Title: Classifying the simulation complexities of extended Clifford circuits

Date: Dec 05, 2018 04:00 PM

URL: http://pirsa.org/18120019

Abstract: Extended Clifford circuits straddle the boundary between classical and quantum computational power. Whether such circuits are efficiently classically simulable seems to depend delicately on the ingredients of the circuits. While some combinations of ingredients lead to efficiently classically simulable circuits, other combinations, which might just be slightly different, lead to circuits which are likely not. We extend the results of Jozsa and Van den Nest [Quantum Inf. Comput. 14, 633 (2014)] by studying various further extensions of Clifford circuits. First, we consider how the classical simulation complexity changes when we allow for more general measurements. Second, we investigate different notions of what it means to "classically simulate" a quantum circuit. Third, we consider the class of conjugated Clifford circuits, where one conjugates every qubit in a Clifford circuit by the same single-qubit gate. Our results provide more examples where seemingly modest changes to the ingredients of Clifford circuits lead to "large" changes in the classical simulation complexities of the circuits, and also include new examples of extended Clifford circuits that are potential candidates for "quantum supremacy". Based on Quantum Inf. Comput. 17, 0262 (2017) and proceedings of CCCâ€™18 pp.21:1â€“21:25 (2018) (joint work with Adam Bouland and Joseph F. Fitzsimons).

Classifying the simulation complexities of extended Clifford circuits

Dax Enshan Koh

Massachusetts Institute of Technology
daxkoh@mit.edu

5 December 2018

Based on:
Quantum Inf. Comput. **17**, *0262 (2017), and*
In Proc. CCC'18 21:1–21:25 (2018) (with Adam Bouland and Joseph F. Fitzsimons).

Outline

1. Motivation
2. Classifying extended Clifford circuits
3. Classifying conjugated Clifford circuits

Extended Church-Turing thesis

Goal: to formally capture the notion of what it means for a computation to be efficient in the physical world.

Extended Church-Turing thesis (ECT)

Any realistic model of computation can be efficiently simulated on a Turing Machine.

- realistic: physically realizable in principle
- examples: Turing machine, RAM model etc.
- non-example: analog computers

Extended Church-Turing thesis

Goal: to formally capture the notion of what it means for a computation to be efficient in the physical world.

Extended Church-Turing thesis (ECT)

Any realistic model of computation can be efficiently simulated on a Turing Machine.

- efficient: at most a polynomial overhead

On the Extended Church-Turing thesis

- ECT says that the Turing machine model is sufficient to capture the notion of efficient computation in the physical world.
- Is a bridge between the physical world and the computational world.
- Is a falsifiable claim

Quantum computers and the ECT

Questions

- Are quantum computers a realistic model of computation?
- Can a quantum computer be efficiently simulated by a classical computer?

Restricted models of quantum computation

- Universal quantum computer: captures the full power of quantum computation
- Example of gates forming a universal gate set:

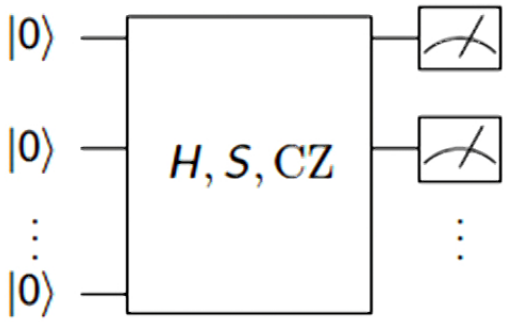
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- Restricted model of quantum computation: access to limited quantum ingredients. For example, in the circuit model, we could place restrictions on
  - types of inputs
  - types of measurements
  - structure of circuit

Restricted models of quantum computation

- Examples of restricted models: Clifford circuits, matchgate circuits, IQP circuits, DQC1 circuits, etc.

Example 1: Clifford circuits

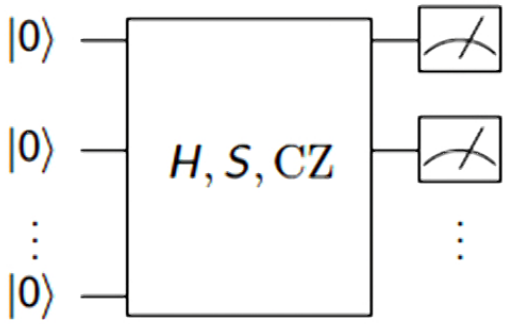


- Start with $|0\rangle^{\otimes n}$
- Apply the following gates (called Clifford gates):

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \; \mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

- Measure a subset of the qubits in the computational basis

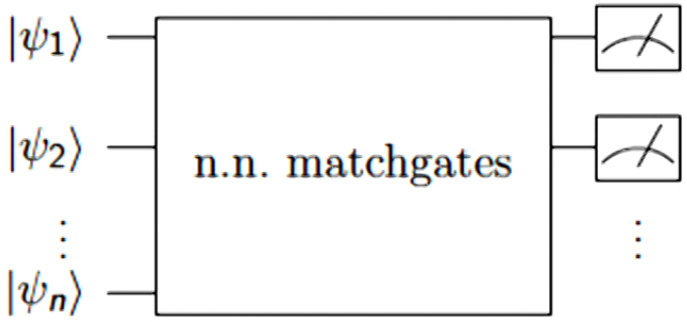
Example 1: Clifford circuits



- H, S, CZ do not form a universal set of gates.
- Clifford circuits can be efficiently simulated by a classical computer, by the Gottesman-Knill Theorem[1].

[1] Gottesman (1997).

Example 2: Matchgate circuits



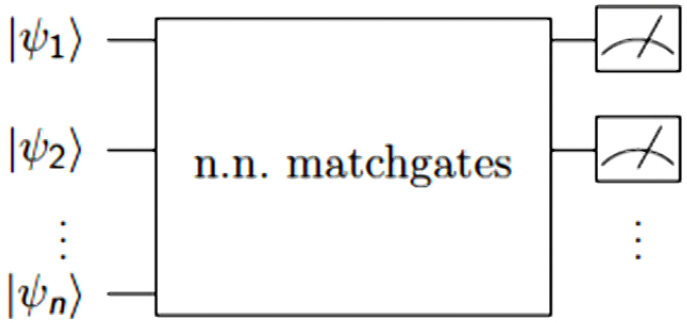
- Start with a product state $|\psi_1\rangle|\psi_2\rangle \ldots |\psi_n\rangle$.
- Apply nearest neighbor matchgates, i.e. gates of the form

$$G(A,B) = \begin{pmatrix} A_{11} & 0 & 0 & A_{12} \\ 0 & B_{11} & B_{12} & 0 \\ 0 & B_{11} & B_{12} & 0 \\ A_{21} & 0 & 0 & A_{22} \end{pmatrix}$$

  where $\det A = \det B$.

- Measure a subset of the qubits in the computational basis

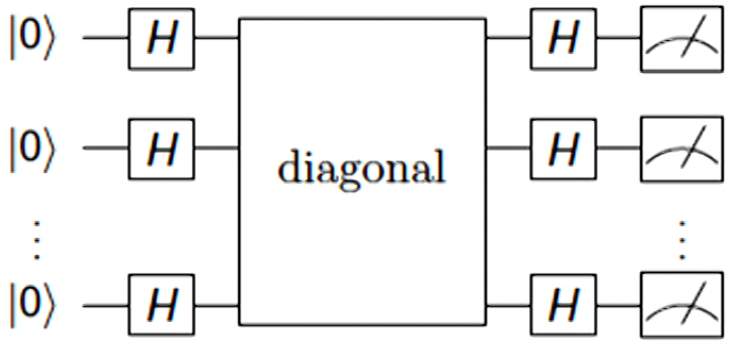
Example 2: Matchgate circuits



- Can be efficiently simulated by a classical computer[2].

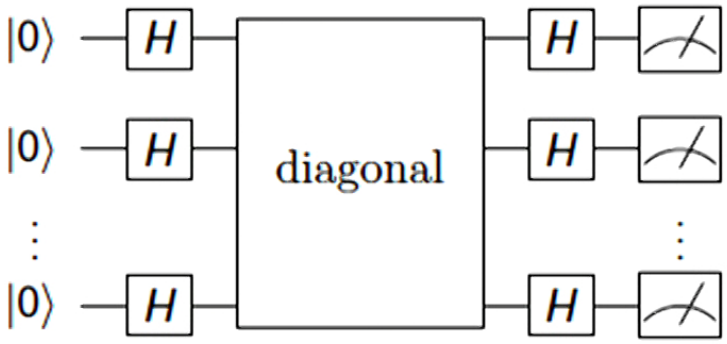
[2] Valiant (2002), Brod (2016).

Example 3: IQP circuits



- Start with $|0\rangle^{\otimes n}$
- Apply $H^{\otimes n}$
- Apply diagonal gates.
- Apply $H^{\otimes n}$
- Measure all qubits in the computational basis.

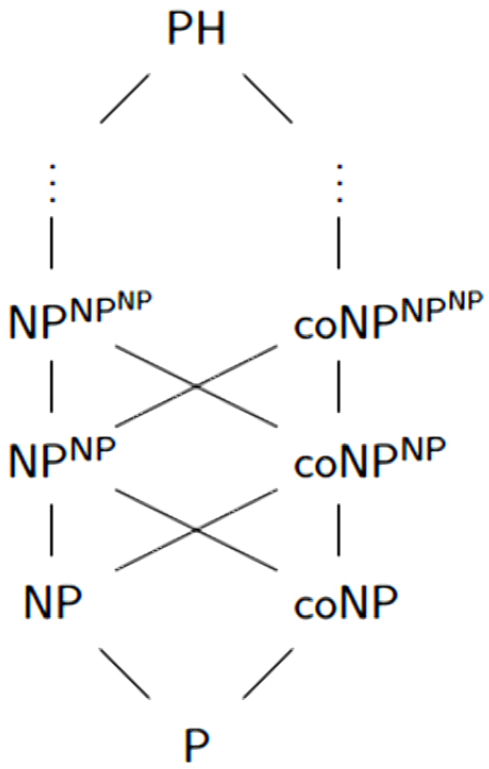
Example 3: IQP circuits



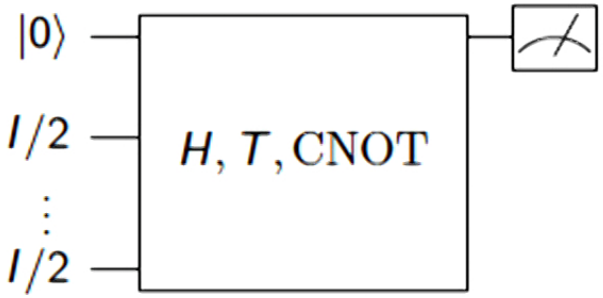
- There is no efficient classical algorithm that (exactly) samples from the output distribution of IQP circuits, unless the polynomial hierarchy collapses[3].

[3] Bremner, Jozsa and Shepherd (2010).

Polynomial hierarchy

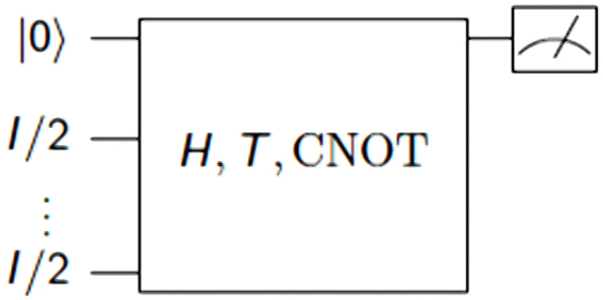


Example 4: DQC1 circuits



- Start with $|0\rangle\langle 0| \otimes \left(\frac{I}{2}\right)^{\otimes n}$
- Apply gates from a universal gate set, e.g. $\{H, T, \mathrm{CNOT}\}$
- Measure first qubit in the computational basis

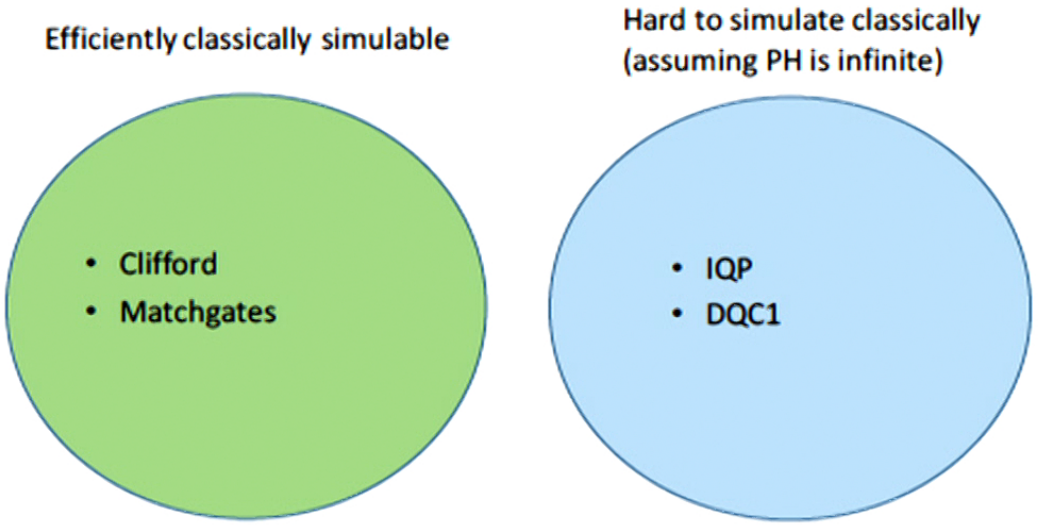
Example 4: DQC1 circuits



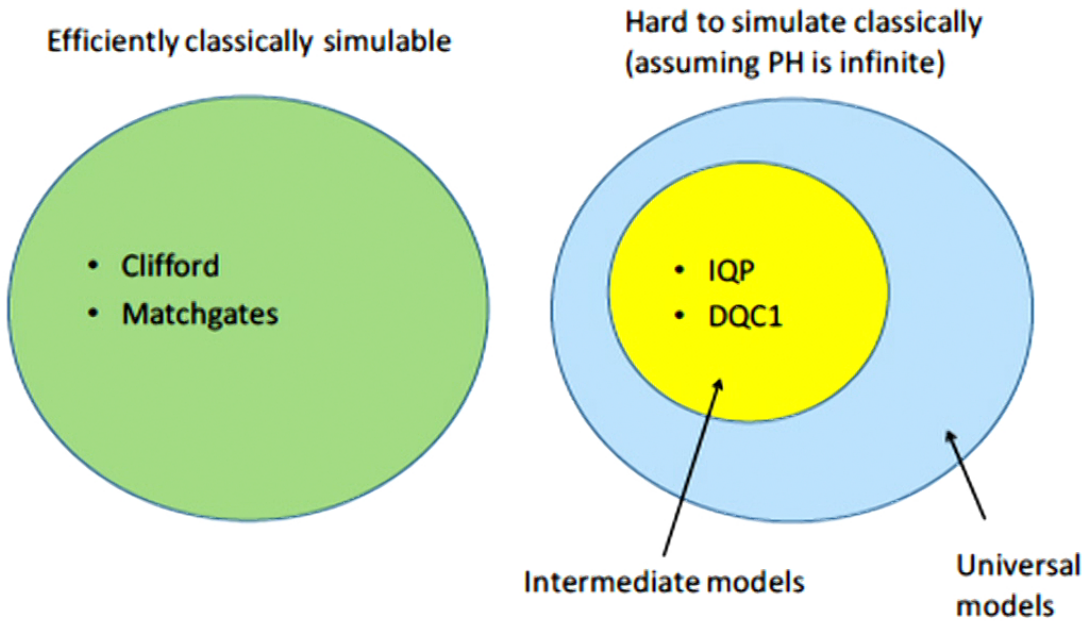
- There is no efficient classical algorithm that (exactly) samples from the output distribution of DQC1 circuits, unless the polynomial hierarchy collapses.[4].

[4] Fujii et al (2014).

Classical simulability of restricted models



Classical simulability of restricted models



- Intermediate model: a model that is (believed to be) neither universal nor classically simulable.

Intermediate models and the ECT

- Recall: to violate the ECT with quantum computers, we need to show that they are a realistic model of computation that cannot be efficiently simulated by a classical computer,
  - i.e. we need to be able to build large quantum computers, and demonstrate a super-polynomial separation between their power and that of classical computers.
  - Hard to perform with current technology.
- Less ambitious goal: perform a well-defined computational task using a quantum computer that is beyond the ability of today's state-of-the-art classical computers (called quantum computational supremacy).

Intermediate models and the ECT

Why study intermediate models?

- Might be easier to implement
- Under plausible complexity assumptions, these can generate output distributions that classical computers cannot simulate (i.e. can demonstrate quantum supremacy, and provide evidence against the ECT)
- To help us understand the quantum-classical boundary, and (hopefully) help us prove separations between quantum and classical computing, for example, by identifying resources necessary for quantum speedup

Outline

Clifford circuits

- The Pauli group is the set of operators of the form $P = i^k P_1 \otimes \ldots \otimes P_n$, where $k = 0, 1, 2, 3$ and each $P_i \in \{1, X, Y, Z\}$ is a Pauli matrix.
- The n-qubit *Clifford group* $\mathcal{C}_n$ is the normalizer of the Pauli group $\mathcal{P}_n$ in the n-qubit unitary group $\mathcal{U}_n$, i.e. $\mathcal{C}_n = \{U \in \mathcal{U}_n | U\mathcal{P}_n U^\dagger = \mathcal{P}_n\}$. Elements of the Clifford group are called *Clifford operations*.
- Claim: An operator C is a Clifford operation iff it can be implemented by a circuit consisting of the following gates (called the *basic Clifford gates*):
  - Hadamard gate $H = 1/\sqrt{2}(X + Z)$
  - phase gate $S = \mathrm{diag}(1, i)$
  - CNOT gate $CX_{ab} = |0\rangle\langle 0|_a \otimes I_b + |1\rangle\langle 1|_a \otimes X_b$
- A *Clifford circuit* (or *stabilizer circuit*) is one that consists of the basic Clifford gates and single-qubit intermediate measurement gates in the computational basis.

Clifford circuits

- Numerous applications in quantum error correction, measurement-based quantum computing, etc.
- Rich enough to encompass many 'quantum' features like quantum teleportation and entanglement.

Theorem (Gottesman-Knill)

Clifford circuits can be efficiently simulated on a classical computer.

- How robust is the Gottesman-Knill Theorem to changes in its ingredients?

Gottesman-Knill Theorem

Theorem (Gottesman-Knill)

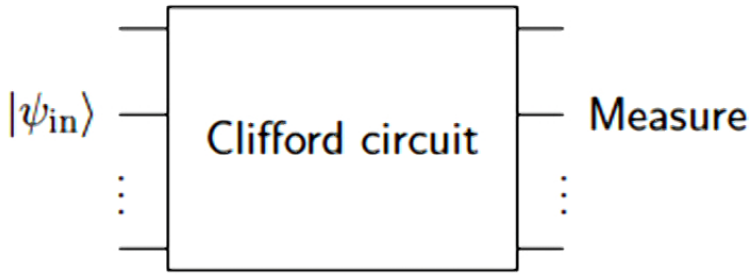
Clifford circuits can be efficiently simulated on a classical computer.

- Does the theorem still hold, if we
  - change the ingredients of the Clifford circuit, or
  - use different notions of efficient simulation?
- Circuits with different ingredients are called *extended Clifford circuits*.

Goals

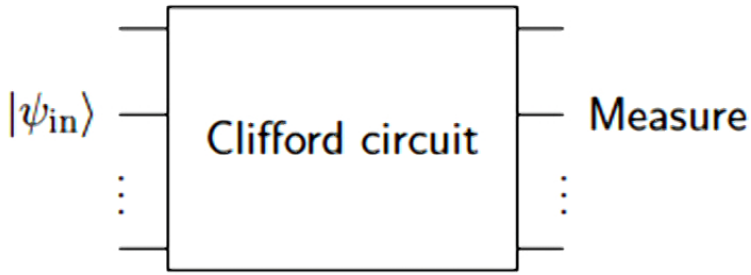
- Discuss extensions of Clifford circuits and clarify the different notions of classical simulation of quantum computation
- Determine which extended Clifford circuits are efficiently classically simulable
- Provide evidence that particular extended Clifford circuits are not efficiently classically simulable (based on plausible complexity assumptions).

Three types of ingredients of Clifford circuits



1. Inputs: IN(BITS) vs IN(PROD)
   - IN(BITS): computational basis inputs, i.e. $|\psi_{\text{in}}\rangle = |x_1, \ldots, x_n\rangle$, where $x_i \in \{0, 1\}$.
   - IN(PROD): product state inputs: i.e. $|\psi_{\text{in}}\rangle = |\alpha_1\rangle \otimes \ldots \otimes |\alpha_n\rangle$, where $\alpha_i \in \mathbb{C}^2$.

Three types of ingredients of Clifford circuits

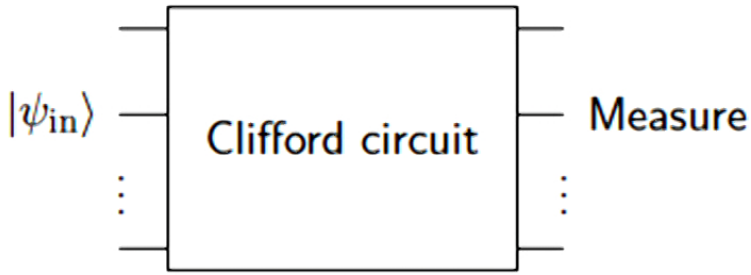


2. Intermediate measurements: ADAPTIVE vs NONADAPTIVE
   - ADAPTIVE: Input states transform as follows:

$$|\psi\rangle \rightarrow C_K(x_1,\ldots,x_K)M_{i_K(x_1,\ldots,x_{K-1})}(x_K)\ldots C_2(x_1,x_2)M_{i_2(x_1)}(x_2)C_1(x_1)M_{i_1}(x_1)C_0|\psi\rangle$$

   - NONADAPTIVE: same as above, except that C_i's and i_k's do not depend on $x_1,\ldots,x_K$.

Three types of ingredients of Clifford circuits



3. Outputs: OUT(BITS) vs OUT(PROD)
   - OUT(BITS): computational basis measurements.
   - OUT(PROD): arbitrary single-qubit measurements.

Notions of classical simulation

Informal definitions:

- Strong (called STR) simulation of a quantum circuit: a classical algorithm that calculates the probabilities of any subset of outcomes of the quantum circuit.
- Weak (called WEAK) simulation of a quantum circuit: an classical algorithm that samples from the same distribution as the quantum circuit.
- Strong-$f(n)$ (called STR($f(n)$)) simulation of a quantum circuit: like strong simulation, except that the size of the subset to be simulated is equal to $f(n)$.
- Weak-$f(n)$ (called WEAK($f(n)$)) simulation of a quantum circuit: like weak simulation, except that the size of the subset to be simulated is equal to $f(n)$.

Relationships between notions of classical simulation

Restrict our attention to the cases where $f(n) = 1$ or n.

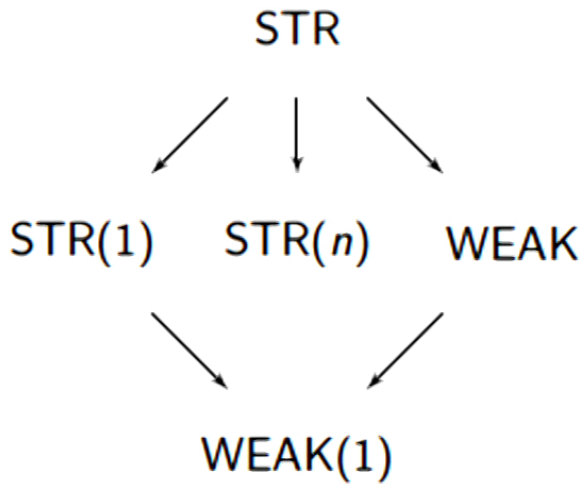


Figure: $A \to B$ means that an efficient A-simulation of a computational task implies that there is an efficient B-simulation for the same task.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)					
		IN (PROD)					
	ADAPT	IN (BITS)					
		IN (PROD)					
OUT (PROD)	NON-ADAPT	IN (BITS)					
		IN (PROD)					
	ADAPT	IN (BITS)					
		IN (PROD)					

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)					
		IN (PROD)					
	ADAPT	IN (BITS)		P (GK)			
		IN (PROD)					
OUT (PROD)	NON-ADAPT	IN (BITS)					
		IN (PROD)					
	ADAPT	IN (BITS)					
		IN (PROD)					

GK = Gottesman-Knill [Gottesman '98]. P means efficiently classically simulable.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)			
		IN (PROD)					
	ADAPT	IN (BITS)	P (vi)	P (GK)			
		IN (PROD)					
OUT (PROD)	NON-ADAPT	IN (BITS)					
		IN (PROD)					
	ADAPT	IN (BITS)					
		IN (PROD)					

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)			P (JV4)
		IN (PROD)					
	ADAPT	IN (BITS)	P (vi)	P (GK/JV5)			
		IN (PROD)					
OUT (PROD)	NON-ADAPT	IN (BITS)					
		IN (PROD)			P (Thm 5)		
	ADAPT	IN (BITS)	P (Thm 6)				
		IN (PROD)					

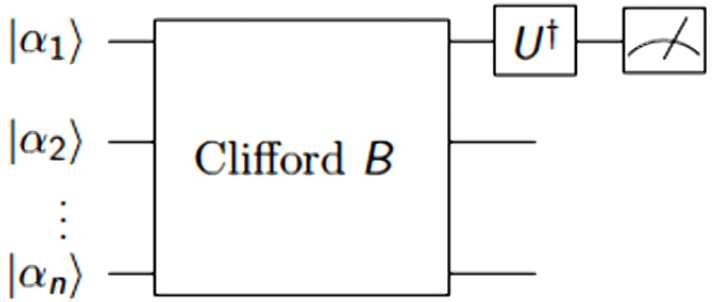
JV = Jozsa and Van den Nest [Jozsa and Van den Nest '14]

Proof of Theorem 5

Theorem

The class of IN(PROD), NONADAPT and OUT(PROD) extended Clifford circuits has an efficient strong(1) simulation.

Proof:



Proof of Theorem 5 (continued)

- Since $p_0 + p_1 = 1$, it suffices to be able to calculate $p_0 - p_1$ efficiently.
- By Born's rule, this is given by

$$p_0 - p_1 = \langle \alpha | B^\dagger (UZU^\dagger)_1 B | \alpha \rangle. \quad (1)$$

where B is the nonadaptive Clifford circuit (which we can assume is unitary).

Proof of Theorem 5 (continued)

- Since the Pauli matrices $\{\sigma^i\}_i$ form a basis for the set of 2×2 matrices , we can write

$$U = \sum_{i=0}^{3} a_i \sigma^i,$$

for some $a_i \in \mathbb{C}$.

- Hence,

$$UZU^\dagger = \sum_{i,j=0}^{3} a_i \bar{a}_j \sigma^i Z \sigma^j.$$

- But $\sigma^i Z \sigma^j$ is a Pauli operator. Since the basic Clifford gates map Pauli operators to Pauli operators,

$$B^\dagger (\sigma^i Z \sigma^j)_1 B = \gamma_{ij} P_1^{ij} \otimes \ldots \otimes P_n^{ij}.$$

Proof of Theorem 5 (continued)

- Putting this into Eq. (1), we get the following expression for $p_0 - p_1$:

$$\begin{aligned} p_0 - p_1 &= \sum_{i,j=0}^{3} a_i \bar{a}_j \gamma_{ij} \langle \alpha_1 \dots \alpha_n | P_1^{ij} \otimes \dots \otimes P_n^{ij} | \alpha_1 \dots \alpha_n \rangle \\ &= \sum_{i,j=0}^{3} a_i \bar{a}_j \gamma_{ij} \prod_{k=1}^{n} \langle \alpha_k | P_k^{ij} | \alpha_k \rangle. \end{aligned} \tag{2}$$

which can be computed efficiently.

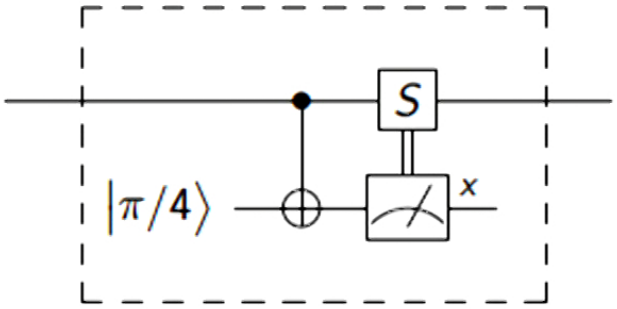
Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)		P (JV1)		
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)			
		IN (PROD)					
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)		P (xiii)		
		IN (PROD)	P (xv)		**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)				
		IN (PROD)					

JV = Jozsa and Van den Nest [Jozsa and Van den Nest '14]

Magic states

- Clifford + T gate is universal for quantum computation.
- The T gate can be simulated by the following gadget:



where $|\pi/4\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)		P (JV1)		
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)			
		IN (PROD)	QC (JV3)				
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)		P (xiii)		
		IN (PROD)	P (xv)		**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)				
		IN (PROD)					

QC means universal for quantum computation

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)		P (JV1)		
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)			
		IN (PROD)	**QC** (JV3)	QC (viii)			
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)		P (xiii)		
		IN (PROD)	P (xv)		**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)				
		IN (PROD)	QC (xxiii)	QC (xxiv)			

QC means universal for quantum computation

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)	**PH** (JV7)	P (JV1)		
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)			
		IN (PROD)	**QC** (JV3)	QC (viii)			
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)	**PH** (Thm 3)	P (xiii)		
		IN (PROD)	P (xv)		**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)				
		IN (PROD)	QC (xxiii)	QC (xxiv)			

PH means that if the problem is efficiently classical simulable, then the polynomial hierarchy collapses.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)	**PH** (JV7)	P (JV1)		
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)			
		IN (PROD)	**QC** (JV3)	QC (viii)			
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)	**PH** (Thm 3)	P (xiii)		
		IN (PROD)	P (xv)	PH (xvi)	**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)	PH (xix)			
		IN (PROD)	QC (xxiii)	QC (xxiv)			

PH means that if the problem is efficiently classical simulable, then the polynomial hierarchy collapses.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)	**PH** (JV7)	P (JV1)	**#P** (Thm 1)	
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)	**#P** (JV2)	**#P** (Thm 2)	
		IN (PROD)	**QC** (JV3)	QC (viii)			
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)	**PH** (Thm 3)	P (xiii)	**#P** (Thm 4)	
		IN (PROD)	P (xv)	PH (xvi)	**P** (Thm 5)		
	ADAPT	IN (BITS)	**P** (Thm 6)	PH (xix)			
		IN (PROD)	QC (xxiii)	QC (xxiv)			

#P means that the problem of classically simulating the circuits is a #P-hard problem.

Proof of Theorem 1

Theorem

The strong(n)-simulation of the class of IN(PROD), NONADAPT and OUT(BITS) extended Clifford circuits is #P-hard.

Proof:

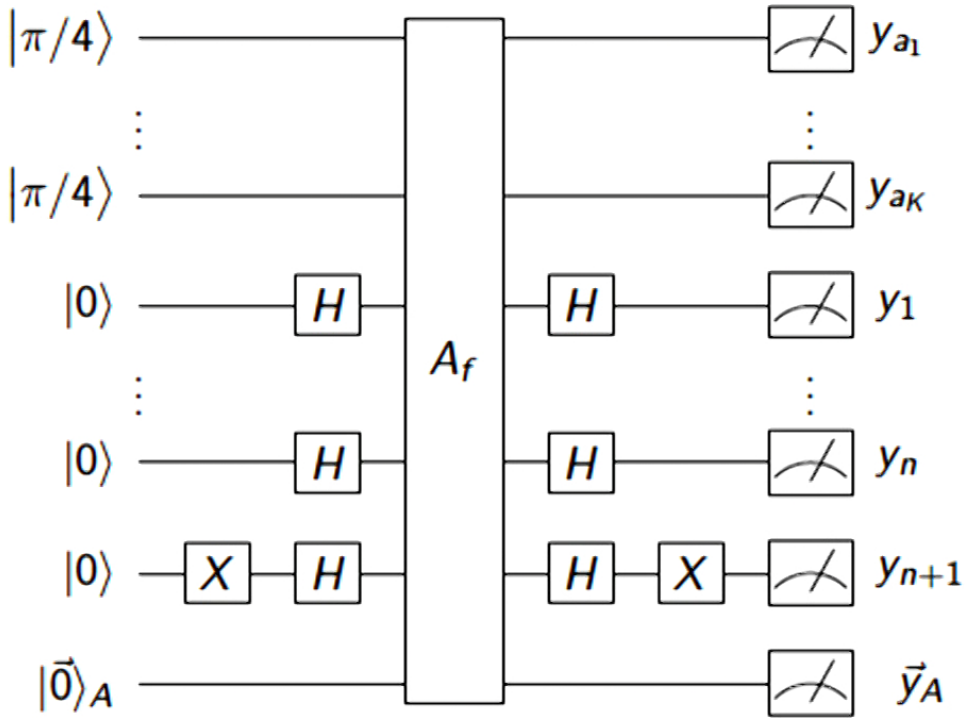
- Let $f : \{0,1\}^n \to \{0,1\}$ be a 3-CNF formula with N clauses.
- Let Q_f be a quantum circuit consisting of only the basic Clifford gates and T gates that acts as follows:

$$Q_f |x_1, \ldots, x_n, 0\rangle |\vec{0}\rangle_A = |x_1, \ldots, x_n, f(x_1, \ldots, x_n)\rangle |\vec{0}\rangle_A.$$

- Let K be the number of T gates in Q_f. For the jth T gate (acting on the l_jth line), for $j = 1, \ldots, K$, introduce an ancilla line a_j, and replace the T gate with the CNOT gate CX_{l_j, a_j}. Call the resulting circuit A_f.

Proof of Theorem 1 (continued)

- Let M_f be the following circuit:



Proof of Theorem 1 (continued)

- The gap of f is related to the outcome probabilities as follows:

$$\left|\sum_x (-1)^{f(x)}\right| = 2^{n+K/2}\sqrt{\Pr(0_{a_1}\ldots 0_{a_K}, 0_1\ldots 0_{n+1}, \vec{0}_A)}.$$

- Since computing (the absolute value of) the gap is #P-hard, so is computing the outcome probabilities.

Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)	**PH** (JV7)	P (JV1)	**#P** (Thm 1)	#P (JV6)
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)	**#P** (JV2)	**#P** (Thm 2)	#P (vii)
		IN (PROD)	**QC** (JV3)	QC (viii)	#P (ix)	#P (x)	#P (xi)
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)	**PH** (Thm 3)	P (xiii)	**#P** (Thm 4)	#P (xiv)
		IN (PROD)	P (xv)	PH (xvi)	**P** (Thm 5)	#P (xvii)	#P (xviii)
	ADAPT	IN (BITS)	**P** (Thm 6)	PH (xix)	#P (xx)	#P (xxi)	#P (xxii)
		IN (PROD)	QC (xxiii)	QC (xxiv)	#P (xxv)	#P (xxvi)	#P (xxvii)

#P means that the problem of classically simulating the circuits is a #P-hard problem.

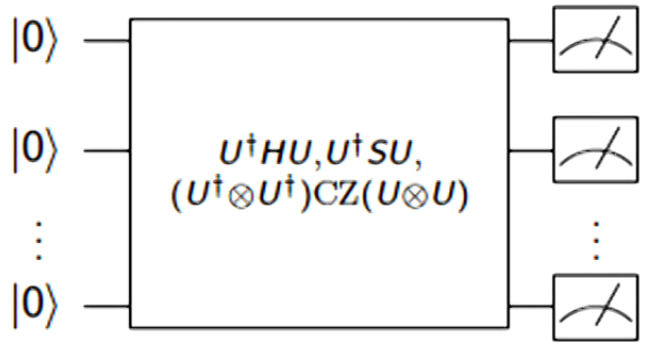
Classification of classical simulation complexities of extended Clifford circuits

			Weak		Strong		
			WEAK(1)	WEAK(n)	STR(1)	STR(n)	STR
OUT (BITS)	NON-ADAPT	IN (BITS)	P (i)	P (ii)	P (iii)	P (iv)	**P** (JV4)
		IN (PROD)	P (v)	**PH** (JV7)	P (JV1)	**#P** (Thm 1)	#P (JV6)
	ADAPT	IN (BITS)	P (vi)	**P** (JV5)	**#P** (JV2)	**#P** (Thm 2)	#P (vii)
		IN (PROD)	**QC** (JV3)	QC (viii)	#P (ix)	#P (x)	#P (xi)
OUT (PROD)	NON-ADAPT	IN (BITS)	P (xii)	**PH** (Thm 3)	P (xiii)	**#P** (Thm 4)	#P (xiv)
		IN (PROD)	P (xv)	PH (xvi)	**P** (Thm 5)	#P (xvii)	#P (xviii)
	ADAPT	IN (BITS)	**P** (Thm 6)	PH (xix)	#P (xx)	#P (xxi)	#P (xxii)
		IN (PROD)	QC (xxiii)	QC (xxiv)	#P (xxv)	#P (xxvi)	#P (xxvii)

Outline

U-conjugated Clifford circuits (U-CCCs)

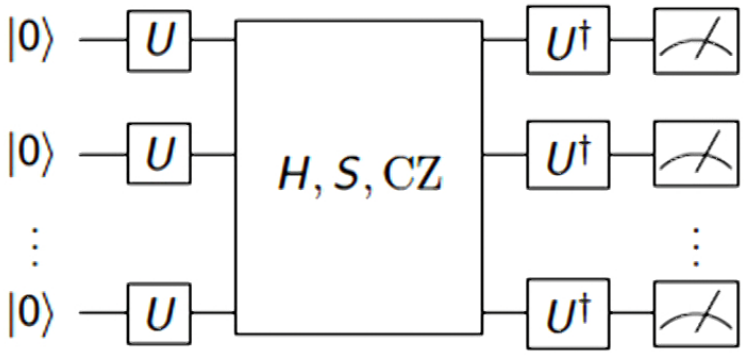
Let U be a single-qubit unitary. A U-CCC is a circuit of the following form:



- Start with $|0\rangle^{\otimes n}$
- Apply gates from the gate set $\{U^\dagger HU, U^\dagger SU, (U^\dagger \otimes U^\dagger)\mathrm{CZ}(U \otimes U)\}$.
- Measure all qubits in the computational basis.

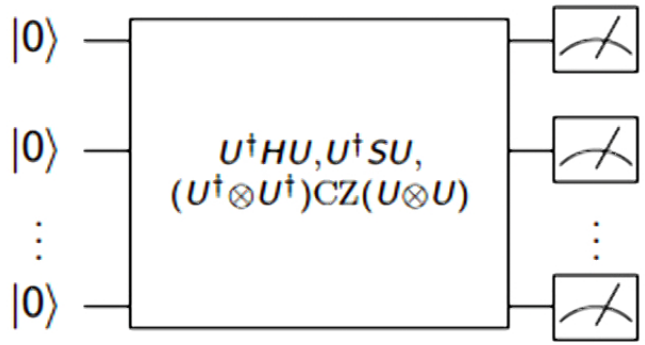
U-conjugated Clifford circuits

Equivalently, a U-CCC is a circuit of the following form:



U-conjugated Clifford circuits (U-CCCs)

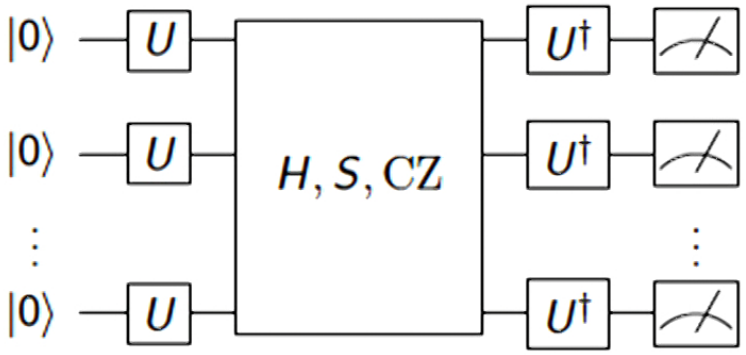
Let U be a single-qubit unitary. A U-CCC is a circuit of the following form:



- Start with $|0\rangle^{\otimes n}$
- Apply gates from the gate set $\{U^\dagger HU, U^\dagger SU, (U^\dagger \otimes U^\dagger)\mathrm{CZ}(U \otimes U)\}$.
- Measure all qubits in the computational basis.

U-conjugated Clifford circuits

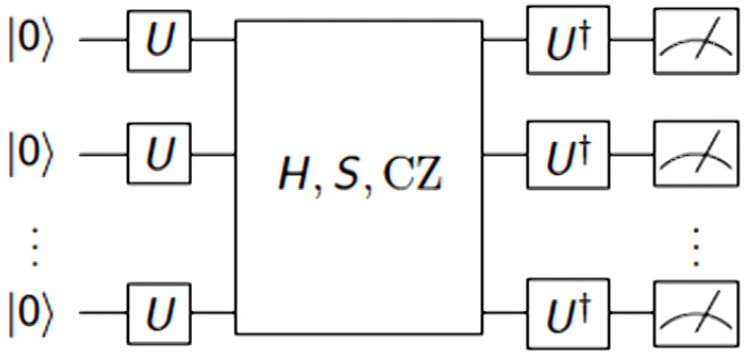
Equivalently, a U-CCC is a circuit of the following form:



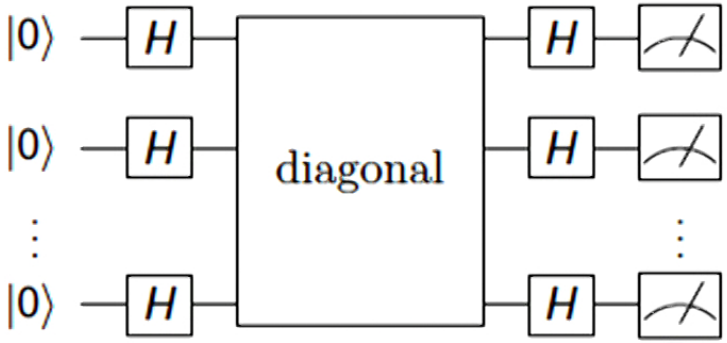
- Start with $|0\rangle^{\otimes n}$
- Apply $U^{\otimes n}$
- Apply gates from the gate set $\{H, S, \mathrm{CZ}\}$.
- Apply $(U^\dagger)^{\otimes n}$
- Measure all qubits in the computational basis.

CCC vs IQP

CCC:

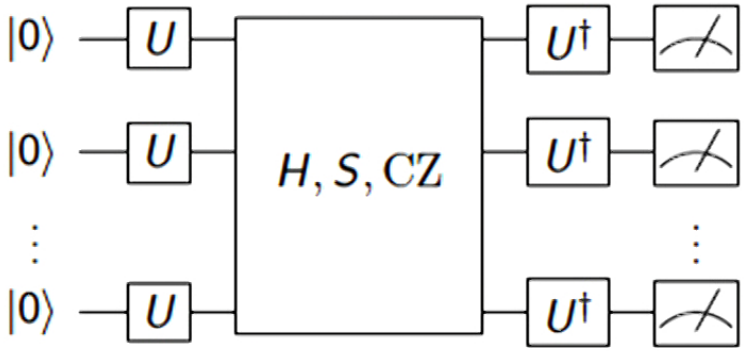


IQP:

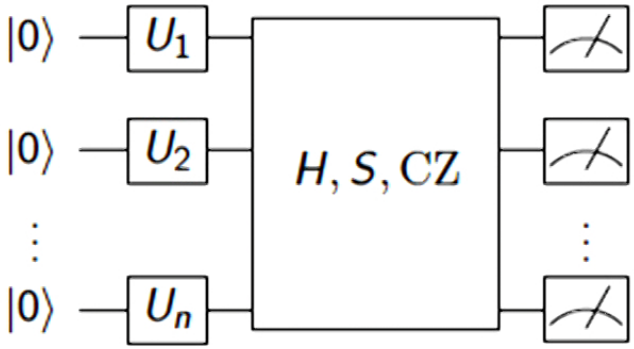


CCCs vs Clifford circuits with product inputs

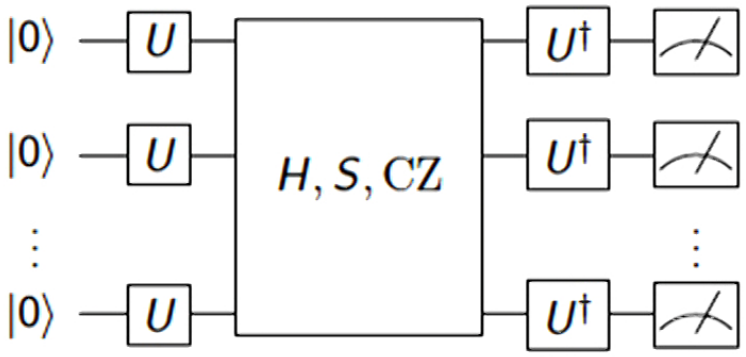
CCC:



Clifford circuits with product inputs [Jozsa and Van den Nest '14]

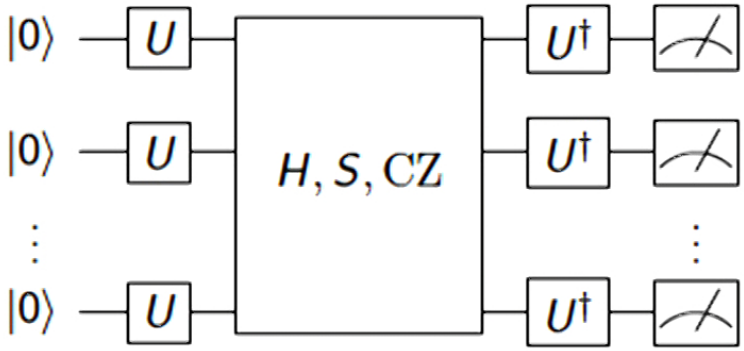


When is a U-CCC efficiently simulable?



- when U is a Clifford gate
- when U is a Z-rotation

When is a U-CCC efficiently simulable?



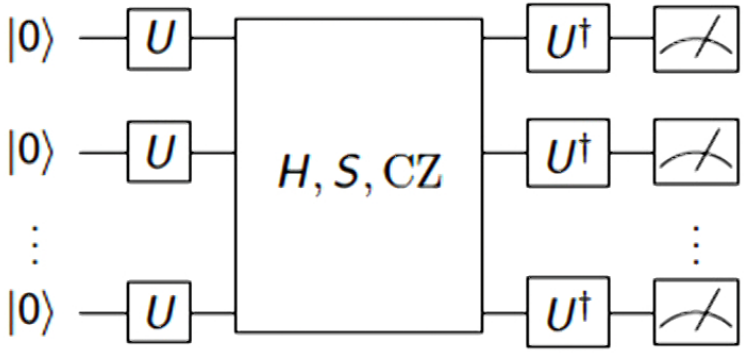
- when $U = CR_z(\theta)$, where C is a Clifford gate, and $R_z(\theta)$ is a Z-rotation.

Results

Theorem (Bouland, Fitzsimons and K. '17)

Assuming that the polynomial hierarchy is infinite, a U-CCC is classically efficiently simulable (in the weak sense) if and only if $U = CR_z(\theta)$, where C is a Clifford gate, and $R_z(\theta)$ is a Z-rotation.

Proof strategy

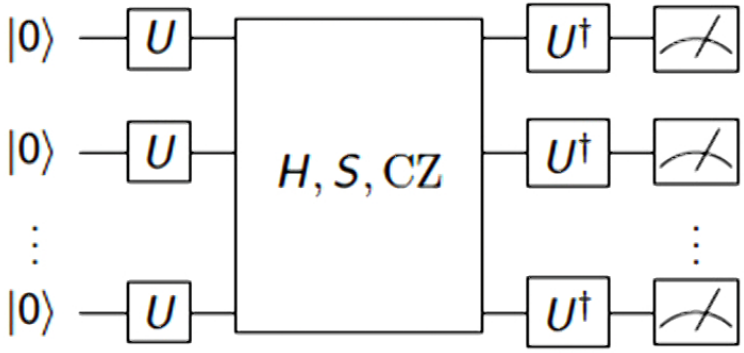


Write

$$U = e^{i\alpha} R_z(\phi) R_x(\theta) R_z(\lambda)$$

where $R_t(\theta) = e^{-i\theta\sigma_t/2} = \cos(\theta/2)I - i\sin(\theta/2)\sigma_t$.

Proof strategy



Write

$$U = \cancel{e^{i\alpha}} R_z(\phi) R_x(\theta) \cancel{R_z(\lambda)}$$

Classification result

Let $U = R_z(\phi)R_x(\theta)$. Then the classical simulation complexities of the class of U-CCCs is given by

ϕ \ θ	$\pi\mathbb{Z}$	$\frac{\pi}{2}\mathbb{Z}_{odd}$	$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$
$\frac{\pi}{2}\mathbb{Z}$	P	P	PH
$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$	P	PH	PH

Proof sketch

- It suffices to show that PostU-CCC = PostBQP.
- To see this, note that if PostU-CCC = PostBQP is true, then if the output probability distribution generated by uniform families of U-CCCs can be weakly simulated, then PostBQP = PostBPP.
- This would imply that

$$\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\mathsf{PostBQP}} = \mathsf{P}^{\mathsf{PostBPP}} \subseteq \Delta_3,$$

  i.e. the polynomial hierarchy collapses (to the third level).

Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

Let $U = R_z(\phi)R_x(\theta)$. Then the classical simulation complexities of the class of U-CCCs is given by

ϕ \ θ	$\pi\mathbb{Z}$	$\frac{\pi}{2}\mathbb{Z}_{odd}$	$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$
$\frac{\pi}{2}\mathbb{Z}$	P	P	PH (case 1)
$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$	P	PH	PH (case 1)

Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

- Pad a universal circuit with U and $U^\dagger$ gates so that each line starts with a U gate and ends with a $U^\dagger$ gate.

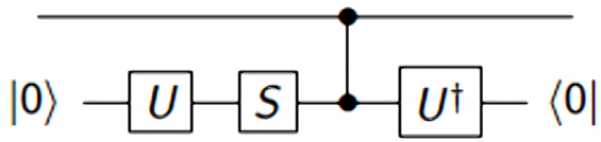
Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

- Pad a universal circuit with U and $U^\dagger$ gates so that each line starts with a U gate and ends with a $U^\dagger$ gate.
- Use the Solovay-Kitaev Theorem to compile the internal circuit into a circuit with only Clifford and $G(\theta)$ gates, where

$$G(\theta) = S^\dagger R_z(2\arctan(\cos\theta)).$$

  - $G(\theta)$ is non-Clifford, so the Clifford group + $G(\theta)$ forms a universal set of gates.
- Replace each $G(\theta)$ gate in the circuit by the following gadget:

$J(\phi, \theta) =$



  - The gadget $J(\phi, \theta)$ implements the unitary $G(\theta)$ (up to a proportionality constant).

Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

- These replacements result in a U-CCC circuit with some extra post-selections, and with the same output conditional probabilities as originally.

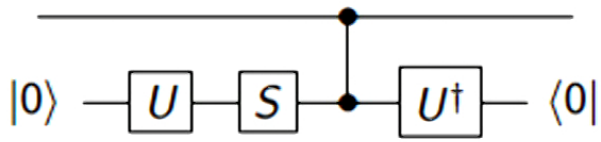
Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

- Pad a universal circuit with U and $U^\dagger$ gates so that each line starts with a U gate and ends with a $U^\dagger$ gate.
- Use the Solovay-Kitaev Theorem to compile the internal circuit into a circuit with only Clifford and $G(\theta)$ gates, where

$$G(\theta) = S^\dagger R_z(2\arctan(\cos\theta)).$$

  - $G(\theta)$ is non-Clifford, so the Clifford group + $G(\theta)$ forms a universal set of gates.
- Replace each $G(\theta)$ gate in the circuit by the following gadget:

$J(\phi, \theta) =$



  - The gadget $J(\phi, \theta)$ implements the unitary $G(\theta)$ (up to a proportionality constant).

Case 1: $U = R_z(\phi)R_x(\theta)$, where $\theta \notin \frac{\pi}{2}\mathbb{Z}$

- These replacements result in a U-CCC circuit with some extra post-selections, and with the same output conditional probabilities as originally.
- This shows that PostU-CCC = PostBQP

  $\Longrightarrow$ if the output probability distribution generated by uniform families of U-CCCs can be weakly simulated, then the polynomial hierarchy collapses (to third level).

Case 2: $U = R_z(\phi)R_x(\theta)$, where $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$

Let $U = R_z(\phi)R_x(\theta)$. Then the classical simulation complexities of the class of U-CCCs is given by

ϕ \ θ	$\pi\mathbb{Z}$	$\frac{\pi}{2}\mathbb{Z}_{odd}$	$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$
$\frac{\pi}{2}\mathbb{Z}$	P	P	PH
$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$	P	PH (case 2)	PH

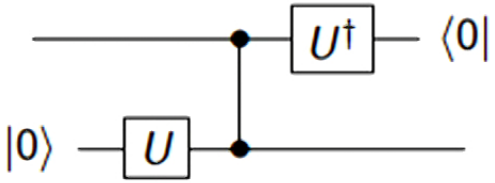
Case 2: $U = R_z(\phi)R_x(\theta)$, where $\phi \notin \frac{\pi}{2}\mathbb{Z}$ and $\theta \in \frac{\pi}{2}\mathbb{Z}_{odd}$

- Same as before, except that we use the Solovay-Kitaev Theorem to compile the internal circuit into a circuit with only Clifford and $H(\theta)$ gates, where

$$H(\phi,\theta) = \begin{pmatrix} \cos^2\frac{\theta}{2} & \frac{i}{2}\sin\theta\ e^{-i\phi} \\ -\frac{i}{2}\sin\theta\ e^{i\phi} & -\sin^2\frac{\theta}{2} \end{pmatrix}.$$

  - $H(\phi,\theta)$ is non-Clifford, so the Clifford group + $H(\phi,\theta)$ forms a universal set of gates.
- Replace each $H(\phi,\theta)$ gate in the circuit by the following gadget:

$I(\phi,\theta) =$



  - The gadget $I(\phi,\theta)$ implements the unitary $H(\phi,\theta)$ (up to a proportionality constant).

Classification result

Let $U = R_z(\phi)R_x(\theta)$. Then the classical simulation complexities of the class of U-CCCs is given by

ϕ \ θ	$\pi\mathbb{Z}$	$\frac{\pi}{2}\mathbb{Z}_{odd}$	$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$
$\frac{\pi}{2}\mathbb{Z}$	P	P	PH
$\left(\frac{\pi}{2}\mathbb{Z}\right)^c$	P	PH	PH

Approximate notions of simulation

Let $\mathcal{P} = \{p_z\}_z$ and $\mathcal{Q} = \{q_z\}_z$ be (discrete) probability distributions, and let $\epsilon \geq 0$.

- $\mathcal{Q}$ is a *multiplicative ϵ-approximation* of $\mathcal{P}$ if for all z,

$$|p_z - q_z| \leq \epsilon p_z . \tag{3}$$

- $\mathcal{Q}$ is an *additive ϵ-approximation* of $\mathcal{P}$ if

$$\frac{1}{2} \sum_z |p_z - q_z| \leq \epsilon. \tag{4}$$

Note that any multiplicative ϵ-approximation is also an additive $\epsilon/2$-approximation, since summing (3) over all z produces (4).

Approximate notions of simulation

Definition (multiplicative (additive) error)

A *weak simulation with multiplicative (additive) error* $\epsilon > 0$ of a family of quantum circuits is a classical randomized algorithm that samples from a distribution that is a multiplicative (additive) ϵ-approximation of the output distribution of the circuit.

Approximate notions of simulation

- Previous classification results hold for weak simulation with multiplicative error $c \geq 1$.
- Do they also hold for weak simulation with additive error?
  - We are able to prove hardness, only if we make further assumptions.

Results: Hardness of weak simulation with additive error

Let V be a Clifford circuit on n qubits, U be a one-qubit unitary which is not a Z-rotation times a Clifford, and $y \in \{0,1\}^n$ be an n-bit string. Define

$$p_{y,U,V} = \left| \langle y | (U^\dagger)^{\otimes n} V U^{\otimes n} | 0^n \rangle \right|^2 .$$

Let the corresponding probability distribution on y's given U and V be denoted $D(U,V)$.

Lemma (Anti-concentration lemma for Clifford circuits)

For any fixed U and y as above, and for any constant $0 < a < 1$, we have that at least $\frac{(1-a)^2}{2}$ fraction of the Clifford circuits V have the property that

$$p_{y,U,V} \geq \frac{a}{2^n}.$$

Results: Hardness of weak simulation with additive error

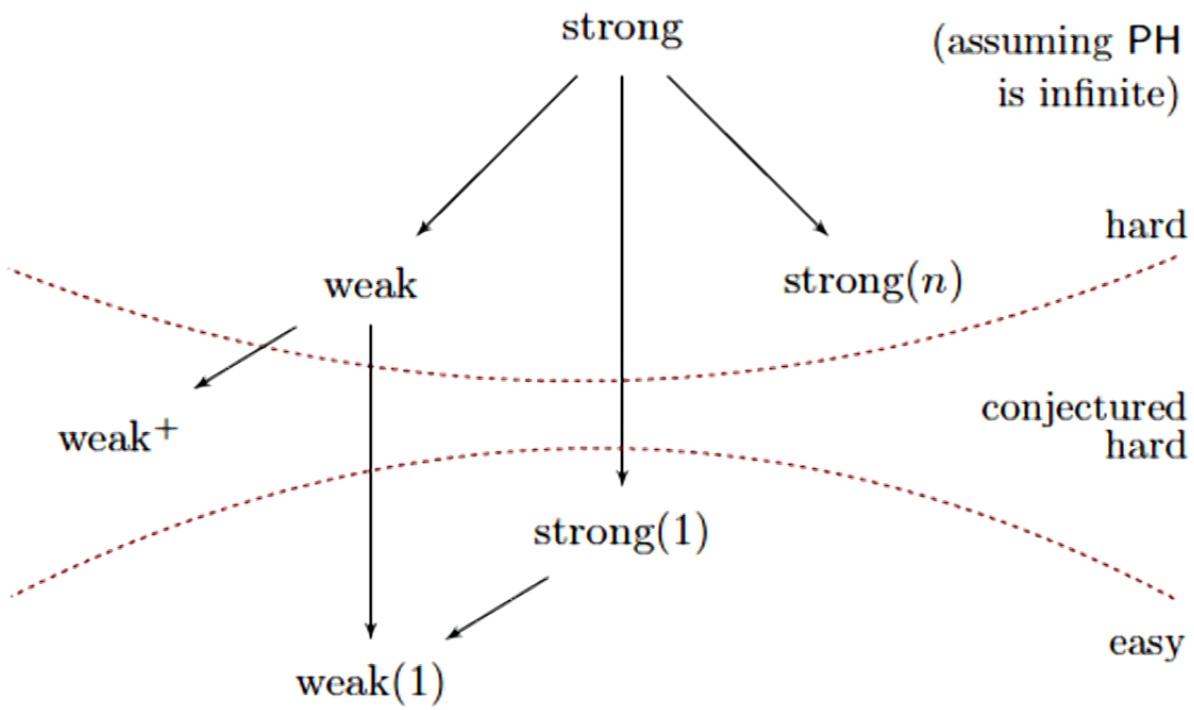
Conjecture

For any U which is not equal to a Clifford times a Z-rotation, it is #P-hard to approximate a $6/50$ fraction of the $p_{y,U,V}$ over the choice of y, V to within multiplicative error $1/2 + o(1)$.

Theorem

Assume the above conjecture and that PH is infinite. Then there is no efficient classical algorithm which, when given a one-qubit unitary U and an n-qubit Clifford circuit V, outputs a probability distribution which is $1/100$ close to $D(U, V)$ in total variation distance.

Relationships between different notions of classical simulation for CCCs



Concluding remarks

- Whether we can efficiently classically simulate extended Clifford circuits depends delicately on the ingredients of the circuit
- Seemingly 'modest' changes to the ingredients can lead to large complexity changes
- Several extensions can be proven to be hard to simulate, under plausible complexity assumptions.

Questions

- Other restricted models?
- Better conjectures?
- Candidate for quantum supremacy?

References

Bremner, M. J., Jozsa, R., and Shepherd, D. J. (2010).

Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy.

In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20100301. The Royal Society.

Brod, D. J. (2016).

Efficient classical simulation of matchgate circuits with generalized inputs and measurements.

Physical Review A, 93(6):062332.

Fujii, K., Kobayashi, H., Morimae, T., Nishimura, H., Tamate, S., and Tani, S. (2014).

Impossibility of classically simulating one-clean-qubit computation.

arXiv preprint arXiv:1409.6777.

Gottesman, D. (1998).

The Heisenberg representation of quantum computers.

Talk at International Conference on Group Theoretic Methods in Physics.

Jozsa, R. and Van den Nest, M. (2014).

Classical simulation complexity of extended Clifford circuits.

Quantum Info. Comput., 14:633–648.

Valiant, L. G. (2001).

Quantum computers that can be simulated classically in polynomial time.

In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 114–123. ACM.