, $\langle 1| \mapsto |1\rangle$, $tof \mapsto tof$.
  For example:

The total points look like an n-fold tensor product of computational ancillary bits.

The other points are equivalent to a circuit containing the map  .

Generalized controlled-not Gates

Generalized controlled not gates

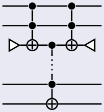
Before we can construct a normal form for the restriction idempotents of TOF, we must construct generalized controlled not gates:

Definition

$$cnot_0 := not, \qquad cnot_1 := cnot, \qquad cnot_2 := tof$$

$$cnot_{n+1} \equiv n \left\{ \right.$$

$$:=$$



The wires with the dots are called the **control wires** and the wire with the $\oplus$ is called the **target wire**.

Algebraically denote a $cnot_n$ gate with gaps/permuted wires by $\oplus_x^X$, where X are the control wires and x is the target wire.

To prove the completeness of TOF, we must also exhibit some of the basic properties of $cnot_n$ gates.

Iwama's identities

In their paper, "Transformation rules for designing cnot-based quantum circuits," Iwama, Kambayashi, and Yamashita, gave an infinite, complete set of identities for circuits of the form:

$$|x_1, \cdots, x_n, y\rangle \mapsto |x_1, \cdots, x_n, y + f(x_1, \cdots, x_n) \mod 2\rangle$$

generated by $cnot_n$ gates and finitely many $|0\rangle$ auxiliary bits.

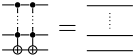
An auxiliary bit for the state $|x\rangle$ is a designated pair of extra ignored input and output wires, satisfying the condition that if $|x\rangle$ is plugged into an auxiliary bit input wire, $|x\rangle$ will be produced on the designated output wire.

Note, that *these circuits are only a small fragment of the circuits of* TOF. For example, using auxiliary bits instead of ancillary bits forces all circuits to be total.

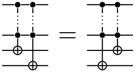
Iwama's identities

The identities are as follows: (where $\rhd_x$ denotes the input of a $|0\rangle$ auxiliary bit on wire x wedged by identity wires):

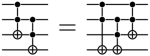
(i) $\oplus_x^X \oplus_x^X = 1$ graphically:



(ii) $\oplus_x^X \oplus_y^Y = \oplus_y^Y \oplus_x^X$ if $x \notin Y$ and $y \notin X$ for example:



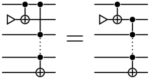
(iii) $\oplus_x^X \oplus_y^{\{x\} \sqcup Y} = \oplus_y^{X \cup Y} \oplus_y^{\{x\} \sqcup Y} \oplus_x^X$ for example:



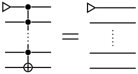
We call this identity the "pushing Lemma" because it allows $cnot_n$,$cnot_m$ gates to be pushed past each other with a trailing $cnot_k$ gate.

(iv) $\oplus_y^{\{x\} \sqcup Y} \oplus_x^X = \oplus_x^X \oplus_y^{\{x\} \sqcup Y} \oplus_y^{X \cup Y}$ this is dual to (iii)

(v) $\rhd_z \oplus_z^{\{x\}} \oplus_y^{\{x\} \sqcup X} = \rhd_z \oplus_z^{\{x\}} \oplus_y^{\{z\} \sqcup X}$ for example:



(vi) $\rhd_x \oplus_y^{\{x\} \sqcup X} = \rhd_x$ for example:



Indeed, all of these identities hold in TOF.

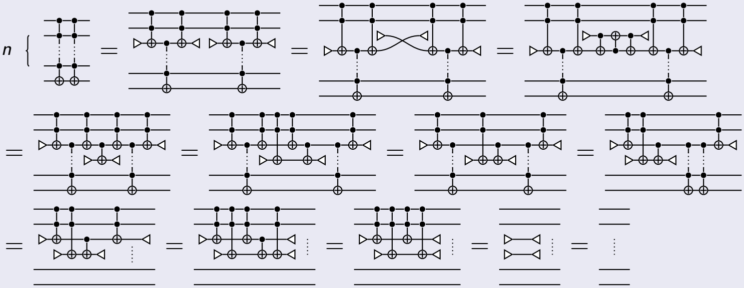
Identity (i) is easy to prove:

Lemma

$cnot_n$ gates are self-inverse.

Proof.

The base cases for *not*, *cnot* and *tof* are easy. For the inductive case:



$\square$

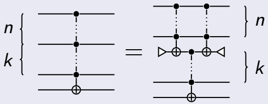
The zipper

With these two Lemmas, it isn't too hard to prove the following claim (by simultaneous induction on claims (i) and (ii)):

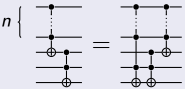
Proposition

For $n \geq 1$ and $k \geq 1$:

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



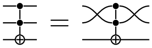
(ii) *$cnot_n$ gates can be pushed past Toffoli gates in the following sense:*

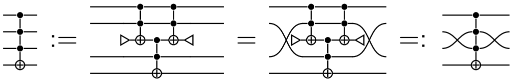


Notice that part (ii) is a special case of Iwama's identity (iii), where $|X| = 2$.

Recall the two identities:

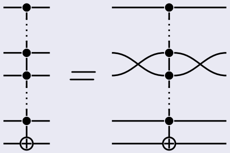
[TOF.16] **[TOF.17]**





These two identities and part (i) of the previous proposition imply:

Corollary



Completeness of TOF

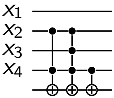
Representations of Polynomials in TOF

Iwama et. al give a normal form for their restricted classes of circuits; in TOF this corresponds to:

Definition

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 generalized controlled-not gate targeting the last wire.

These circuits correspond to polynomials (up to the normal form for polynomials over $\mathbb{Z}_2$), for example, the following circuit corresponds to the polynomial $x_2x_4 + x_2x_3x_4 + x_4$ in $\mathbb{Z}_2[x_1, x_2, x_3, x_4]$:



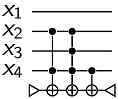
A Normal Form for the Restriction Idempotents of TOF

For the normal form for the restriction idempotents of TOF, we restrict the value of the polynomial to 0:

Definition

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 corresponds to the polynomial equation $x_2x_4 + x_2x_3x_4 + x_4 = 0$:



The uniqueness of polyforms follows from the uniqueness of polynomial expansions along with the self-inverse property of $cnot_n$ gates and obvious commutativity results.

Polyforms are Idemptotent

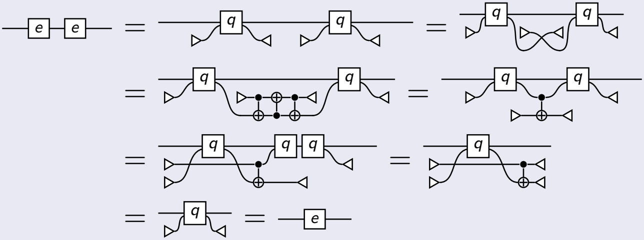
For the one direction:

Lemma

Polyforms are idempotent.

Proof.

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



$\square$

Idemptotents have polyforms

Conversely:

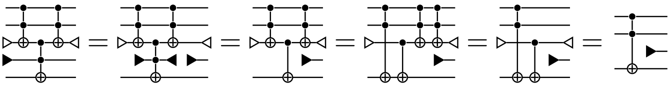
Lemma

Idempotents have polyforms.

The proof is by structural induction, wedging maps between all of the generators and their partial inverses.

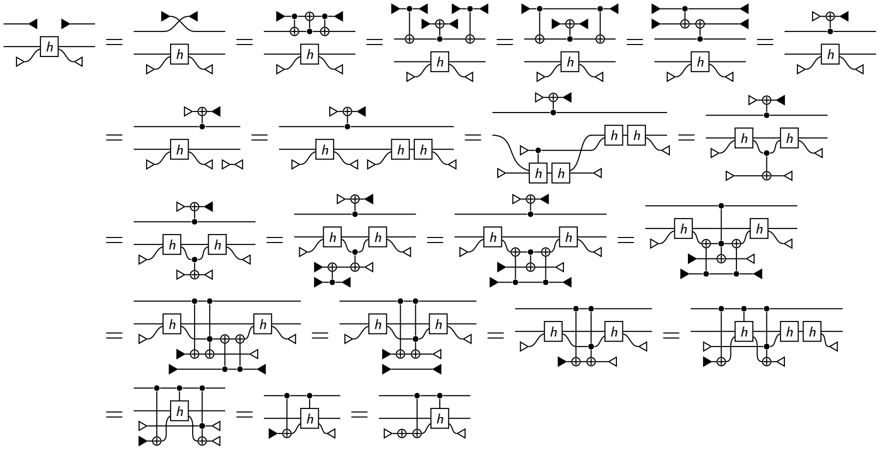
Case 1: For the generator *tof*, the claim follows from Iwama's identity.

Case 2: For $|1\rangle$ we can use the previous corollary to only consider the case where $|1\rangle$ is on the very bottom control wire:



Case 3: For $\langle 1|$: The structure proof similar to the proof that polyforms are Idempotent, but involves Iwama's pushing identity.

Case 3: For $\langle 1|$:



The Full and Faithful $(\_)^{\circ}$-Functor from TOF

Definition

Let FPinj_2 be the full subcategory of Pinj with objects: sets with cardinalities finite powers of 2.

Define a functor into this category (which will be shown to be an equivalence):

Definition

Define the functor $H : \mathsf{TOF} \to \mathsf{FPinj}_2$:

On Objects: $H(n) := \{f \in \mathsf{TOF}(0,n) | \overline{f} = 1_0\}$

On Maps: For each map $f : n \to m$, for all $g \in H(n)$:

$$(H(f))(g) := \begin{cases} gf & \text{if } \overline{gf} = 1_0 \\ \uparrow & \text{otherwise} \end{cases}$$

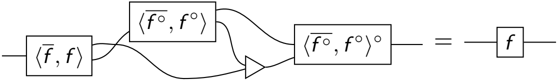
It is not hard to show that $H : \mathsf{TOF} \to \mathsf{FPinj}_2$

- ...preserves inverse products.
- ...is full and faithful on idempotents (using their normal form).

Completeness

We lift the fullness and faithfulness of $H : \mathrm{TOF} \to \mathrm{FPinj}_2$ on idempotents, to its fullness and faithfulness in general.

For the fullness, note that for all total maps f in FPinj_2, using polynomial forms we can construct a map g in TOF such that $H(g) = \Delta(1 \otimes f) = \langle 1, f \rangle$. But since H is full on restriction idempotents, for any map f in FPinj_2, the following map is in $H(\mathrm{TOF})$:



For the faithfulness we use the fact that discrete inverse categories have meets, given by $f \cap g := \Delta(f \otimes g)\Delta^\circ$.

Therefore:

Theorem

TOF *is discrete-inverse equivalent to* FPinj_2.

Thank you for Listening.
Questions?

References

Scott Aaronson, Daniel Grier, and Luke Schaeffer, *The classification of reversible bit operations*, LIPIcs-Leibniz International Proceedings in Informatics, vol. 67, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

Robin Cockett, Cole Comfort, and Priyaa Srinivasan, *The category CNOT*, Electronic Proceedings in Theoretical Computer Science **266** (2018), 258–293.

J Robin B Cockett and Stephen Lack, *Restriction categories i: categories of partial maps*, Theoretical computer science **270** (2002), no. 1-2, 223–259.

Edward Fredkin and Tommaso Toffoli, *Conservative logic*, Collision-based computing, Springer, 2002, pp. 47–81.

Brett Giles, *An investigation of some theoretical aspects of reversible computing*, Ph.D. thesis, University of Calgary, 2014.

Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita, *Transformation rules for designing cnot-based quantum circuits*, Proceedings of the 39th annual Design Automation Conference, ACM, 2002, pp. 419–424.

Yves Lafont, *Towards an algebraic theory of boolean circuits*, Journal of Pure and Applied Algebra **184** (2003), no. 2-3, 257–310.