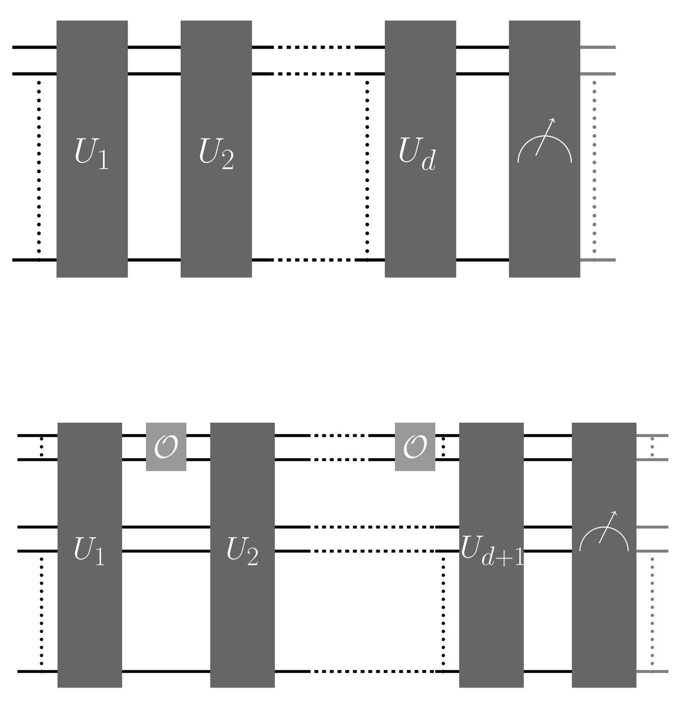
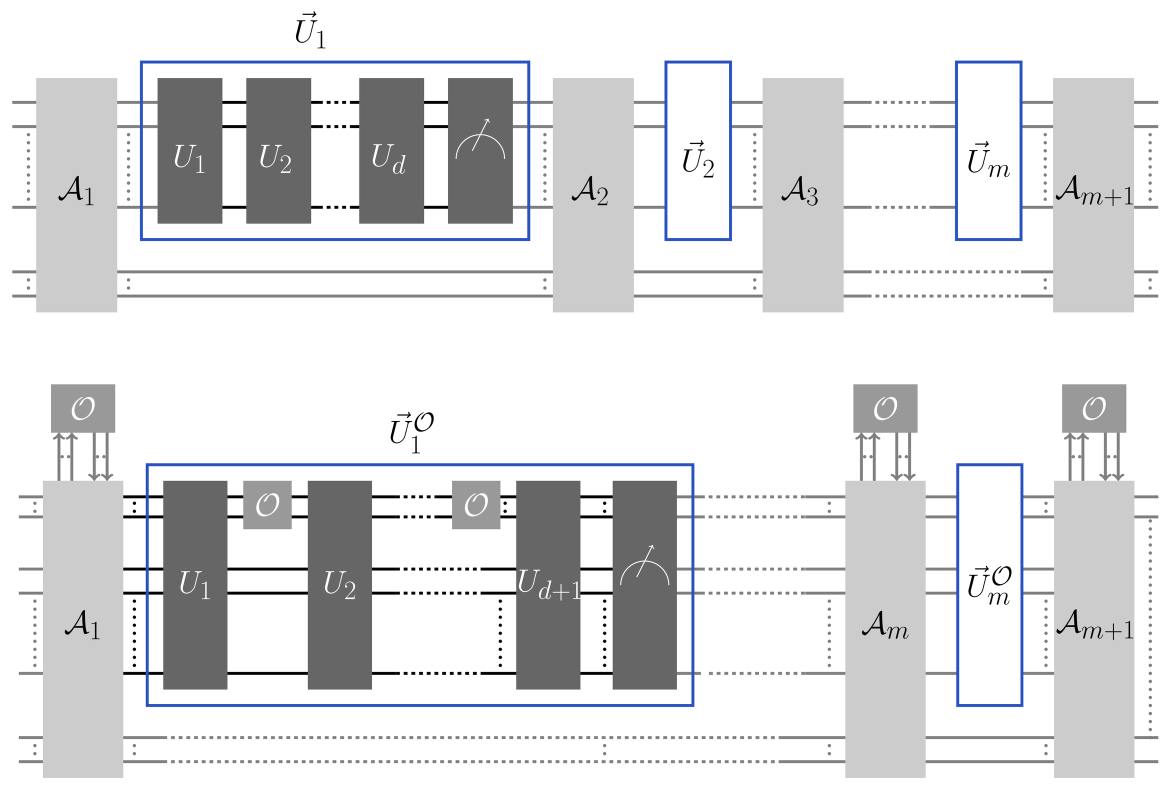
Oracle separations of Hybrid Quantum-Classical circuits

Atul Singh Arora   Alexandru Gheorghiu   Uttam Singh

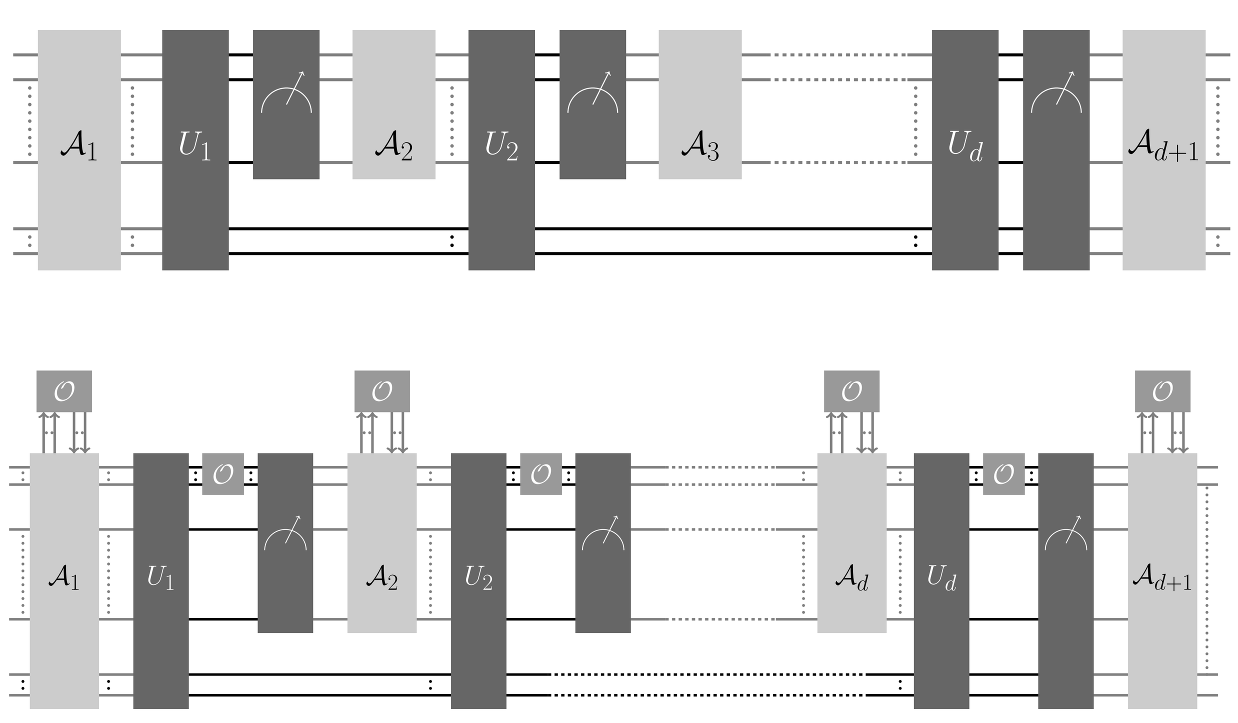
The Models of Computation



QNC$_d$ ~ QNC when $d = \log^{O(1)}(n)$



CQ$_d$ or BPP$^{\text{QNC}_d}$



QC$_d$ or "QNC$_d^{\text{BPP}}$"

Motivation

Belief: BPP ⊂ BQP

Why? Period Finding, Integer Factoring, Discrete Log

But. These can be solved by QNC with poly-time classical pre-post-processing

Extended Josza's conjecture*:

$\text{BPP}^{\text{QNC}} = \text{QNC}^{\text{BPP}} = \text{BQP}$

Results (and Prior Work)

	QC$_d$	CQ$_d$	Oracle	
d'-SeS	$d'+1 \le d \le 2d'+2$	$d \le 1$	Standard	This work
d'-SCS	$d \le 4$	$d'+1 \le d \le d'+5$	Stochastic	This work
d'-SSP	$d'+1 \le d \le 2d'+2$	$d'+1 \le d \le 2d'+1$	Standard	CCL*
d'-SS		$d'+1 \le d \le 2d'+1$	Standard	This work

wrt to an oracle

$\text{BPP}^{\text{QNC}} \subset \text{BQP}$

$\text{QNC}^{\text{BPP}} \subset \text{BQP}$

Prior Art (CCL* and CM)

$\text{BPP}^{\text{QNC}} \nsubseteq \text{QNC}^{\text{BPP}}$

$\text{BPP}^{\text{QNC}} \nsubseteq \text{QNC}^{\text{BPP}}$

This work

Background

Recall | Simon's Problem

Given a Simon's function $f: \{0,1\}^n \to \{0,1\}^n$, i.e. a two-to-one function s.t. $f(x) = f(x \oplus s)$ for some hidden period s, find the period s.

Recall | Simon's Algorithm

$$|0^n\rangle_X |0^n\rangle_Y \overset{H}{\mapsto} \sum_x |x\rangle|0\rangle$$

$$\overset{O}{\mapsto} \sum_x |x\rangle|g(x)\rangle$$

$$\overset{\Pi_Y}{\mapsto} (|x\rangle + |x \oplus s\rangle)|y\rangle$$

$$\overset{H}{\mapsto} \sum_d (-1)^{x \cdot d}(1 + (-1)^{s \cdot d})|d\rangle|y\rangle$$

Repeat, obtain equations $s \cdot d = 0$ and solve to obtain s.

d-Shuffler

Consider d random permutations, $f'_0, \cdots, f'_{d-1}$ from $\{0,1\}^{2n} \to \{0,1\}^{2n}$.

Define f'_d to be such that $f'_d(\cdots f'_0(x)) = f(x)$ for $x \in \{0,1\}^n$.

Define $f_i = \begin{cases} f'_i(\cdots f'_0(x)) & \text{if } x \in \{0,1\}^n \\ \perp & \text{otherwise} \end{cases}$.

$(f_i)_{i=0}^d$ is called a d-Shuffler and we denote it as Ξ.

Stochastic Oracle

Let

X, Y be finite sets,
$\mathbb{F}_Y$ be some distribution over Y,
$g(x, y) : X \times Y \to Z$ be a function.

An *intrinsically stochastic oracle* $\mathcal{S}$ wrt $\mathbb{F}_Y$ corresponding to g acts on each query as:

Samples $y \leftarrow \mathbb{F}_Y$ and on input $|x\rangle|z\rangle$ produces $|x\rangle|z \oplus g(x, y)\rangle$.

The Problems

d-Serial Simon's Problem (d-SeS)

Sample $d+1$ random Simon's functions $\{f_i\}_{i=0}^d$ with periods $\{s_i\}$.

The problem: to find the period s_d of the last Simon's function.

However, only access to f_0 is given directly. Access to f_i, for $i \ge 1$, is given via a function L_{f_i} which outputs $f_i(x)$ if the input is (s_{i-1}, x) and $\perp$ otherwise.

NB: To access the ith Simon's function, one needs the period of the $(i-1)$th Simon's function.

d-Shuffled Collisions to Simon's Problem (d-SCS)

Uniformly sample f from all 2-to-1 functions, g from all Simon's functions, and h from all 1-to-1 functions.

Let p be some canonical bijection which maps colliding pairs of f to those of g (and p_{inv} be the inverse).

Let p' be such that $p'(h(f(x)), x) = p(x)$ and Ξ is a d-Shuffler encoding h.

The problem: given p', p'_{inv}, Ξ and a *stochastic* oracle $\mathcal{S}$ for f, find the period of g.

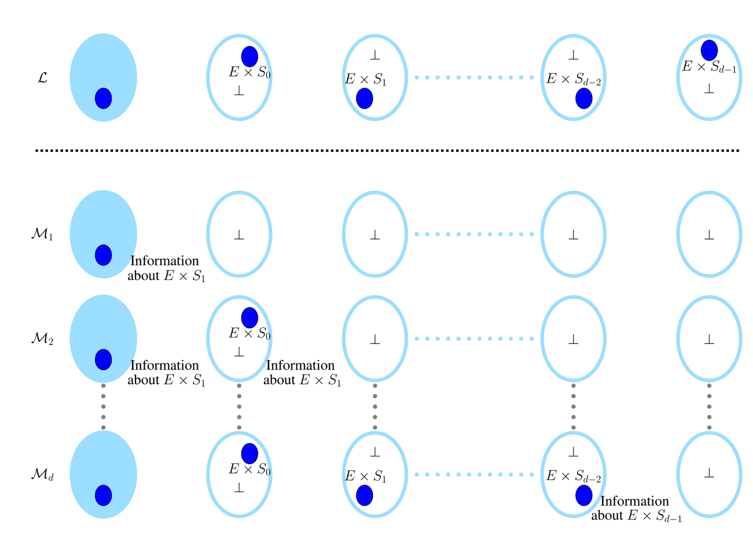
Bounds

CQ$_1$ solves d-SeS

CQ$_1$ can make polynomially many oracle calls to QNC$_d$.

Thus, CQ$_1$ can parallely unlock the periods s_i, hence the Simon function f_d, and can find s_d.

QC$_d$ cannot



QC$_4$ solves d- SCS

1. Apply the stochastic oracle $\mathcal{S}$ on inputs $(|0\rangle + |1\rangle)_Q|0\rangle_{RR'} \mapsto (|0\rangle_Q|x_0\rangle_R + |1\rangle_Q|x_1\rangle_R)|y\rangle_{R'}$ where $y = f(x_0) = f(x_1)$ is random.
2. Classically, compute, $h(y)$ using Ξ.
3. Quantumly, use p' with $h(y)$ to get $|0\rangle|x_0\rangle|p(x_0)\rangle + |1\rangle|x_1\rangle|p(x_1)\rangle$
4. Proceed as in Simon's to get $p(x_0) \oplus p(x_1) = s$ the period.

CQ$_d$ cannot

Oracle access is to a generic 2-to-1 function f instead of the Simon function g. Superpositions over colliding pairs are no longer related by the period s. To obtain any information about s, query to the bijection p is needed. But in CQ$_d$ the quantum subroutines must measure their states completely before invoking the classical subroutines. Only the classical subroutines can obtain access to the bijection as the shuffler can only be invoked by a circuit of depth at least d.

References, Affiliation, PDF and related | QR

Caltech

QIP, 2022