Towards Large-scale Functional Verification of Universal Quantum Circuits, Or: Verifying a Quantum Computing Textbook

Matthew Amy

University of Waterloo & Institute for Quantum Computing

Quantum Physics and Logic
June 6th, 2018

Outline

Motivation

The path-sum model

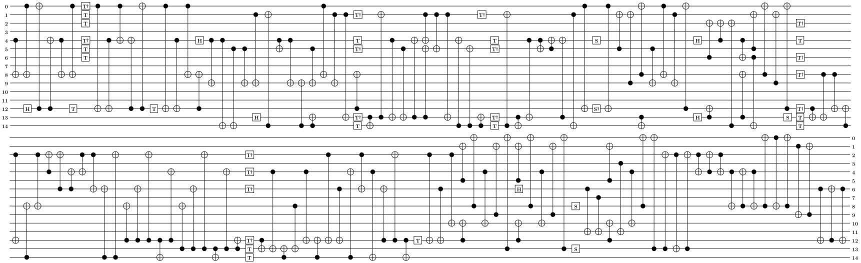
A calculus for path-sums

Completeness

Experimental results

Goal

Automatically verify this:



Against this:

$$|\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{0}\rangle \mapsto |\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{x}+\mathbf{y}\rangle$$

Motivation, Pt I

Specification

How should the functionality be specified?

Motivation, Pt I

Specification

How should the functionality be specified?

- Matrix?

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Motivation, Pt I

Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Motivation, Pt I

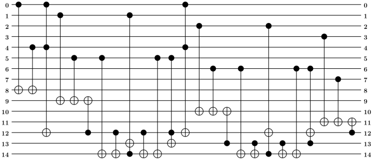
Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Higher-level circuit?



Motivation, Pt I

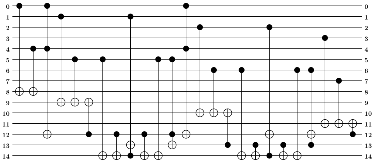
Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Higher-level circuit? Still pretty illegible, no “meta-information” i.e. which bits contain the result



Motivation, Pt I

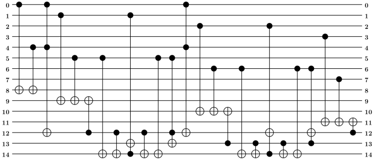
Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Higher-level circuit? Still pretty illegible, no “meta-information” i.e. which bits contain the result



- Matrix/circuit generating program?

Motivation, Pt I

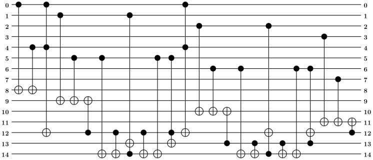
Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Higher-level circuit? Still pretty illegible, no “meta-information” i.e. which bits contain the result



- Matrix/circuit generating program? Probably circuit-like, just another thing to verify

Motivation, Pt I

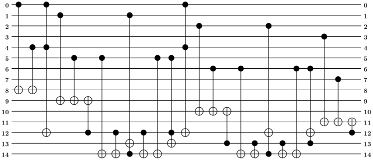
Specification

How should the functionality be specified?

- Matrix? Exponential space, illegible

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

- Higher-level circuit? Still pretty illegible, no “meta-information” i.e. which bits contain the result



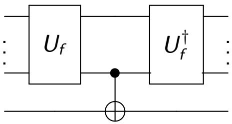
- Matrix/circuit generating program? Probably circuit-like, just another thing to verify

Bottom line: $|\mathbf{x}\rangle|\mathbf{x}\rangle|\mathbf{0}\rangle \mapsto |\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{x}+\mathbf{y}\rangle$ concisely captures the intuition

Motivation, Pt II

Target circuits

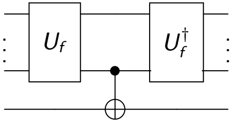
Theory:



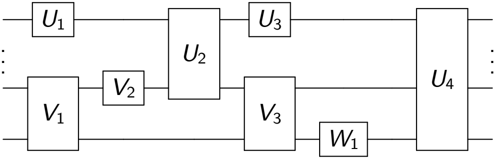
Motivation, Pt II

Target circuits

Theory:



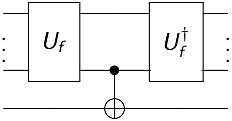
Reality:



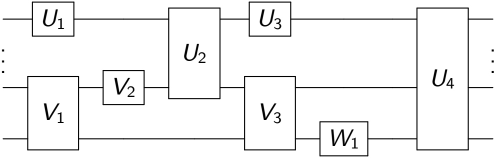
Motivation, Pt II

Target circuits

Theory:



Reality:



Optimizations are really hard to formally prove correct

Path-sums

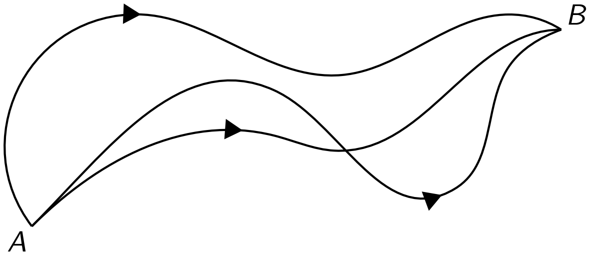
- Natural to write specifications for quantum algorithms
- Poly-time computable for fixed levels of the Clifford hierarchy
- Admits a natural notion of reduction

Path-sums

- Natural to write specifications for quantum algorithms
- Poly-time computable for fixed levels of the Clifford hierarchy
- Admits a natural notion of reduction
- Only computational paths matter!

The Feynman path integral

Amplitude of a quantum state is a sum over all paths leading to it



Path-sums

phase polynomials on steroids

$$H : \quad |x\rangle \quad \mapsto \frac{1}{\sqrt{2}} \textstyle\sum_{y \in \mathbb{Z}_2} \quad e^{2\pi i \frac{xy}{2}} \quad |y\rangle$$

---

[0] [Dawson et. al., 2004]

Path-sums

phase polynomials on steroids

$$H : \quad |x\rangle \quad \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} \quad e^{2\pi i \frac{xy}{2}} \quad |y\rangle$$

Definition (path-sum)

An n-qubit path-sum ξ consists of

---

[0] [Dawson et. al., 2004]

Path-sums

phase polynomials on steroids

$$H : \underset{\substack{\uparrow \\ 1.}}{|x\rangle} \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} e^{2\pi i \frac{xy}{2}} |y\rangle$$

Definition (path-sum)

An n-qubit path-sum ξ consists of

1. an input signature of n variables or Boolean constants

---

[0] [Dawson et. al., 2004]

Path-sums

phase polynomials on steroids

$$H : \underset{\substack{\uparrow \\ 1.}}{|x\rangle} \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} \underset{\substack{\uparrow \\ 2.}}{e^{2\pi i \frac{xy}{2}}} |y\rangle$$

Definition (path-sum)

An n-qubit path-sum ξ consists of

1. an input signature of n variables or Boolean constants
2. a multilinear phase polynomial over input (x_i) and path (y_i) variables with coefficients of the form $\frac{a}{2^b}$

---

[0] [Dawson et. al., 2004]

Path-sums

phase polynomials on steroids

$$H : \underset{\substack{\uparrow \\ 1.}}{|x\rangle} \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} \underset{\substack{\uparrow \\ 2.}}{e^{2\pi i \frac{xy}{2}}} \underset{\substack{\uparrow \\ 3.}}{|y\rangle}$$

Definition (path-sum)

An n-qubit path-sum ξ consists of

1. an input signature of n variables or Boolean constants
2. a multilinear phase polynomial over input (x_i) and path (y_i) variables with coefficients of the form $\frac{a}{2^b}$
3. an output signature of n Boolean polynomials over x_i and y_i

---

[0] [Dawson et. al., 2004]

Path-sums

phase polynomials on steroids

$$H: \underset{\underset{1.}{\uparrow}}{|x\rangle} \mapsto \frac{1}{\sqrt{2}} \sum_{y\in\mathbb{Z}_2} \underset{\underset{2.}{\uparrow}}{e^{2\pi i \frac{xy}{2}}} \underset{\underset{3.}{\uparrow}}{|y\rangle}$$

Definition (path-sum)

An n-qubit path-sum ξ consists of

1. an input signature of n variables or Boolean constants
2. a multilinear phase polynomial over input (x_i) and path (y_i) variables with coefficients of the form $\frac{a}{2^b}$
3. an output signature of n Boolean polynomials over x_i and y_i

Note: *well-formed* $=$ *partial isometry*

---

[0] [Dawson et. al., 2004]

Examples

$$T : |x\rangle \mapsto e^{2\pi i \frac{x}{8}} |x\rangle$$

$$H : |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} e^{2\pi i \frac{xy}{2}} |y\rangle$$

$$\text{Toffoli}_n : |x_1 x_2 \cdots x_n\rangle \mapsto |x_1 x_2 \cdots (x_n \oplus \prod_{i=1}^{n-1} x_i)\rangle$$

$$\text{Adder}_n : |\mathbf{x}\rangle |\mathbf{y}\rangle |\mathbf{0}\rangle \mapsto |\mathbf{x}\rangle |\mathbf{y}\rangle |\mathbf{x} + \mathbf{y}\rangle$$

$$\text{QFT}_n : |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{Z}_2^n} e^{2\pi i \frac{[\mathbf{x} \cdot \mathbf{y}]}{2^n}} |\mathbf{y}\rangle$$

Examples

$$T : |x\rangle \mapsto e^{2\pi i \frac{x}{8}} |x\rangle$$

$$H : |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} e^{2\pi i \frac{xy}{2}} |y\rangle$$

$$\text{Toffoli}_n : |x_1 x_2 \cdots x_n\rangle \mapsto |x_1 x_2 \cdots (x_n \oplus \prod_{i=1}^{n-1} x_i)\rangle$$

$$\text{Adder}_n : |\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{0}\rangle \mapsto |\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{x} + \mathbf{y}\rangle$$

$$\text{QFT}_n : |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y} \in \mathbb{Z}_2^n} e^{2\pi i \frac{[\mathbf{x} \cdot \mathbf{y}]}{2^n}} |\mathbf{y}\rangle$$

Composing path sums

$$\xi = |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})} |f(\mathbf{x},\mathbf{y})\rangle$$

$$\xi' = |\mathbf{x}'\rangle \mapsto \frac{1}{\sqrt{2^{m'}}} \sum_{\mathbf{y}'\in\mathbb{Z}_2^{m'}} e^{2\pi i P'(\mathbf{x}',\mathbf{y}')} |f'(\mathbf{x}',\mathbf{y}')\rangle$$

Tensor:

$$\xi \otimes \xi' = |\mathbf{x}\rangle|\mathbf{x}'\rangle \mapsto \frac{1}{\sqrt{2^{m+m'}}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{y}'\in\mathbb{Z}_2^{m'}} e^{2\pi i \left(P(\mathbf{x}\,\mathbf{y})+P'(\mathbf{x}',\mathbf{y}')\right)} |f(\mathbf{x},\mathbf{y})\rangle|f'(\mathbf{x}',\mathbf{y}')\rangle$$

Functional:

$$\xi' \circ \xi = ???$$

Functional composition

$$|x_1'x_2'x_3'\rangle \mapsto |x_1'x_2'(x_2' \oplus x_3')\rangle \circ |x_1x_2x_3\rangle \mapsto |x_1(x_1 \oplus x_2)x_3\rangle$$

Functional composition

$$\begin{aligned}|x_1'x_2'x_3'\rangle \mapsto |x_1'x_2'(x_2' \oplus x_3')\rangle \circ |x_1x_2x_3\rangle \mapsto |x_1(x_1 \oplus x_2)x_3\rangle \\ = |x_1x_2x_3\rangle \mapsto |x_1'x_2'(x_2' \oplus x_3')\rangle[x_1' \leftarrow x_1, x_2' \leftarrow x_1 \oplus x_2, x_3' \leftarrow x_3]\end{aligned}$$

Functional composition

$$\begin{aligned}
|x_1'x_2'x_3'\rangle \mapsto |x_1'x_2'(x_2' \oplus x_3')\rangle \circ |x_1x_2x_3\rangle \mapsto |x_1(x_1 \oplus x_2)x_3\rangle \\
= |x_1x_2x_3\rangle \mapsto |x_1'x_2'(x_2' \oplus x_3')\rangle[x_1' \leftarrow x_1, x_2' \leftarrow x_1 \oplus x_2, x_3' \leftarrow x_3] \\
= |x_1x_2x_3\rangle \mapsto |x_1(x_1 \oplus x_2)(x_1 \oplus x_2 \oplus x_3)\rangle
\end{aligned}$$

Functional composition

Composing isometries

What about the following composition?

$$|0\rangle \mapsto |0\rangle \circ |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} e^{\pi i x y} |y\rangle$$

Functional composition

Composing isometries

What about the following composition?

$$|0\rangle \mapsto |0\rangle \circ |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} e^{\pi i x y} |y\rangle$$

An output signature is $|f(\mathbf{x}, \mathbf{y})\rangle$ compatible with an input signature $|\mathbf{x}'\rangle$ if and only if whenever $x'_i = 0$ or 1, $f_i(\mathbf{x}, \mathbf{y}) = x'_i$

> *E.g.* $|1\rangle$ *is compatible with* $|x\rangle$ *while* $|x\rangle$ *is not compatible with* $|1\rangle$

Functional composition

Substitutions inside phase polynomials

$$|x\rangle \mapsto e^{2\pi i \frac{x}{4}}|x\rangle \circ |x\rangle \mapsto |1 \oplus x\rangle$$

Need to lift the Boolean polynomial $1 \oplus x$ to a functionally equivalent polynomial $\overline{1 \oplus x}$ over dyadic fractions

Functional composition

Substitutions inside phase polynomials

$$|x\rangle \mapsto e^{2\pi i \frac{x}{4}}|x\rangle \circ |x\rangle \mapsto |1 \oplus x\rangle$$

Need to lift the Boolean polynomial $1 \oplus x$ to a functionally equivalent polynomial $\overline{1 \oplus x}$ over dyadic fractions

$$\begin{aligned}\overline{\mathbf{x}^{\alpha}} &= \mathbf{x}^{\alpha}, \\ \overline{P + Q} &= \overline{P} + \overline{Q} - 2\overline{PQ},\end{aligned}$$

Proposition

For any Boolean-valued polynomial P and all $\mathbf{x} \in \mathbb{Z}_2^n$, $\overline{P}(\mathbf{x}) = P(\mathbf{x})$ mod 2*.*

Composing path sums

$$\xi = |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})} |f(\mathbf{x},\mathbf{y})\rangle$$

$$\xi' = |\mathbf{x}'\rangle \mapsto \frac{1}{\sqrt{2^{m'}}} \sum_{\mathbf{y}'\in\mathbb{Z}_2^{m'}} e^{2\pi i P'(\mathbf{x}',\mathbf{y}')} |f'(\mathbf{x}',\mathbf{y}')\rangle$$

Tensor:

$$\xi \otimes \xi' = |\mathbf{x}\rangle|\mathbf{x}'\rangle \mapsto \frac{1}{\sqrt{2^{m+m'}}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m, \mathbf{y}'\in\mathbb{Z}_2^{m'}} e^{2\pi i \left(P(\mathbf{x}\,\mathbf{y}) + P'(\mathbf{x}',\mathbf{y}')\right)} |f(\mathbf{x},\mathbf{y})\rangle|f'(\mathbf{x}',\mathbf{y}')\rangle$$

Functional:

$$\xi' \circ \xi = |\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^{m+m'}}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m, \mathbf{y}'\in\mathbb{Z}_2^{m'}} e^{2\pi i \left(P + P'[x_i' \leftarrow \overline{f_i}]\right)(\mathbf{x},\mathbf{y},\mathbf{y}')} | \left(f'[x_i' \leftarrow f_i]\right)(\mathbf{x},\mathbf{y},\mathbf{y}')\rangle$$

The path-sum model

Path-sum semantics for Clifford+R_k circuits:

$$\begin{aligned}
[\![H]\!] &= |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}} e^{2\pi i \frac{xy}{2}} |y\rangle \\
[\![R_k]\!] &= |x\rangle \mapsto e^{2\pi i \frac{x}{2^k}} |x\rangle \\
[\![R_k^\dagger]\!] &= |x\rangle \mapsto e^{2\pi i \frac{-x}{2^k}} |x\rangle \\
[\![\mathrm{CNOT}]\!] &= |x_1 x_2\rangle \mapsto |x_1 (x_1 \oplus x_2)\rangle \\
[\![C_1; C_2]\!] &= [\![C_2]\!] \circ [\![C_1]\!].
\end{aligned}$$

The path-sum model

Path-sum semantics for Clifford+R_k circuits:

$$
\begin{aligned}
\llbracket H \rrbracket &= |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}} e^{2\pi i \frac{xy}{2}} |y\rangle \\
\llbracket R_k \rrbracket &= |x\rangle \mapsto e^{2\pi i \frac{x}{2^k}} |x\rangle \\
\llbracket R_k^\dagger \rrbracket &= |x\rangle \mapsto e^{2\pi i \frac{-x}{2^k}} |x\rangle \\
\llbracket \mathrm{CNOT} \rrbracket &= |x_1 x_2\rangle \mapsto |x_1 (x_1 \oplus x_2)\rangle \\
\llbracket C_1; C_2 \rrbracket &= \llbracket C_2 \rrbracket \circ \llbracket C_1 \rrbracket.
\end{aligned}
$$

Proposition

The path-sum of an n-qubit Clifford+R_k circuit C for fixed k has size polynomial in the volume of C and can be computed in polynomial time.

Digression: only computational paths matter

The path-sum model normalizes[1] most structural equivalences, as well as some semantic equivalences.

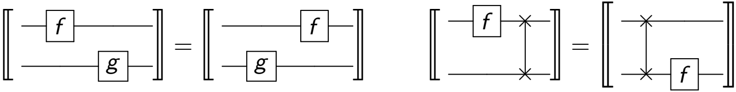
---

[1] Caveat: up to variable renaming

Digression: only computational paths matter

The path-sum model normalizes[1] most structural equivalences, as well as some semantic equivalences.

Structural equivalences:



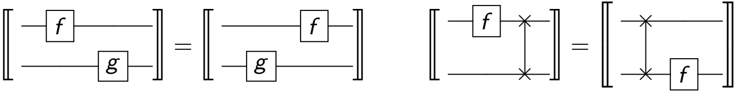
---

[1] Caveat: up to variable renaming

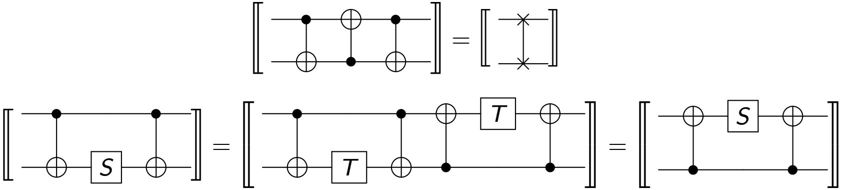
Digression: only computational paths matter

The path-sum model normalizes[1] most structural equivalences, as well as some semantic equivalences.

Structural equivalences:



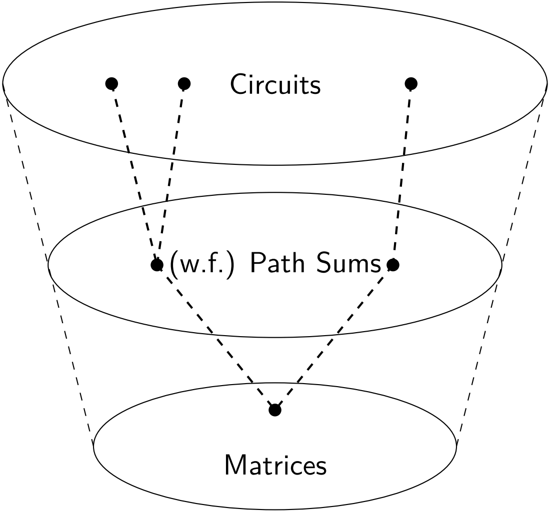
Semantic equivalences:



---

[1] Caveat: up to variable renaming

Path-sums as an intermediary model



Motivation

The path-sum model

A calculus for path-sums

Completeness

Experimental results

Reducing path-sums

- Path-sums are an un-evaluated representation of the branching computational paths in a circuit
- Lose any computational advantage if we just expand all paths
- Instead, find groups of paths which interfere in recognizable ways

Reducing path-sums

- Path-sums are an un-evaluated representation of the branching computational paths in a circuit
- Lose any computational advantage if we just expand all paths
- Instead, find groups of paths which interfere in recognizable ways

reduction $\equiv$ *path variable elimination*

Example

$HH = I$

$$HH : |x\rangle \mapsto \frac{1}{2} \sum_{y_1, y_2 \in \mathbb{Z}_2} e^{2\pi i \frac{xy_1 + y_1 y_2}{2}} |y_2\rangle$$

Example

$HH = I$

$$\frac{1}{2} \sum_{y_1, y_2 \in \mathbb{Z}_2} e^{2\pi i \frac{x y_1 + y_1 y_2}{2}} \left| y_2 \right\rangle$$

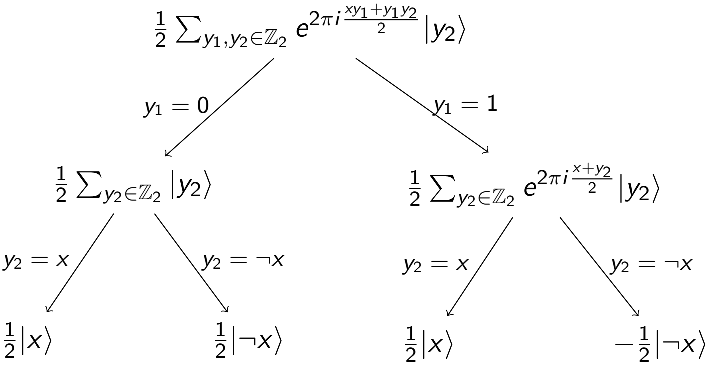
Example

$HH = I$

$$\begin{tikzcd}
 & \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{xy_1+y_1y_2}{2}}\left|y_2\right\rangle \arrow[dl, "y_1=0"'] \arrow[dr, "y_1=1"] & \\
\frac{1}{2}\sum_{y_2\in\mathbb{Z}_2}\left|y_2\right\rangle & & \frac{1}{2}\sum_{y_2\in\mathbb{Z}_2} e^{2\pi i\frac{x+y_2}{2}}\left|y_2\right\rangle
\end{tikzcd}$$

Example

$HH = I$



$$\frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{xy_1+y_1y_2}{2}}|y_2\rangle$$

$y_1 = 0$

$y_1 = 1$

$$\frac{1}{2}\sum_{y_2\in\mathbb{Z}_2}|y_2\rangle$$

$$\frac{1}{2}\sum_{y_2\in\mathbb{Z}_2} e^{2\pi i\frac{x+y_2}{2}}|y_2\rangle$$

$y_2 = x$

$y_2 = \neg x$

$y_2 = x$

$y_2 = \neg x$

$\frac{1}{2}|x\rangle$

$\frac{1}{2}|\neg x\rangle$

$\frac{1}{2}|x\rangle$

$-\frac{1}{2}|\neg x\rangle$

Example

$HH = I$

$$\begin{tikzcd}
 & & & \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{xy_1+y_1y_2}{2}}\left|y_2\right\rangle \arrow[dll, "y_1 = 0"'] \arrow[drr, "y_1 = 1"] & & & \\
 & \frac{1}{2}\sum_{y_2\in\mathbb{Z}_2}\left|y_2\right\rangle \arrow[dl, "y_2 = x"'] \arrow[dr, "y_2 = \neg x"] & & & & \frac{1}{2}\sum_{y_2\in\mathbb{Z}_2} e^{2\pi i\frac{x+y_2}{2}}\left|y_2\right\rangle \arrow[dl, "y_2 = x"'] \arrow[dr, "y_2 = \neg x"] & \\
\frac{1}{2}\left|x\right\rangle \arrow[drr] & & \frac{1}{2}\left|\neg x\right\rangle \arrow[drr] & & \frac{1}{2}\left|x\right\rangle \arrow[dll] & & -\frac{1}{2}\left|\neg x\right\rangle \arrow[dll] \\
 & & \frac{2}{2}\left|x\right\rangle & + & \frac{0}{2}\left|\neg x\right\rangle & &
\end{tikzcd}$$

Generalization

Whenever

$$P(\mathbf{x}, \mathbf{y}) = \frac{1}{2} y_0 (y_i + Q(\mathbf{x}, \mathbf{y})) + R(\mathbf{x}, \mathbf{y})$$

for an internal path variable y_0, $y_i \notin Q$ and Q Boolean,

- the paths defined by $y_i = Q(\mathbf{x}, \mathbf{y})$, $y_0 = 0$ and $y_0 = 1$ add, and
- the paths defined by $y_i = \neg Q(\mathbf{x}, \mathbf{y})$, $y_0 = 0$ and $y_0 = 1$ cancel

Generalization

Whenever

$$P(\mathbf{x},\mathbf{y}) = \frac{1}{2}y_0(y_i + Q(\mathbf{x},\mathbf{y})) + R(\mathbf{x},\mathbf{y})$$

for an internal path variable y_0, $y_i \notin Q$ and Q Boolean,

- the paths defined by $y_i = Q(\mathbf{x},\mathbf{y})$, $y_0 = 0$ and $y_0 = 1$ add, and
- the paths defined by $y_i = \neg Q(\mathbf{x},\mathbf{y})$, $y_0 = 0$ and $y_0 = 1$ cancel

Equationally,

$$\begin{aligned} &\tfrac{1}{\sqrt{2^{m+1}}} \textstyle\sum_{y_0\in\mathbb{Z}_2} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{2}y_0(y_i+Q(\mathbf{x},\mathbf{y}))+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \\ &= \tfrac{1}{\sqrt{2^{m+1}}} \textstyle\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(R[y_i\leftarrow\overline{Q}]\right)(\mathbf{x},\mathbf{y})}|\left(f[y_i \leftarrow Q]\right)(\mathbf{x},\mathbf{y})\rangle \end{aligned}$$

Rewrite rules

$$\frac{1}{\sqrt{2^{m+2}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \qquad \text{[Elim]}$$

$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{4}y_0+\frac{1}{2}y_0 Q(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{y\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{8}-\frac{1}{4}\overline{Q}(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \qquad [\omega]$$

$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{2}y_0(y_i+Q(\mathbf{x},\mathbf{y}))+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^{m+1}}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(R[y_i\leftarrow\overline{Q}]\right)(\mathbf{x},\mathbf{y})}|\,(f[y_i\leftarrow Q])\,(\mathbf{x},\mathbf{y})\rangle \qquad \text{[HH]}$$

$$\frac{P(\mathbf{x},\mathbf{y}) = \frac{1}{4}y_i x + \frac{1}{2}y_i(y_j + Q(\mathbf{x},\mathbf{y})) + R(\mathbf{x},\mathbf{y}) = \frac{1}{4}y_j(1-x) + \frac{1}{2}y_j(y_i + Q'(\mathbf{x},\mathbf{y})) + R'(\mathbf{x},\mathbf{y})}{\frac{1}{\sqrt{2^{m+2}}}\sum_{\mathbf{y}\in\mathbb{Z}_2^{m+2}} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left((1-x)R[y_j\leftarrow\overline{Q}]+xR'[y_i\leftarrow\overline{Q'}]\right)(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle} \qquad \text{[Case]}$$

Rewrite rules

$$\frac{1}{\sqrt{2^{m+2}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \qquad \text{[Elim]}$$

$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{4}y_0+\frac{1}{2}y_0 Q(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{y\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{8}-\frac{1}{4}\overline{Q}(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \qquad [\omega]$$

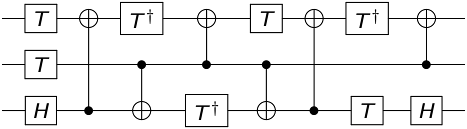
$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{2}y_0(y_i+Q(\mathbf{x},\mathbf{y}))+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^{m+1}}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(R[y_i\leftarrow\overline{Q}]\right)(\mathbf{x},\mathbf{y})}|\left(f[y_i\leftarrow Q]\right)(\mathbf{x},\mathbf{y})\rangle \qquad \text{[HH]}$$

$$\frac{P(\mathbf{x},\mathbf{y}) = \frac{1}{4}y_i x + \frac{1}{2}y_i(y_j + Q(\mathbf{x},\mathbf{y})) + R(\mathbf{x},\mathbf{y}) = \frac{1}{4}y_j(1-x) + \frac{1}{2}y_j(y_i + Q'(\mathbf{x},\mathbf{y})) + R'(\mathbf{x},\mathbf{y})}{\frac{1}{\sqrt{2^{m+2}}}\sum_{\mathbf{y}\in\mathbb{Z}_2^{m+2}} e^{2\pi i P(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left((1-x)R[y_j\leftarrow\overline{Q}]+xR'[y_i\leftarrow\overline{Q'}]\right)(\mathbf{x},\mathbf{y})}|f(\mathbf{x},\mathbf{y})\rangle} \qquad \text{[Case]}$$

Key property: number of path variables are always reduced!

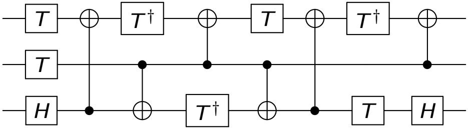
Example

Toffoli$_3$: $|x_1 x_2 x_3\rangle \mapsto |x_1 x_2 (x_3 \oplus x_1 x_2)\rangle$



Example

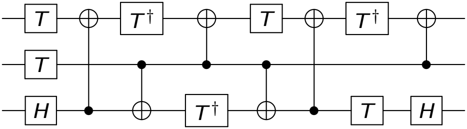
Toffoli$_3$: $|x_1x_2x_3\rangle \mapsto |x_1x_2(x_3 \oplus x_1x_2)\rangle$



$$|x_1x_2x_3\rangle \mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1x_2 y_1 + y_1 y_2)} |x_1x_2y_2\rangle$$

Example

Toffoli$_3$: $|x_1x_2x_3\rangle \mapsto |x_1x_2(x_3 \oplus x_1x_2)\rangle$

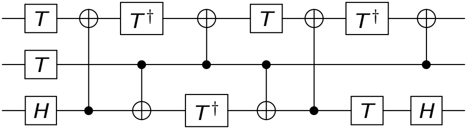


$$|x_1x_2x_3\rangle \mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1x_2 y_1 + y_1 y_2)} |x_1x_2y_2\rangle$$

$$\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2} y_1 (y_2 + x_3 + x_1x_2)} |x_1x_2y_2\rangle$$

Example

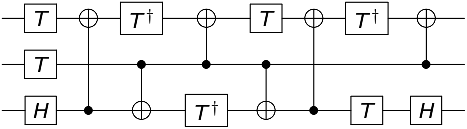
Toffoli$_3$: $|x_1x_2x_3\rangle \mapsto |x_1x_2(x_3 \oplus x_1x_2)\rangle$



$$
\begin{aligned}
|x_1x_2x_3\rangle &\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1x_2 y_1 + y_1 y_2)} |x_1x_2y_2\rangle \\
&\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2} y_1 (y_2 + x_3 + x_1x_2)} |x_1x_2y_2\rangle \\
&\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_2\in\mathbb{Z}_2} |x_1x_2(x_3 \oplus x_1x_2)\rangle \qquad [\mathrm{HH},\ y_2 \leftarrow x_3 \oplus x_1x_2]
\end{aligned}
$$

Example

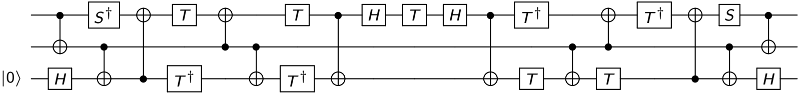
Toffoli$_3$: $|x_1x_2x_3\rangle \mapsto |x_1x_2(x_3 \oplus x_1x_2)\rangle$



$$\begin{aligned}
|x_1x_2x_3\rangle &\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3y_1+x_1x_2y_1+y_1y_2)}|x_1x_2y_2\rangle \\
&\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}y_1(y_2+x_3+x_1x_2)}|x_1x_2y_2\rangle \\
&\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_2\in\mathbb{Z}_2} |x_1x_2(x_3 \oplus x_1x_2)\rangle && [\text{HH, } y_2 \leftarrow x_3 \oplus x_1x_2] \\
&\mapsto |x_1x_2(x_3 \oplus x_1x_2)\rangle && [\text{Elim } y_2]
\end{aligned}$$

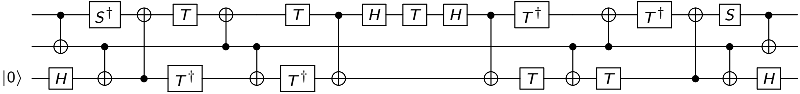
Example

Controlled-T : $|x_1 x_2\rangle \mapsto e^{2\pi i \frac{x_1 x_2}{8}} |x_1 x_2\rangle$



Example

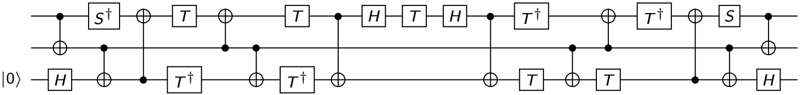
Controlled-T : $|x_1 x_2\rangle \mapsto e^{2\pi i \frac{x_1 x_2}{8}} |x_1 x_2\rangle$



$$|x_1 x_2\rangle|0\rangle \mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \frac{1}{8}(4x_1x_2y_1+4x_1y_2+4y_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)}|x_1 x_2 y_4\rangle$$

Example

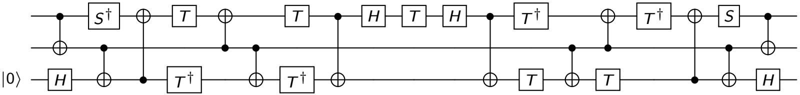
Controlled-T : $|x_1x_2\rangle \mapsto e^{2\pi i \frac{x_1x_2}{8}} |x_1x_2\rangle$



$$
\begin{aligned}
|x_1x_2\rangle|0\rangle &\mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \frac{1}{8}(4x_1x_2y_1+4x_1y_2+4y_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)} |x_1x_2y_4\rangle \\
&\mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \left(\frac{1}{2}y_1(y_2+x_1x_2)+\frac{1}{8}(4x_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)\right)} |x_1x_2y_4\rangle
\end{aligned}
$$

Example

Controlled-T : $|x_1x_2\rangle \mapsto e^{2\pi i \frac{x_1x_2}{8}} |x_1x_2\rangle$



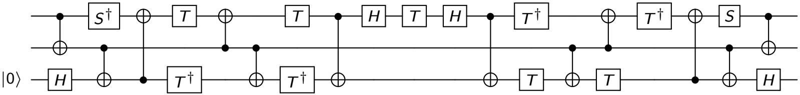
$$|x_1x_2\rangle|0\rangle \mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \frac{1}{8}(4x_1x_2y_1+4x_1y_2+4y_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)}|x_1x_2y_4\rangle$$

$$\mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i\left(\frac{1}{2}y_1(y_2+x_1x_2)+\frac{1}{8}(4x_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)\right)}|x_1x_2y_4\rangle$$

$$\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_3,y_4\in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4x_1x_2+x_1x_2+4x_1x_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)}|x_1x_2y_4\rangle \quad \text{[HH, Elim]}$$

Example

Controlled-T : $|x_1x_2\rangle \mapsto e^{2\pi i \frac{x_1x_2}{8}}|x_1x_2\rangle$



$$|x_1x_2\rangle|0\rangle \mapsto \frac{1}{\sqrt{2^4}}\sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \frac{1}{8}(4x_1x_2{\color{red}y_1}+4x_1y_2+4{\color{red}y_1}y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)}|x_1x_2y_4\rangle$$

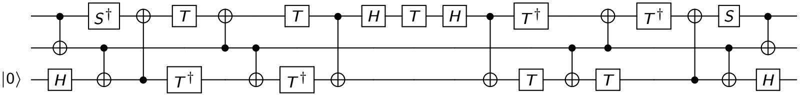
$$\mapsto \frac{1}{\sqrt{2^4}}\sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i\left(\frac{1}{2}{\color{red}y_1}(y_2+x_1x_2)+\frac{1}{8}(4x_1y_2+y_2+4y_2y_3+4x_1x_2y_3+4x_1y_4+4y_3y_4+4x_1x_2)\right)}|x_1x_2y_4\rangle$$

$$\mapsto \frac{1}{\sqrt{2^2}}\sum_{y_3,y_4\in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4x_1x_2+x_1x_2+4x_1x_2{\color{red}y_3}+4x_1x_2{\color{red}y_3}+4x_1y_4+4{\color{red}y_3}y_4+4x_1x_2)}|x_1x_2y_4\rangle \quad \text{[HH, Elim]}$$

$$\mapsto \frac{1}{\sqrt{2^2}}\sum_{y_3,y_4\in\mathbb{Z}_2} e^{2\pi i\left(\frac{1}{2}{\color{red}y_3}y_4+\frac{1}{8}(x_1y_4+x_1x_2)\right)}|x_1x_2y_4\rangle$$

Example

Controlled-T : $|x_1 x_2\rangle \mapsto e^{2\pi i \frac{x_1 x_2}{8}} |x_1 x_2\rangle$



$$|x_1 x_2\rangle|0\rangle \mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \frac{1}{8}(4x_1x_2y_1 + 4x_1y_2 + 4y_1y_2 + y_2 + 4y_2y_3 + 4x_1x_2y_3 + 4x_1y_4 + 4y_3y_4 + 4x_1x_2)} |x_1 x_2 y_4\rangle$$

$$\mapsto \frac{1}{\sqrt{2^4}} \sum_{\mathbf{y}\in\mathbb{Z}_2^4} e^{2\pi i \left(\frac{1}{2}y_1(y_2 + x_1x_2) + \frac{1}{8}(4x_1y_2 + y_2 + 4y_2y_3 + 4x_1x_2y_3 + 4x_1y_4 + 4y_3y_4 + 4x_1x_2)\right)} |x_1 x_2 y_4\rangle$$

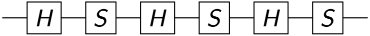
$$\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_3, y_4 \in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4x_1x_2 + x_1x_2 + 4x_1x_2y_3 + 4x_1x_2y_3 + 4x_1y_4 + 4y_3y_4 + 4x_1x_2)} |x_1 x_2 y_4\rangle \quad \text{[HH, Elim]}$$

$$\mapsto \frac{1}{\sqrt{2^2}} \sum_{y_3, y_4 \in\mathbb{Z}_2} e^{2\pi i \left(\frac{1}{2}y_3y_4 + \frac{1}{8}(x_1y_4 + x_1x_2)\right)} |x_1 x_2 y_4\rangle$$

$$\mapsto e^{2\pi i \frac{x_1 x_2}{8}} |x_1 x_2\rangle|0\rangle \qquad \text{[HH, Elim]}$$

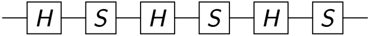
Example

$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



Example

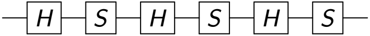
$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$(\mathrm{SH})^3 : |x\rangle \mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1,y_2,y_3\in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4xy_1+2y_1+4y_1y_2+2y_2+4y_2y_3+2y_3)}|y_3\rangle$$

Example

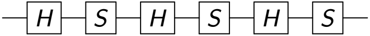
$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$
\begin{aligned}
(\mathrm{SH})^3 : |x\rangle &\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4x y_1 + 2y_1 + 4y_1 y_2 + 2y_2 + 4y_2 y_3 + 2y_3)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{4} y_1 + \frac{1}{2} y_1 (y_2 + x) + \frac{1}{8}(2y_2 + 4y_2 y_3 + 2y_3) \right)} |y_3\rangle
\end{aligned}
$$

Example

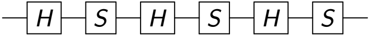
$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$\begin{aligned}
(\mathrm{SH})^3 : |x\rangle &\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1,y_2,y_3\in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4xy_1+2y_1+4y_1y_2+2y_2+4y_2y_3+2y_3)}|y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1,y_2,y_3\in\mathbb{Z}_2} e^{2\pi i\left(\frac{1}{4}y_1+\frac{1}{2}y_1(y_2+x)+\frac{1}{8}(2y_2+4y_2y_3+2y_3)\right)}|y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2,y_3\in\mathbb{Z}_2} e^{2\pi i \frac{1}{8}(1-2(y_2+x-2y_2x)+2y_2+4y_2y_3+2y_3)}|y_3\rangle \qquad [\omega]
\end{aligned}$$

Example

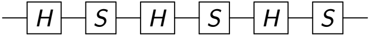
$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$
\begin{aligned}
(\mathrm{SH})^3 : |x\rangle &\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4xy_1 + 2y_1 + 4y_1y_2 + 2y_2 + 4y_2y_3 + 2y_3)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{4} y_1 + \frac{1}{2} y_1 (y_2 + x) + \frac{1}{8} (2y_2 + 4y_2y_3 + 2y_3) \right)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(1 - 2(y_2 + x - 2y_2x) + 2y_2 + 4y_2y_3 + 2y_3)} |y_3\rangle \qquad [\omega] \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{2} y_2 (x + y_3) + \frac{1}{8} (1 - 2x + 2y_3) \right)} |y_3\rangle
\end{aligned}
$$

Example

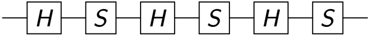
$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$\begin{aligned}
(\mathrm{SH})^3 : |x\rangle &\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1,y_2,y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4xy_1+2y_1+4y_1y_2+2y_2+4y_2y_3+2y_3)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1,y_2,y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{4}y_1+\frac{1}{2}y_1(y_2+x)+\frac{1}{8}(2y_2+4y_2y_3+2y_3)\right)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2,y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(1-2(y_2+x-2y_2x)+2y_2+4y_2y_3+2y_3)} |y_3\rangle \qquad [\omega] \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2,y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{2}y_2(x+y_3)+\frac{1}{8}(1-2x+2y_3)\right)} |y_3\rangle \\
&\mapsto e^{2\pi i \frac{1}{8}(1-2x+2x)} |x\rangle \qquad [\text{HH, Elim}]
\end{aligned}$$

Example

$(\mathrm{SH})^3 : |x\rangle \mapsto \omega|x\rangle$



$$\begin{aligned}
(\mathrm{SH})^3 : |x\rangle &\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(4xy_1 + 2y_1 + 4y_1y_2 + 2y_2 + 4y_2y_3 + 2y_3)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^3} \sum_{y_1, y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{4}y_1 + \frac{1}{2}y_1(y_2 + x) + \frac{1}{8}(2y_2 + 4y_2y_3 + 2y_3)\right)} |y_3\rangle \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{8}(1 - 2(y_2 + x - 2y_2x) + 2y_2 + 4y_2y_3 + 2y_3)} |y_3\rangle \qquad [\omega] \\
&\mapsto \frac{1}{\sqrt{2}^2} \sum_{y_2, y_3 \in \mathbb{Z}_2} e^{2\pi i \left(\frac{1}{2}y_2(x + y_3) + \frac{1}{8}(1 - 2x + 2y_3)\right)} |y_3\rangle \\
&\mapsto e^{2\pi i \frac{1}{8}(1 - 2x + 2x)} |x\rangle \qquad [\mathrm{HH,\ Elim}] \\
&\mapsto \omega |x\rangle.
\end{aligned}$$

Motivation

The path-sum model

A calculus for path-sums

Completeness

Experimental results

Completeness

Linear number of steps to reach an irreducible form

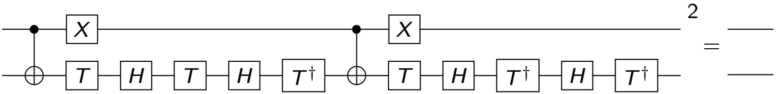
$\Longrightarrow$ *incomplete in general, in the sense that normal forms are not unique*

Completeness

Linear number of steps to reach an irreducible form

$\Longrightarrow$ *incomplete in general, in the sense that normal forms are not unique*

E.g. [Selinger and Bian, 2016]



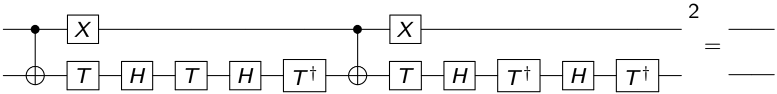
not provable with current set of rules

Completeness

Linear number of steps to reach an irreducible form

$\Longrightarrow$ *incomplete in general, in the sense that normal forms are not unique*

E.g. [Selinger and Bian, 2016]



not provable with current set of rules

However, complete for Clifford group with a little extra work

Output restriction

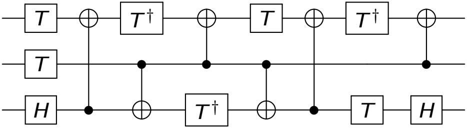
Observation:

If ξ is an isometry then $\xi \equiv |\mathbf{x}\rangle \mapsto |\mathbf{x}'\rangle$ if and only if

$$\frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\ s.t.\ f(\mathbf{x},\mathbf{y})=\mathbf{x}'} e^{2\pi i P(\mathbf{x},\mathbf{y})} = 1$$

Example

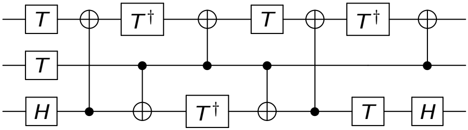
Toffoli redux



$$|x_1 x_2 x_3\rangle \mapsto \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1 x_2 y_1 + y_1 y_2)} |x_1 x_2 y_2\rangle$$

Example

Toffoli redux

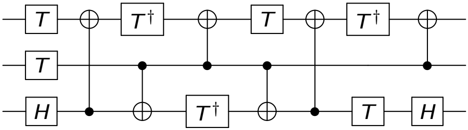


$$|x_1x_2x_3\rangle \mapsto \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{1}{2}(x_3y_1+x_1x_2y_1+y_1y_2)}|x_1x_2y_2\rangle$$

$$\mapsto \frac{1}{2}\sum_{\substack{y_1\in\mathbb{Z}_2,\\ y_2=x_3\oplus x_1x_2}} e^{2\pi i\frac{1}{2}\left(x_3y_1+x_1x_2y_1+y_1(\overline{x_3\oplus x_1x_2})\right)}|x_1x_2(x_3\oplus x_1x_2)\rangle$$

Example

Toffoli redux



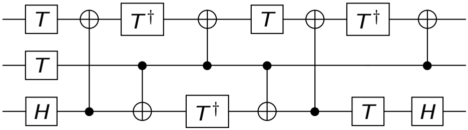
$$|x_1x_2x_3\rangle \mapsto \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{1}{2}(x_3y_1+x_1x_2y_1+y_1y_2)}|x_1x_2y_2\rangle$$

$$\mapsto \frac{1}{2}\sum_{\substack{y_1\in\mathbb{Z}_2,\\ \color{red}{y_2=x_3\oplus x_1x_2}}} e^{2\pi i\frac{1}{2}\left(x_3y_1+x_1x_2y_1+y_1(\overline{x_3\oplus x_1x_2})\right)}|x_1x_2(x_3\oplus x_1x_2)\rangle$$

$$\mapsto \frac{1}{2}\sum_{y_1\in\mathbb{Z}_2} e^{2\pi i\frac{1}{2}(x_3y_1+x_1x_2y_1+x_3y_1+x_1x_2y_1)}|x_1x_2(x_3\oplus x_1x_2)\rangle$$

Example

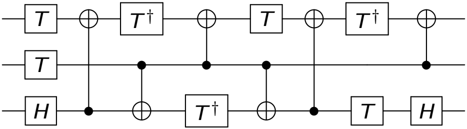
Toffoli redux



$$
\begin{aligned}
|x_1 x_2 x_3\rangle &\mapsto \frac{1}{2} \sum_{y_1, y_2 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1 x_2 y_1 + y_1 y_2)} |x_1 x_2 y_2\rangle \\
&\mapsto \frac{1}{2} \sum_{\substack{y_1 \in \mathbb{Z}_2, \\ y_2 = x_3 \oplus x_1 x_2}} e^{2\pi i \frac{1}{2}\left(x_3 y_1 + x_1 x_2 y_1 + y_1 (\overline{x_3 \oplus x_1 x_2})\right)} |x_1 x_2 (x_3 \oplus x_1 x_2)\rangle \\
&\mapsto \frac{1}{2} \sum_{y_1 \in \mathbb{Z}_2} e^{2\pi i \frac{1}{2}(x_3 y_1 + x_1 x_2 y_1 + x_3 y_1 + x_1 x_2 y_1)} |x_1 x_2 (x_3 \oplus x_1 x_2)\rangle \\
&\mapsto \frac{1}{2} \sum_{y_1 \in \mathbb{Z}_2} |x_1 x_2 (x_3 \oplus x_1 x_2)\rangle
\end{aligned}
$$

Example

Toffoli redux



$$\begin{aligned}
|x_1x_2x_3\rangle &\mapsto \frac{1}{2}\sum_{y_1,y_2\in\mathbb{Z}_2} e^{2\pi i\frac{1}{2}(x_3y_1+x_1x_2y_1+y_1y_2)}|x_1x_2y_2\rangle \\
&\mapsto \frac{1}{2}\sum_{\substack{y_1\in\mathbb{Z}_2,\\ \textcolor{red}{y_2=x_3\oplus x_1x_2}}} e^{2\pi i\frac{1}{2}\left(x_3y_1+x_1x_2y_1+y_1(\overline{x_3\oplus x_1x_2})\right)}|x_1x_2(x_3\oplus x_1x_2)\rangle \\
&\mapsto \frac{1}{2}\sum_{y_1\in\mathbb{Z}_2} e^{2\pi i\frac{1}{2}(x_3y_1+x_1x_2y_1+x_3y_1+x_1x_2y_1)}|x_1x_2(x_3\oplus x_1x_2)\rangle \\
&\mapsto \frac{1}{2}\sum_{y_1\in\mathbb{Z}_2} |x_1x_2(x_3\oplus x_1x_2)\rangle \\
&\mapsto |x_1x_2(x_3\oplus x_1x_2)\rangle \qquad \text{[Elim]}
\end{aligned}$$

Non-equivalence

Observation:

In the LHS of [HH],

$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{2}y_0 Q(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle$$

if Q contains only input variables, then there exists an input basis state $\mathbf{x}$ *such that* $Q(\mathbf{x},\mathbf{y}) = 1 \mod 2$ *for all* $\mathbf{y}$*, so*

$$\frac{1}{\sqrt{2^{m+1}}}\sum_{y_0\in\mathbb{Z}_2}\sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i\left(\frac{1}{2}y_0 Q(\mathbf{x},\mathbf{y})+R(\mathbf{x},\mathbf{y})\right)}|f(\mathbf{x},\mathbf{y})\rangle = 0$$

(Semi)-Completeness for Clifford group circuits

Theorem

Equivalence of Clifford group circuits can be checked in polynomial time.

Proof sketch

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})} |\mathbf{x}\rangle$$

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|\mathbf{x}\rangle$$

   - I.e. output restriction observation

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|\mathbf{x}\rangle$$

    - I.e. output restriction observation
    - Output polynomial is linear, can solve $f(\mathbf{x},\mathbf{y}) = \mathbf{x}$ for $\mathbf{y}$ if such a solution exists in poly-time w/ Gaussian elimination

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|\mathbf{x}\rangle$$

    - I.e. output restriction observation
    - Output polynomial is linear, can solve $f(\mathbf{x}, \mathbf{y}) = \mathbf{x}$ for $\mathbf{y}$ if such a solution exists in poly-time w/ Gaussian elimination
2. Progress and preservation

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|\mathbf{x}\rangle$$

   - I.e. output restriction observation
   - Output polynomial is linear, can solve $f(\mathbf{x},\mathbf{y}) = \mathbf{x}$ for $\mathbf{y}$ if such a solution exists in poly-time w/ Gaussian elimination

2. Progress and preservation
   - Clifford path-sum has phase polynomial of degree ≤ 2

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})}|\mathbf{x}\rangle$$

   - I.e. output restriction observation
   - Output polynomial is linear, can solve $f(\mathbf{x},\mathbf{y}) = \mathbf{x}$ for $\mathbf{y}$ if such a solution exists in poly-time w/ Gaussian elimination
2. Progress and preservation
   - Clifford path-sum has phase polynomial of degree ≤ 2

   - Either reduction is possible, or $P(\mathbf{x},\mathbf{y}) = \frac{1}{2}y_0 Q(\mathbf{x}) + R(\mathbf{x},\mathbf{y})$

Proof sketch

1. Reduce to checking identity of Clifford path sum with form

$$|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} e^{2\pi i P(\mathbf{x},\mathbf{y})} |\mathbf{x}\rangle$$

    - I.e. output restriction observation
    - Output polynomial is linear, can solve $f(\mathbf{x},\mathbf{y}) = \mathbf{x}$ for $\mathbf{y}$ if such a solution exists in poly-time w/ Gaussian elimination
2. Progress and preservation
    - Clifford path-sum has phase polynomial of degree ≤ 2
    - Reductions don't increase degree of P when $\deg(P) \leq 2$
    - Either reduction is possible, or $P(\mathbf{x},\mathbf{y}) = \frac{1}{2} y_0 Q(\mathbf{x}) + R(\mathbf{x},\mathbf{y})$

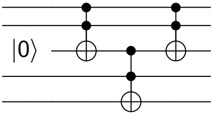
Implementation

https://github.com/meamy/feynman

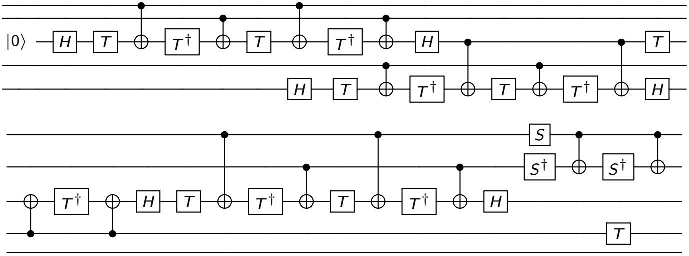
- Written in Haskell
- $\sim$ 500 lines of code
- No real language for specifying path-sums currently

Translation validation

Original (Tof_3):



Optimized:

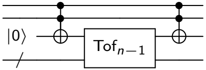


Suite of 38 benchmarks averaging 24 qubits

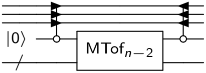
- 31 passing, 4 failing, 3 did not finish
- Largest completed: 96 qubits, 252 path variables, 25k gates in 530s
- Runs out of memory ∼1000 variables

Functional verification

Toff$_n$: $|x_1 x_2 \cdots x_n\rangle \mapsto |x_1 x_2 \cdots (x_n \oplus \prod_{i=1}^{n-1} x_i)\rangle$

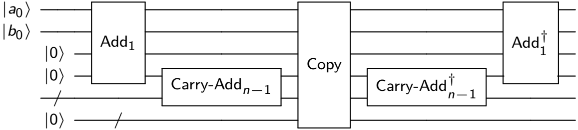


MToff$_n$: $|x_1 x_2 \cdots x_n\rangle \mapsto |x_1 x_2 \cdots (x_n \oplus \prod_{i=1}^{n-1} x_i)\rangle$

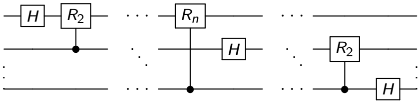


[Maslov 2016]

Adder$_n$: $|\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{0}\rangle \mapsto |\mathbf{x}\rangle|\mathbf{y}\rangle|\mathbf{x}+\mathbf{y}\rangle$

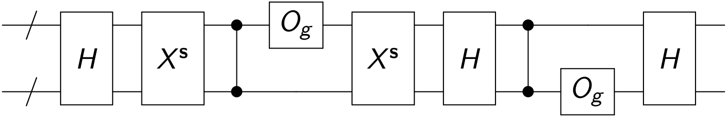


QFT$_n$: $|\mathbf{x}\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} e^{2\pi i \frac{[\mathbf{x}\cdot\mathbf{y}]}{2^n}} |\mathbf{y}\rangle$



Hidden shift

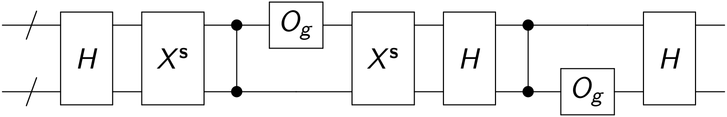
Quantum algorithm to find a hidden shift vector $\mathbf{s}$ *for a pair of shifted Maiorana-McFarland bent functions [Roetteler 2010]*



- Implements transformation $|\mathbf{0}\rangle \mapsto |\mathbf{s}\rangle$
- O_g randomly generated with A CCZ gates and $200 \cdot A$ $\{Z, CZ\}$ gates

Hidden shift

Quantum algorithm to find a hidden shift vector $\mathbf{s}$ *for a pair of shifted Maiorana-McFarland bent functions [Roetteler 2010]*



- Implements transformation $|\mathbf{0}\rangle \mapsto |\mathbf{s}\rangle$
- O_g randomly generated with A CCZ gates and $200 \cdot A$ $\{Z, CZ\}$ gates

Simulation $(n = 40, A = 5)$ in 4s, vs. hours [Brayvi & Gosset 2016]

Results

Algorithm	n	m	Clifford	T	Result	Time (s)
Toffoli_{50}	97	190	855	665	PASS	1.078
Toffoli_{100}	197	390	1755	1365	PASS	5.346
Maslov_{50}	74	192	481	384	PASS	0.759
Maslov_{100}	149	392	981	784	PASS	3.937
Adder_{8}	40	56	334	196	PASS	0.142
Adder_{16}	80	120	710	420	PASS	26.151
QFT_{16}	16	16	256	–	PASS	1.250
QFT_{31}	31	31	961	–	PASS	16.929
$\text{Hidden Shift}_{20,4}$	20	60	5254	56	PASS	1.064
$\text{Hidden Shift}_{40,5}$	40	120	6466	70	PASS	3.573
$\text{Hidden Shift}_{60,10}$	60	180	12784	140	PASS	12.811
$\text{Symbolic Shift}_{20,4}$	40	60	5296	56	PASS	1.877
$\text{Symbolic Shift}_{40,5}$	80	120	6638	70	PASS	6.633
$\text{Symbolic Shift}_{60,10}$	120	180	12804	140	PASS	34.840

Conclusion

Conclusion

- Development of path-sums as a framework for formal methods in quantum circuits

Conclusion

- Development of path-sums as a framework for formal methods in quantum circuits
- A calculus for reducing path-sums

Conclusion

- Development of path-sums as a framework for formal methods in quantum circuits
- A calculus for reducing path-sums
- A verification method which is complete for Clifford group circuits

Future work

Future work

- Implement as a formal specification language and begin collecting optimized, verified benchmark circuits

Future work

- Implement as a formal specification language and begin collecting optimized, verified benchmark circuits
- Extend to measurements

Future work

- Implement as a formal specification language and begin collecting optimized, verified benchmark circuits
- Extend to measurements
- Investigate use as a proof technique in inductive & higher order proofs

Thank you!