

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

QPL2021 — June 8, 2021

Announcement: Quantum Pubquiz

- ▶ What: A quantum Pubquiz!
- ▶ When: Thursday 20:30CEST
- ▶ Where: Gathertown pub

No need to register, just show up :)

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 $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$.

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

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

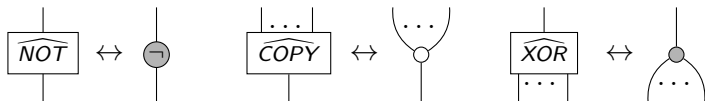
Boolean maps

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

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

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

Examples:



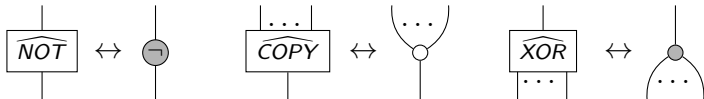
Boolean maps

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

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

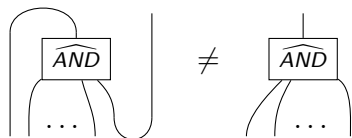


Flexsymmetry

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



Not true for AND:



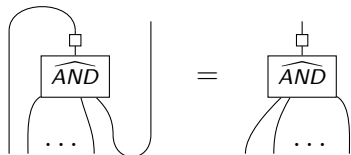
Fixing flexsymmetry

Can we make AND flexsymmetric?

Fixing flexsymmetry

Can we make AND flexsymmetric?

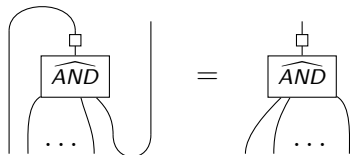
Yes, there exists a linear map such that:



Fixing flexsymmetry

Can we make AND flexsymmetric?

Yes, there exists a linear map such that:



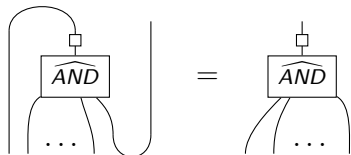
Namely:

$$\begin{array}{c} | \\ \square \\ | \end{array} := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Fixing flexsymmetry

Can we make AND flexsymmetric?

Yes, there exists a linear map such that:



Namely:

$$\begin{array}{c} | \\ \square \\ | \end{array} := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

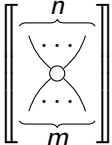
We define:

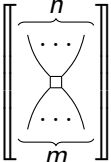
$$\begin{array}{c} | \\ \square \\ \cup \\ \dots \end{array} := \frac{1}{2} \begin{array}{c} | \\ \square \\ \widehat{\text{AND}} \\ \cup \\ \dots \end{array}$$

ZH-calculus generators

Z-spider: $\left[\left[\begin{array}{c} \overbrace{\quad}^n \\ \cdots \\ \circ \\ \cdots \\ \underbrace{\quad}_m \end{array} \right] \right] := |0\rangle^{\otimes n} \langle 0|^{\otimes m} + |1\rangle^{\otimes n} \langle 1|^{\otimes m}$

ZH-calculus generators

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

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

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

ZH-calculus generators

Z-spider: $\left[\left[\begin{array}{c} n \\ \vdots \\ \text{---} \\ \text{---} \\ \text{---} \\ \vdots \\ m \end{array} \right] \right] := |0\rangle^{\otimes n} \langle 0|^{\otimes m} + |1\rangle^{\otimes n} \langle 1|^{\otimes m}$

H-box: $\left[\left[\begin{array}{c} n \\ \vdots \\ \text{---} \\ \text{---} \\ \text{---} \\ \vdots \\ m \end{array} \right] \right] := \sum (-1)^{i_1 \dots i_m j_1 \dots j_n} |j_1 \dots j_n\rangle \langle i_1 \dots i_m|$

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

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

$$\llbracket | \rrbracket := |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\llbracket \cup \rrbracket := |00\rangle + |11\rangle$$

$$\llbracket \cap \rrbracket := \langle 00| + \langle 11|.$$

Universality

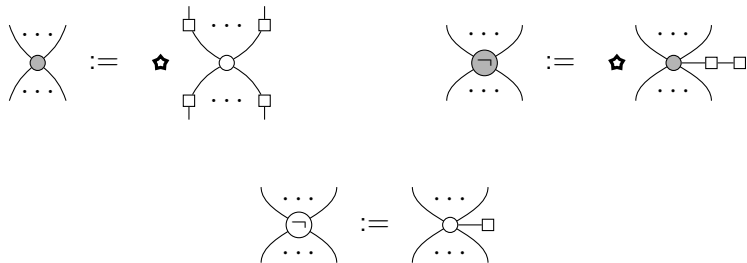
Composing these generators we can represent any $2^n \times 2^m$ matrix with entries in $\mathbb{Z}[\frac{1}{2}]$.

Universality

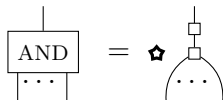
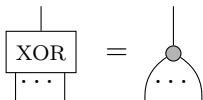
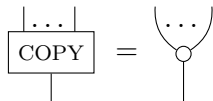
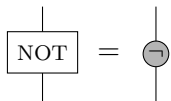
Composing these generators we can represent any $2^n \times 2^m$ matrix with entries in $\mathbb{Z}[\frac{1}{2}]$.

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

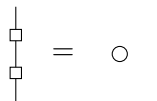
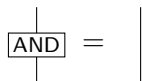
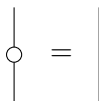
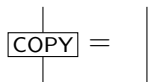
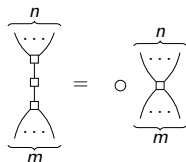
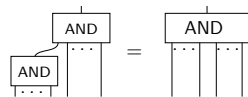
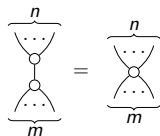
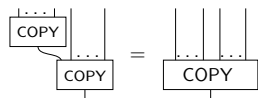
Derived generators



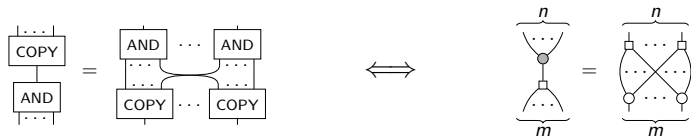
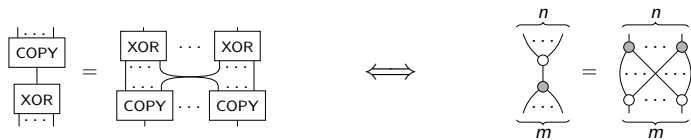
Boolean interpretation



Boolean rules #1

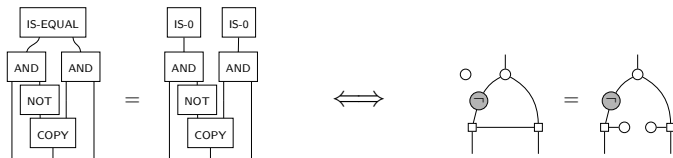


Boolean rules #2



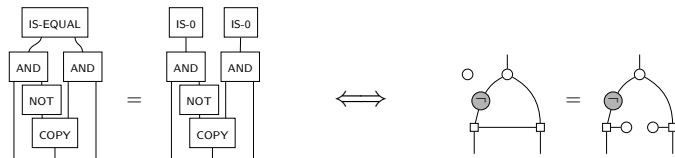
The final rule

Need one more rule:

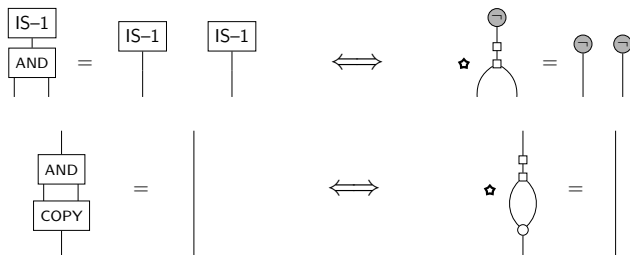


The final rule

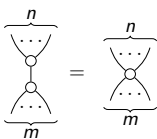
Need one more rule:



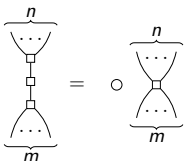
Or equivalently, a pair of rules:



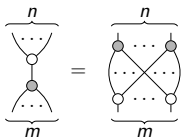
The rules

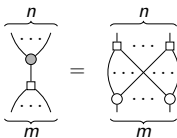
(zs) 

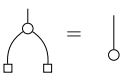
(id) 

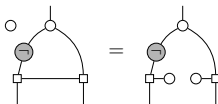
(hs) 

(hh) 

(ba₁) 

(ba₂) 

(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.

Need a couple of ingredients:

- ▶ Labelled H-boxes
- ▶ Annotated !-boxes
- ▶ The normal form
- ▶ Arithmetic

Labelled H-boxes

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

$$\boxed{-1} := \square, \quad \boxed{0} := \bullet, \quad \boxed{1} := \circ$$

Labelled H-boxes

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

$$\boxed{-1} := \square, \quad \boxed{0} := \bullet, \quad \boxed{1} := \circ$$

Extend to higher arity:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \boxed{a} \end{array} := \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \square \\ \square \\ \boxed{a} \end{array} \star$$

Labelled H-boxes

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

$$\boxed{-1} := \square, \quad \boxed{0} := \bullet, \quad \boxed{1} := \circ$$

Extend to higher arity:

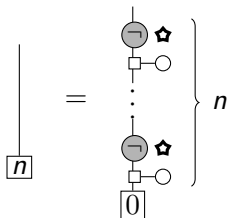
$$\begin{array}{c} \dots \\ \diagdown \quad \diagup \\ \square \\ a \end{array} := \begin{array}{c} \dots \\ \diagdown \quad \diagup \\ \square \\ \star \\ \square \\ a \end{array}$$

Can build higher numbers:

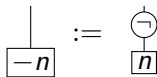
$$\boxed{a+1} := \begin{array}{c} | \\ \ominus \\ \boxed{0} \\ \square \\ a \end{array} = \begin{array}{c} | \\ \ominus \\ \star \\ \square \\ \circ \\ \square \\ a \end{array} = \begin{array}{c} | \\ \triangle \\ \square \\ a \end{array}$$

Integers

Natural numbers:

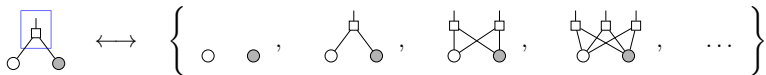


Negation:



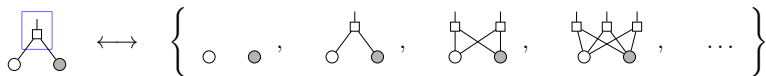
!-boxes

Standard !-boxes:

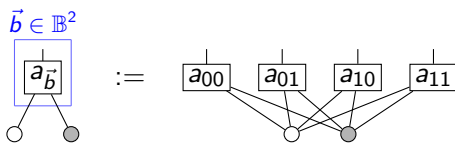


!-boxes

Standard !-boxes:

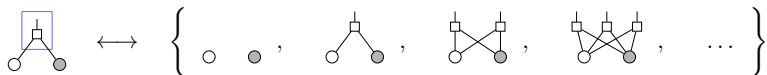


Annotated !-boxes:

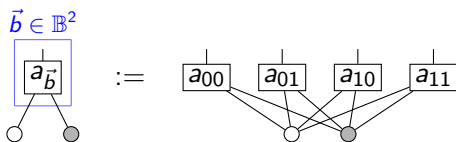


!-boxes

Standard !-boxes:



Annotated !-boxes:

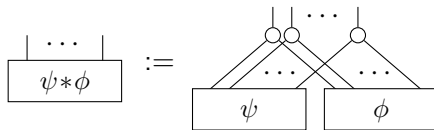


A useful additional definition:

$$\boxed{\vec{b}} := \left(\text{circle with } \neg \right)^{1-b_1} \dots \left(\text{circle with } \neg \right)^{1-b_n} .$$

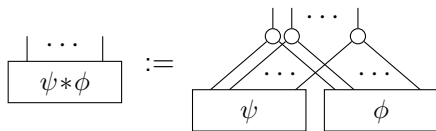
Normal form

Schur product:

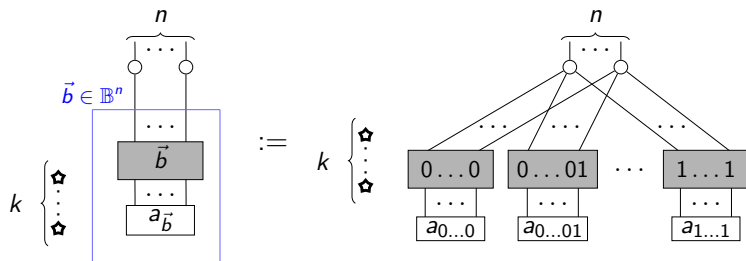


Normal form

Schur product:



Normal form:



We say it is **reduced** when k is minimal

How to reduce to normal form

- ▶ Show each generator can be reduced to normal form
- ▶ Show tensor products of nforms can be reduced to nform
- ▶ Show that any wirings between nforms are reducible

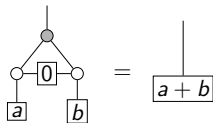
How to reduce to normal form

- ▶ Show each generator can be reduced to normal form
- ▶ Show tensor products of nforms can be reduced to nform
- ▶ Show that any wirings between nforms are reducible

To do this we need to be able to do **arithmetic** on H-box labels

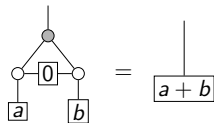
Arithmetic

Addition:

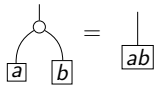


Arithmetic

Addition:

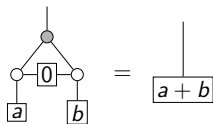


Multiplication:

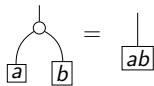


Arithmetic

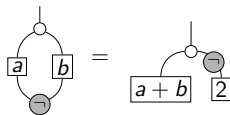
Addition:



Multiplication:

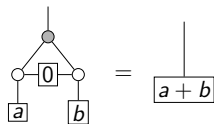


Average:

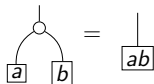


Arithmetic

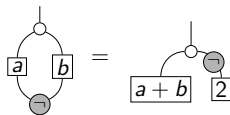
Addition:



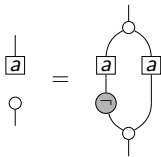
Multiplication:



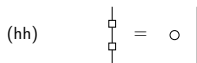
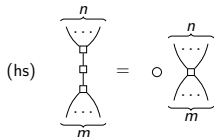
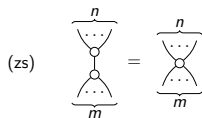
Average:



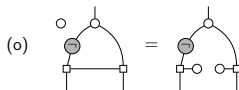
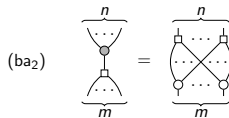
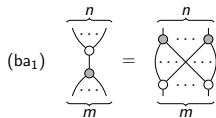
Introduction:



Summary



These 8 rules



are complete and universal for matrices over $\mathbb{Z}[\frac{1}{2}]$.

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

$$\left[\left[\begin{array}{c} \overbrace{}^n \\ \vdots \\ \boxed{r} \\ \vdots \\ \underbrace{}_m \end{array} \right] \right] := \sum r^{i_1 \dots i_m j_1 \dots j_n} |j_1 \dots j_n\rangle \langle i_1 \dots i_m|.$$

ZH over arbitrary rings

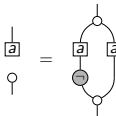
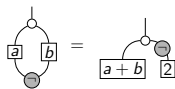
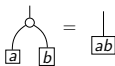
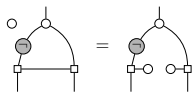
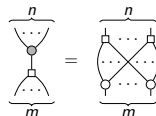
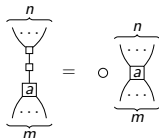
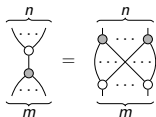
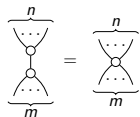
Let's promote labelled H-boxes to actual generators.

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

$$\left[\left[\begin{array}{c} \overbrace{\quad}^n \\ \vdots \\ \boxed{r} \\ \vdots \\ \underbrace{\quad}_m \end{array} \right] \right] := \sum r^{i_1 \dots i_m j_1 \dots j_n} |j_1 \dots j_n\rangle \langle i_1 \dots i_m|.$$

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

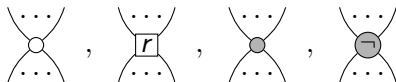
Let R be a commutative ring where 2 has an inverse.
Then this rule set is complete for matrices over R .

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

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

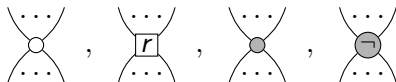
For general rings

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



For general rings

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

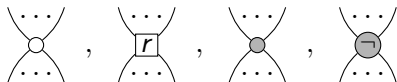


New rules:



For general rings

Don't have a \star . 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

Announcement: Quantum Pubquiz

- ▶ What: A quantum Pubquiz!
- ▶ When: Thursday 20:30CEST
- ▶ Where: Gathertown pub

No need to register, just show up :)