ZH-calculus: completeness and extensions

Miriam Backens	University of Birmingham
Aleks Kissinger	Oxford University
Hector Miller-Bakewell	
John van de Wetering	Radboud/Oxford
Sal Wolffs	Radboud University Nijmegen

ACT2021 — July 15th

An alternative title from `x.writefull.com/title-generator`

x.writefull.com/title-generator/index.html

A ZH-Calculus, an Alternative GUI for Quantum Information

ABSTRACT

There are various gate sets used for describing quantum computation. A particularly popular one consists of Clifford gates and arbitrary single-qubit phase gates. Computations in this gate set can be elegantly described by the \emph{ZX-calculus}, a graphical language for a class of string diagrams describing linear maps between qubits. The ZX-calculus has proven useful in a variety of areas of quantum information, but is less suitable for reasoning about operations outside its natural gate set such as multi-linear Boolean operations like the Toffoli gate. In this paper we study the \emph{ZH-calculus}, an alternative graphical language of string diagrams that does allow straightforward encoding of Toffoli gates and other more complicated Boolean logic circuits. We find a set of simple rewrite rules for this calculus and show it is complete with respect to matrices over $\mathbb Z[\frac12]$, which correspond to the approximately universal Toffoli+Hadamard gateset. Furthermore, we construct an extended version of the ZH-calculus that is complete with respect to matrices over any ring R where $1+1$ is not a zero-divisor.

tl;dr

- ZX-calculus is universal language for quantum computing
- Great for Clifford+Phases gate set, not so great for Toffoli

tl;dr

- ZX-calculus is universal language for quantum computing
- Great for Clifford+Phases gate set, not so great for Toffoli
- ZH-calculus introduced to be great for Toffoli's
- Original ZH [QPL'18] complete for universal fragment

tl;dr

- ZX-calculus is universal language for quantum computing
- Great for Clifford+Phases gate set, not so great for Toffoli
- ZH-calculus introduced to be great for Toffoli's
- Original ZH [QPL'18] complete for universal fragment

In this work:

- We find subset of rules complete for Toffoli+Hadamard
- We find original set of rules complete for (almost) any ring

tl;dr

- ZX-calculus is universal language for quantum computing
- Great for Clifford+Phases gate set, not so great for Toffoli
- ZH-calculus introduced to be great for Toffoli's
- Original ZH [QPL'18] complete for universal fragment

In this work:

- We find subset of rules complete for Toffoli+Hadamard
- We find original set of rules complete for (almost) any ring
- Along the way we find way to encode arithmetic in ZH

First some motivation for the calculus

Boolean maps

A Boolean map is $f : \{0,1\}^n \to \{0,1\}^m$.

This gives linear map $\hat{f} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ by

$$\hat{f} \, |x_1 \ldots x_n\rangle = |f(x_1 \ldots x_n)\rangle$$

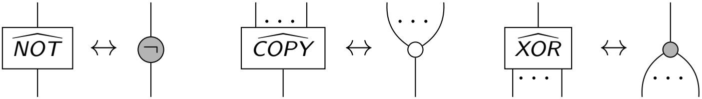
Boolean maps

A Boolean map is $f : \{0,1\}^n \to \{0,1\}^m$.

This gives linear map $\hat{f} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ by

$$\hat{f}\,|x_1 \ldots x_n\rangle = |f(x_1 \ldots x_n)\rangle$$

Examples:



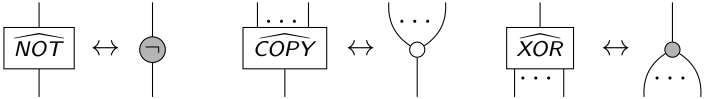
Boolean maps

A Boolean map is $f : \{0,1\}^n \to \{0,1\}^m$.

This gives linear map $\hat{f} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ by

$$\hat{f}\,|x_1 \dots x_n\rangle = |f(x_1 \dots x_n)\rangle$$

Examples:



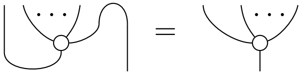
What about $\widehat{AND}$?

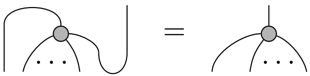
Flexsymmetry

COPY, XOR, AND are symmetric wrt swaps on inputs/outputs

Flexsymmetry

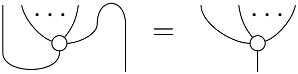
COPY, XOR, AND are symmetric wrt swaps on inputs/outputs
But COPY and XOR are also **flexsymmetric**:

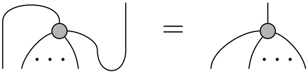




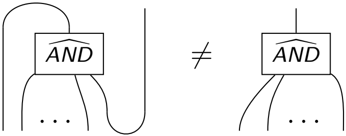
Flexsymmetry

COPY, XOR, AND are symmetric wrt swaps on inputs/outputs
But COPY and XOR are also **flexsymmetric**:





Not true for AND:

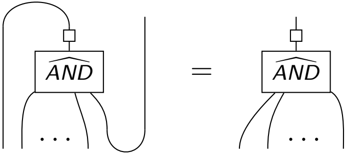


Fixing flexsymmetry

Can we make AND flexsymmetric?

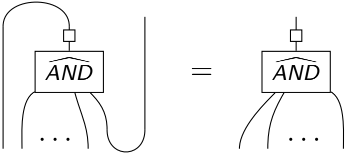
Fixing flexsymmetry

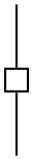
Can we make AND flexsymmetric?
Yes, there exists a linear map such that:



Fixing flexsymmetry

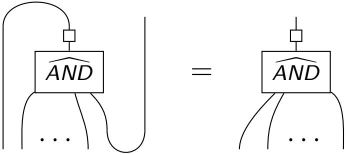
Can we make AND flexsymmetric?
Yes, there exists a linear map such that:

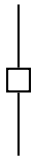


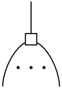
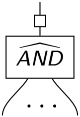
Namely:  $:= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Fixing flexsymmetry

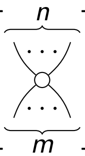
Can we make AND flexsymmetric?
Yes, there exists a linear map such that:



Namely:  $:= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

We define:  $:= \frac{1}{2}$ 

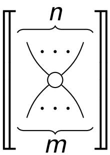
ZH-calculus generators

Z-spider: 

$$\left[\!\!\left[\cdot \right]\!\!\right] := |0\rangle^{\otimes n} \langle 0|^{\otimes m} + |1\rangle^{\otimes n} \langle 1|^{\otimes m}$$

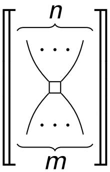
ZH-calculus generators

Z-spider:



$$:= |0\rangle^{\otimes n} \langle 0|^{\otimes m} + |1\rangle^{\otimes n} \langle 1|^{\otimes m}$$

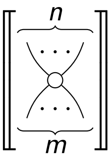
H-box:

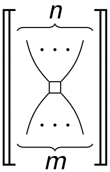


$$:= \sum (-1)^{i_1 \ldots i_m j_1 \ldots j_n} |j_1 \ldots j_n\rangle \langle i_1 \ldots i_m|$$

where the sum is over all $i_1, \ldots, i_m, j_1, \ldots, j_n \in \{0, 1\}$.

ZH-calculus generators

Z-spider:  $:= |0\rangle^{\otimes n} \langle 0|^{\otimes m} + |1\rangle^{\otimes n} \langle 1|^{\otimes m}$

H-box:  $:= \sum (-1)^{i_1 \ldots i_m j_1 \ldots j_n} |j_1 \ldots j_n\rangle \langle i_1 \ldots i_m|$

where the sum is over all $i_1, \ldots, i_m, j_1, \ldots, j_n \in \{0, 1\}$.

$$\llbracket ✿ \rrbracket := \frac{1}{2}$$

$\llbracket \, | \, \rrbracket := |0\rangle\langle 0| + |1\rangle\langle 1|$ $\qquad$ $\llbracket \cup \rrbracket := |00\rangle + |11\rangle$ $\qquad$ $\llbracket \cap \rrbracket := \langle 00| + \langle 11|$.

Universality

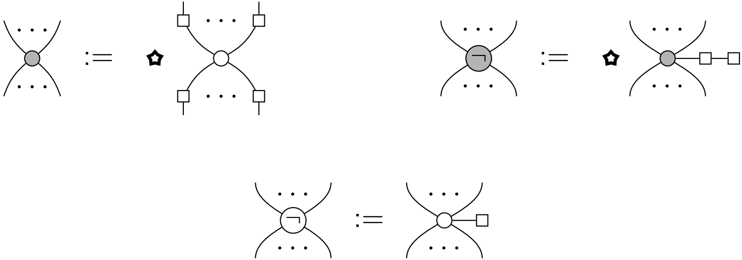
Composing these generators we can represent any $2^n \times 2^m$ matrix with entries in $\mathbb{Z}[\frac{1}{2}]$.

Universality

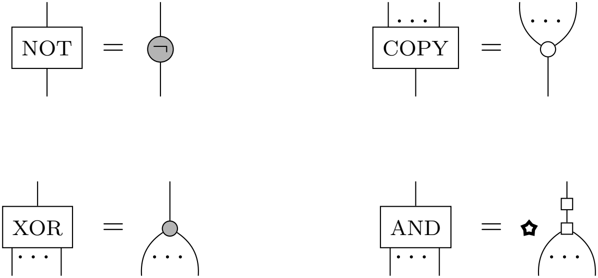
Composing these generators we can represent any $2^n \times 2^m$ matrix with entries in $\mathbb{Z}[\frac{1}{2}]$.

By Amy et al. (arxiv:1908.06076) this corresponds to circuits generated by Toffoli and $H \otimes H$.

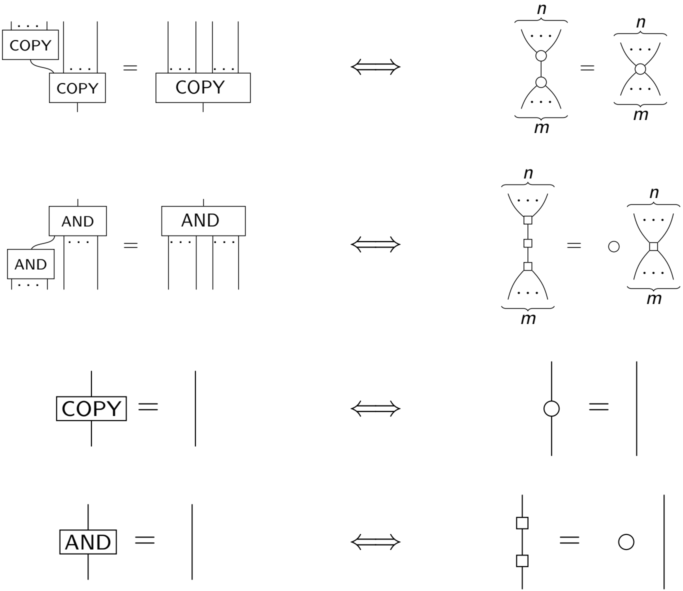
Derived generators



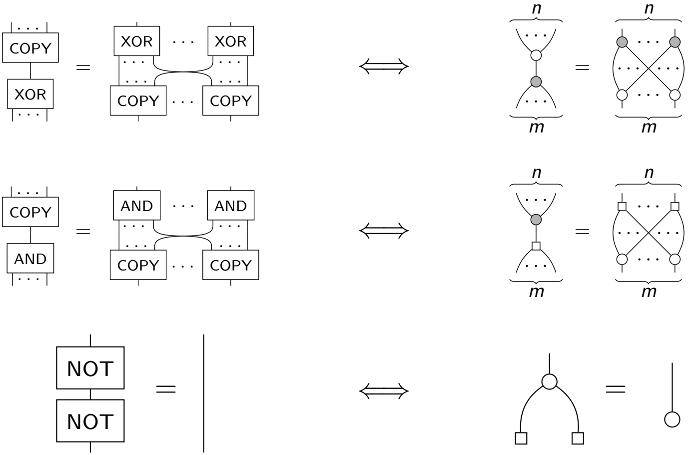
Boolean interpretation



Boolean rules #1

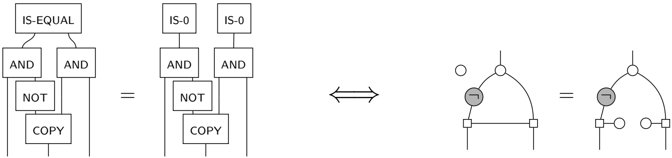


Boolean rules #2



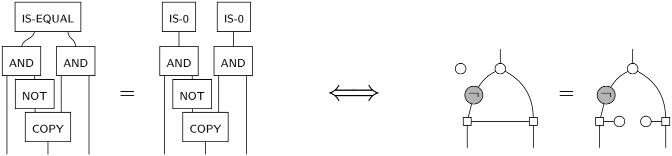
The final rule

Need one more rule:

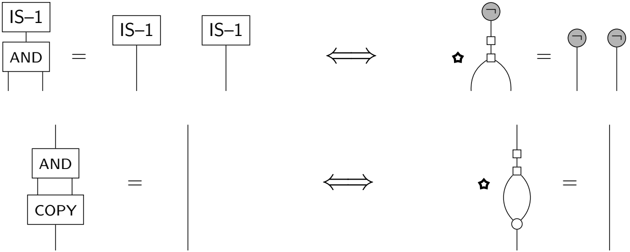


The final rule

Need one more rule:

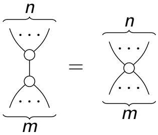


Or equivalently, a pair of rules:

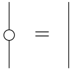


The rules

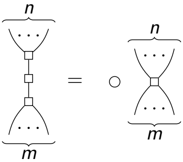
(zs)



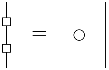
(id)



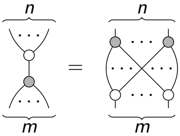
(hs)



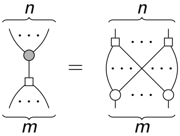
(hh)



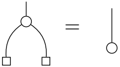
(ba_1)



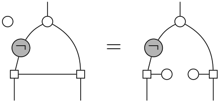
(ba_2)



(m)



(o)



Completeness

Theorem

These 8 rules are complete for matrices over $\mathbb{Z}[\frac{1}{2}]$.

Completeness

Theorem

These 8 rules are complete for matrices over $\mathbb{Z}[\frac{1}{2}]$.

Proof

Reduce each diagram to unique normal form.

Completeness

Theorem

These 8 rules are complete for matrices over $\mathbb{Z}[\frac{1}{2}]$.

Proof

Reduce each diagram to unique normal form.

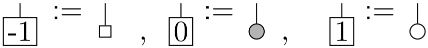
So essentially all of quantum computing boils down to those 8 rules.

Some useful structure

- Labelled H-boxes
- Arithmetic

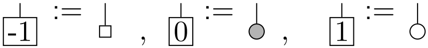
Labelled H-boxes

We represent state $(1, a)^T$ by a *labelled H-box*:

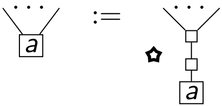


Labelled H-boxes

We represent state $(1, a)^T$ by a *labelled H-box*:

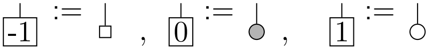


Extend to higher arity:

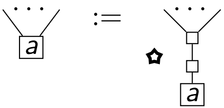


Labelled H-boxes

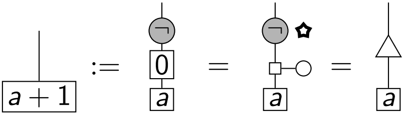
We represent state $(1, a)^T$ by a *labelled H-box*:



Extend to higher arity:

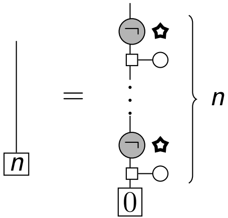


Can build higher numbers:

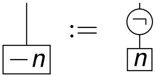


Integers

Natural numbers:

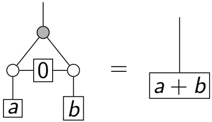


Negation:



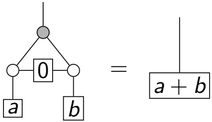
Arithmetic

Addition:

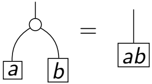


Arithmetic

Addition:

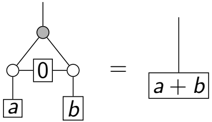


Multiplication:

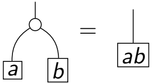


Arithmetic

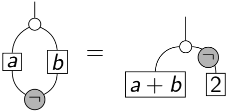
Addition:



Multiplication:



Average:



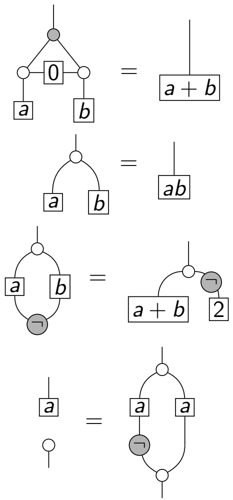
Arithmetic

Addition:

Multiplication:

Average:

Introduction:



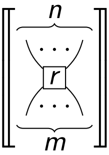
ZH over arbitrary rings

Let's promote labelled H-boxes to actual generators.

ZH over arbitrary rings

Let's promote labelled H-boxes to actual generators.

Pick commutative ring R where $2 := 1 + 1$ has an inverse $\frac{1}{2}$.
For any $r \in R$ define

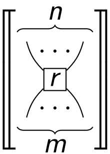


$$:= \sum r^{i_1 \ldots i_m j_1 \ldots j_n} \left|j_1 \ldots j_n\right\rangle \left\langle i_1 \ldots i_m\right| .$$

ZH over arbitrary rings

Let's promote labelled H-boxes to actual generators.

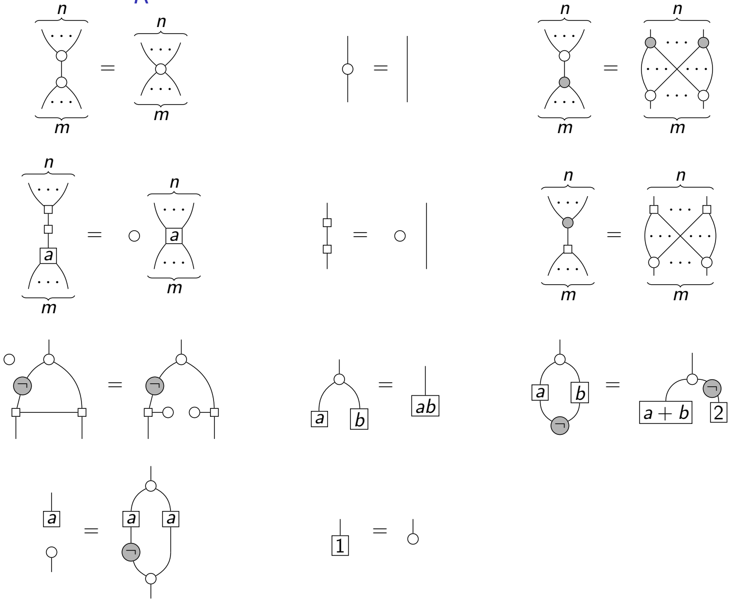
Pick commutative ring R where $2 := 1 + 1$ has an inverse $\frac{1}{2}$.
For any $r \in R$ define



$$:= \sum r^{i_1 \ldots i_m j_1 \ldots j_n} \left| j_1 \ldots j_n \right\rangle \left\langle i_1 \ldots i_m \right| .$$

The resulting ZH_R-diagrams are universal for matrices over R.

Rules for ZH_R



For all $a, b \in R$

Completeness for rings

Theorem

Let R be a commutative ring where 2 has an inverse.
Then this rule set is complete for matrices over R.

Completeness for rings

Theorem

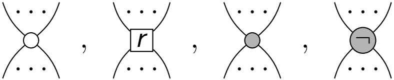
Let R be a commutative ring where 2 has an inverse.
Then this rule set is complete for matrices over R.

But what if 2 does not have an inverse, e.g. if $R = \mathbb{Z}$?
Problem, because:

$$[\![\text{✿}]\!] := \frac{1}{2}$$

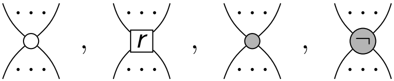
For general rings

Don't have a ✿ . So need other set of generators:



For general rings

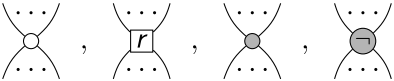
Don't have a ✿ . So need other set of generators:



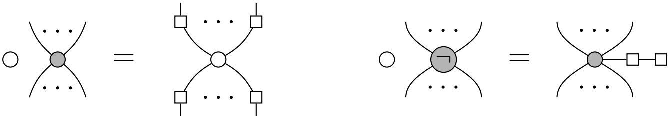
New rules:

For general rings

Don't have a ✿ . So need other set of generators:



New rules:



New meta-rule:

For any diagrams D_1 and D_2: $\circ\, D_1 = \circ\, D_2 \implies D_1 = D_2$

Note: only sound when 2 is not a zero divisor.

General completeness

Theorem

Let R be a commutative ring R where 2 is not a zero divisor. Then the rules + meta-rule make ZH_R complete for matrices over R.

Conclusion

- New small complete axiomatisation of Tof+Had circuits
- Clear relation to Boolean circuits
- Straightforwardly extended to (almost) arbitrary rings

Conclusion

- New small complete axiomatisation of Tof+Had circuits
- Clear relation to Boolean circuits
- Straightforwardly extended to (almost) arbitrary rings

Thank you for your attention

Backens, Kissinger, Miller-Bakewell, vdW, Wolffs 2021, arXiv:2103.06610.
Completeness of the ZH-calculus