On the Computational Power of QAC^0 with Barely Superlinear Ancillae

Wonjun Baek

MITx dept. of Physics(8) Studying disease transmission
Yonsei University dept. of Earth system sciences

Table of contents

Overview

- Major Theorems and concepts
- Basic $\varepsilon - error$ approximations

Pauli/Fourier degree

- Basic concepts of approximation
- Boolean Fourier expansion

Boolean function

- Embedding Booleans as operators
- Approximate degree conservation

Pauli degree growth

- Ancilla models and channels
- Comparison between AC^0 model

Applications

- Comparison between prev. works
- Available applications (lack of insight)

Overview / Abstract

Quantum Arithmetic Circuit의 가장 아래 변환층

$\boxed{\mathsf{QAC}^0}$ is the family of constant-depth polynomial-size quantum circuits consisting of arbitrary single qubit unitaries and multi-qubit Toffoli gates. It was introduced by Moore as a quantum counterpart of AC^0, along with the conjecture that QAC^0 circuits cannot compute PARITY. In this work, we make progress on this long-standing conjecture: we show that any depth-d QAC^0 circuit requires $n^{1+3^{-d}}$ ancillae to compute a function with approximate degree $\boxed{\Theta(n)}$, which includes PARITY, MAJORITY and MOD_k. We further establish superlinear lower bounds on quantum state synthesis and quantum channel synthesis. This is the first lower bound on the super-linear sized QAC^0. Regarding PARITY, we show that any further improvement on the size of $\boxed{\text{ancillae}}$ to $n^{1+\exp(-o(d))}$ would imply that $\mathrm{PARITY} \notin \mathsf{QAC}^0$.

These lower bounds are derived by giving low-degree approximations to QAC^0 circuits. We show that a depth-d QAC^0 circuit with a ancillae, when applied to low-degree operators, has a degree $(n+a)^{1-3^{-d}}$ polynomial approximation in the spectral norm. This implies that the class QLC^0, corresponding to linear size QAC^0 circuits, has an approximate degree $o(n)$. This is a quantum generalization of the result that LC^0 circuits have an approximate degree $o(n)$ by Bun, Kothari, and Thaler. Our result also implies that $\boxed{\mathsf{QLC}^0} \neq \mathsf{NC}^1$.

$$f(n) = O(g(n))$$

$$f(n) = \Theta(g(n))$$

$$f(n) = o(g(n))$$

$$f(n) = \Omega(g(n))$$

Key theorem

For any $2^n \times 2^n$ operator A with degree ℓ, and any unitary U implemented by a depth-d QAC^0 circuit, the approximate degree of $UAU^\dagger$ is upper bounded by $\tilde{O}\left(n^{1-3^{-d}}\ell^{3^{-d}}\right)$.

Let $f\colon\{0,1\}^n \to \{0,1\}$ be a Boolean function with approximate degree $\Omega(n)$. Suppose U is a depth d QAC0 circuit with n input qubits and $a = \tilde{O}(n^{1+3^{-d}})$ ancillae initialized in any quantum state. Then U cannot compute f with the worst-case error strictly below 1/2. And U can't approximate $Parity_n$ nor $Majority_n$ over uniform inputs.

Theorem 1.4 (informal of Corollary 5.3). *If any* QAC^0 *circuit with* $n^{1+\exp(-o(d))}$ *ancillae, where d is the depth of this circuit family, can not compute* Parity_n *with the worst-case error* $\mathrm{negl}(n)$, *then any* QAC^0 *circuit family with arbitrary polynomial ancillae can not compute* Parity_n *with the worst-case error* $\mathrm{negl}(n)$.

Theorem 1.6 (informal of Theorem 7.2). *Suppose* $\mathcal{E}_{U,\psi}$ *is a quantum channel from n qubits to k qubits, implemented by a depth-d* QAC^0 *circuit U with n input qubits and a ancillae. The upper bound of approximate degree of the Choi representation* $\Phi_{U,\psi}$ *of* $\mathcal{E}_{U,\psi}$ *is then given by* $\tilde{O}\left((n+a)^{1-3^{-d}}k^{3^{-d}/2}\right)$.

$$C(\Phi) = \sum_{i,j} |i\rangle\langle j|_{A'} \otimes \Phi(|i\rangle\langle j|_A).$$

More about Choi representation

- We can represent ρ_{AB} as an ensemble of pure states
$$\rho_{AB} = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|.$$
- We can also view ρ_{AB} as part of a pure state (its purification) as
$$\rho_{AB} = \mathrm{Tr}_E \left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right].$$

Theorem 4.1 (Choi and Kraus). *For a linear map $T : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ the following are equivalent:*

1. *The map T is completely positive.*
2. *There exist operators $\{K_i\}_{i=1}^R \subset B(\mathcal{H}_A, \mathcal{H}_B)$ and some $R \in \mathbb{N}$ such that*
$$T = \sum_{i=1}^{R} \mathrm{Ad}_{K_i}. \tag{4.1}$$

$$C(\Phi) = \sum_{i,j} |i\rangle\langle j|_{A'} \otimes \Phi(|i\rangle\langle j|_A).$$

Proof. Since the maps $\mathrm{Ad}_{K_i} : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ are completely positive, it is clear that 2. implies 1.. To see the other direction, consider a completely positive map $T : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$. By Theorem 3.8, the Choi matrix

$$C_T = \dim(\mathcal{H}_A)\,(\mathrm{id}_{A'} \otimes T)\,(\omega_{\mathcal{H}_A})$$

is positive semidefinite. Using the spectral decomposition, we can write

$$C_T = \sum_{i=1}^{R} |\psi_i\rangle\langle\psi_i|,$$

for $R = \mathrm{rk}\,(C_T)$ and some (unnormalized) vectors $|\psi_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Next, we use the inverse of the vectorization isomorphism and Theorem 2.14 to show that

$$|\psi_i\rangle = \mathrm{vec}\,(K_i) = (\mathbb{1}_{\mathcal{H}_A} \otimes K_i)\,|\Omega_{\mathcal{H}_A}\rangle,$$

for some operators $K_i \in B(\mathcal{H}_A, \mathcal{H}_B)$. Combining the previous equations, we find that

$$C_T = \sum_{i=1}^{R} (\mathbb{1}_{d_A} \otimes K_i)\,\omega_{d_A}\,(\mathbb{1}_{d_A} \otimes K_i)^\dagger = \sum_{i=1}^{R} C_{\mathrm{Ad}_{K_i}} = C_{\sum_{i=1}^{R} \mathrm{Ad}_{K_i}}.$$

Finally, we use that the Choi-Jamiolkowski isomorphism is indeed an isomorphism and the last equation implies

$$T = \sum_{i=1}^{R} \mathrm{Ad}_{K_i}.$$

□

Pauli-fourier degrees

$$\mathbb{E}_{\mathbf{x}}[f(\mathbf{x})g(\mathbf{x})]$$

$$\chi_S(x) = (-1)^{\sum_{i\in S} x_i}$$

$$f = \sum_{S\subseteq[n]} \widehat{f}(S)\chi_S$$

$$\|f\|_2^2 = \sum_{S\subseteq[n]} \widehat{f}(S)^2$$

$$\deg(A) = \max_{\sigma:\widehat{A}(\sigma)\neq 0} |\sigma|$$

$$\|M\|_p = \left(\frac{1}{n}\operatorname{Tr}\left[|M|^p\right]\right)^{1/p}$$

Normalized Schatten p-norm

$$F(\rho,\sigma) = \operatorname{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]$$

Fidelity

$$1 - \frac{1}{2}\|\rho-\sigma\|_{TD} \leq F(\rho,\sigma) \leq \sqrt{1-\frac{1}{4}\|\rho-\sigma\|_{TD}^2}$$

Lemma 2.7. *Let $A, B, \widetilde{A}, \widetilde{B}$ be operators satisfying*

- $\|A\| \leq 1$ *and* $\|B\| \leq 1$.
- $\left\|A - \widetilde{A}\right\| \leq \varepsilon_0$.
- $\left\|B - \widetilde{B}\right\| \leq \varepsilon_1$.

Then $\|AB\| \leq 1$ *and* $\left\|AB - \widetilde{A}\widetilde{B}\right\| \leq \varepsilon = \varepsilon_0 + \varepsilon_1 + \varepsilon_0\varepsilon_1 = (1+\varepsilon_0)(1+\varepsilon_1) - 1$.

The Pauli matrices $\mathcal{B}_0, \ldots, \mathcal{B}_3$ are

$$\mathcal{B}_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathcal{B}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \mathcal{B}_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \mathcal{B}_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

which form an orthonormal basis in $\mathcal{M}_2$. For integer $n \geq 1$ and $\sigma \in \{0,1,2,3\}^n$, we define

$$\mathcal{B}_\sigma = \mathcal{B}_{\sigma_1} \otimes \cdots \otimes \mathcal{B}_{\sigma_n}.$$

The set of Pauli matrices $\{\mathcal{B}_\sigma\}_{\sigma\in\{0,1,2,3\}^n}$ forms an orthonormal basis in $\mathcal{M}_{2^n}$. For any $2^n \times 2^n$ matrix A, the Pauli expansion of A is

$$A = \sum_{\sigma\in\{0,1,2,3\}^n} \widehat{A}(\sigma)\cdot\mathcal{B}_\sigma.$$

The coefficients $\widehat{A}(\sigma)$'s are called the Pauli coefficients of A. We can then define the degree and the approximate degree of a matrix.

$$M_f = \sum_x f(x)\cdot|x\rangle\langle x| = \begin{bmatrix} f(0^n) & & \\ & \ddots & \\ & & f(1^n) \end{bmatrix} = \sum_{\sigma\in\{0,3\}^n} \widehat{f}(S_\sigma)\cdot\mathcal{B}_\sigma$$

Quantum circuit application

Initial register $|x\rangle$

Ancillae register $|\psi\rangle$

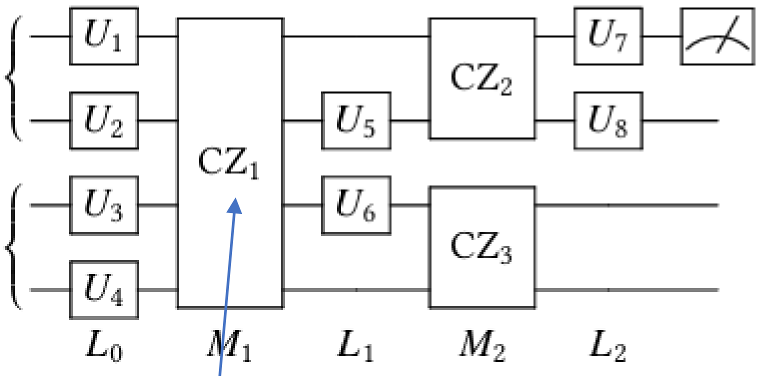


Figure 1: $\mathbf{QAC}^0$ Circuit Example

$$U\left(|\varphi\rangle \otimes |\psi\rangle\right)$$

$$\Pr[C(x) = 1] = \operatorname{Tr}\left[(|1\rangle\langle 1| \otimes I)\, U(|x\rangle\langle x| \otimes |\psi\rangle\langle\psi|)U^\dagger\right]$$

$$\Pr\left[C(x) \neq f(x)\right] \leq \varepsilon$$

Worst case error

$$\mathop{\mathbb{E}}_{\mathbf{x}\in\{0,1\}}\left[\Pr\left[C(\mathbf{x}) \neq f(\mathbf{x})\right]\right] \leq \varepsilon$$

Average case error

$$\mathrm{CZ} = \mathbb{1} - 2\,|1\rangle\langle 1|^n$$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$CZ(X \otimes I)CZ^\dagger = X \otimes Z$$

$$CZ(I \otimes X)CZ^\dagger = Z \otimes X$$

$$|🐱_n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$$

$$|\nu\rangle = \frac{1}{\sqrt{2}}(|0^n, \psi_0\rangle + |1^n, \psi_1\rangle)$$

The complexity class $\mathbf{QAC}^0$ consists of all languages that can be decided by constant-deph and polynomial-sized $\mathbf{QAC}$ quantum circuits. Formally, a language L is in $\mathbf{QAC}^0$ if there exists a family of constant-deph and polynomial-sized $\mathbf{QAC}$ quantum circuits $\{C_n\}_{n\in\mathbb{N}}$ such that for any $n \in \mathbb{N}$ and $x \in \{0,1\}^n$, if $x \in L$ then $\Pr[C_n(x) = 1] \geq 2/3$, and if $x \notin L$, then $\Pr[C_n(x) = 0] \geq 2/3$ where $C_n(x)$ is the measurement outcome on the output qubits of the circuit C_n on input x. We also introduce the class of $\mathbf{QLC}^0$ circuits, which consists of $\mathbf{QAC}^0$ circuits with linear-sized ancillae.

Lemma 3.1 ([AM23, Lemma 3.1], see also [KAAV17]). *Let $H = \sum_{i=1}^{n} H_i$ be a sum of n commuting projectors each acting on ℓ qubits, and $|\psi\rangle$ be the maximum-energy eigenstate of H. Then, for any $r \in (\sqrt{n}, n)$, let $\varepsilon = 2^{-\frac{r^2}{2^8 n}}$,*

$$\widetilde{\deg}_{\varepsilon}(|\psi\rangle\langle\psi|) \le \ell r.$$

Corollary 3.2. *Let $|\psi\rangle$ be an ℓ-qubit pure state. Then for any $r \in (\sqrt{n}, n)$, let $\varepsilon = 2^{-\frac{r^2}{2^8 n}}$. It holds that*

$$\widetilde{\deg}_{\varepsilon}\left(|\psi\rangle\langle\psi|^{\otimes n}\right) \le \ell r.$$

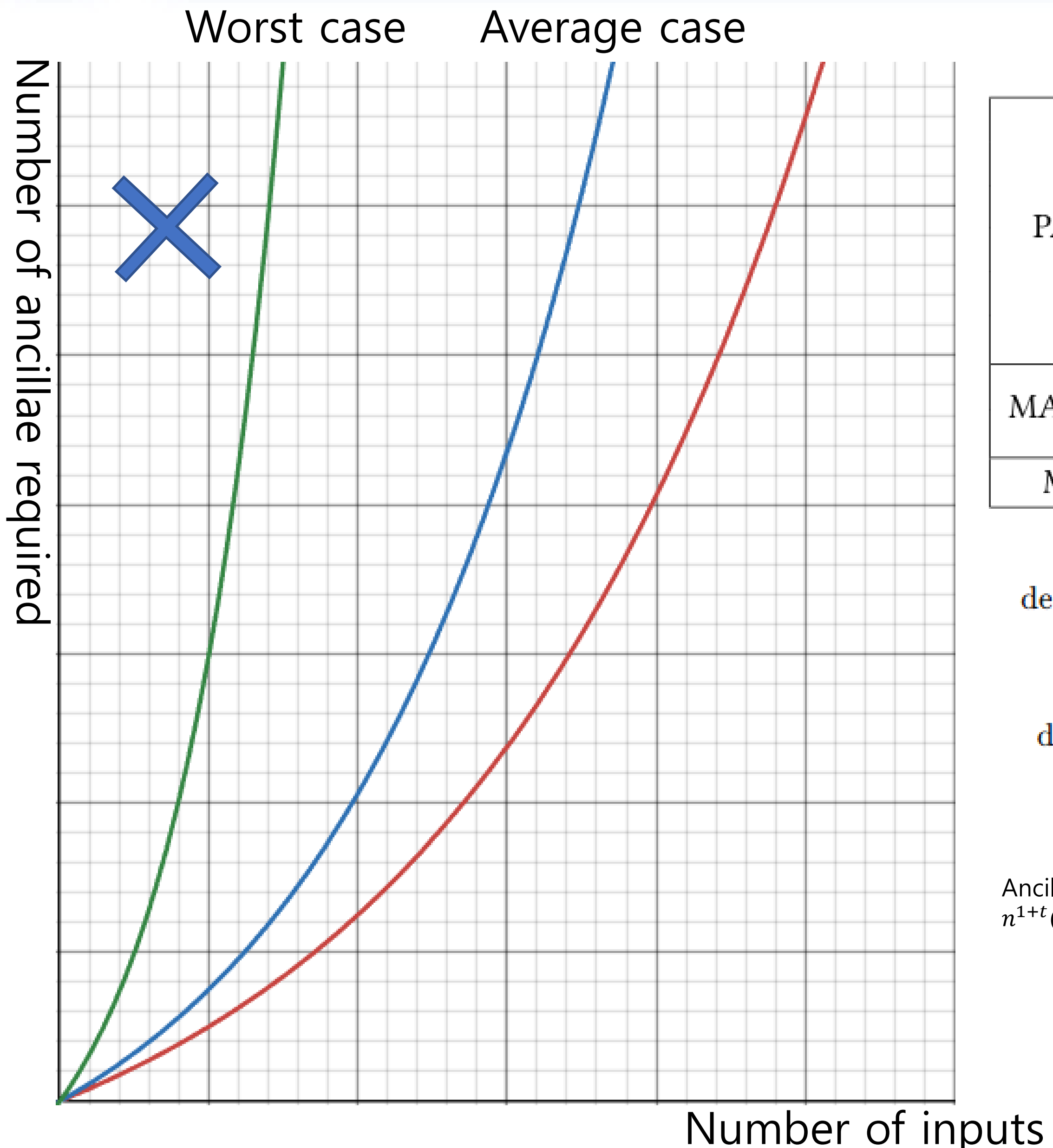
Corollary 3.3. *For any CZ-gate CZ acting on n qubits and real number $1 < r < n$, there exists an operator $\widetilde{\mathrm{CZ}}$ such that*

$$\left\|\mathrm{CZ} - \widetilde{\mathrm{CZ}}\right\| \le 2^{1-2^{-8} r}$$

and

$$\deg\left(\widetilde{\mathrm{CZ}}\right) \le \sqrt{nr}.$$

Overview / Abstract



PARITY	$a \geq n2^{-d} - 1$	exact	[FFG+06]
	impossible when $d = 2$	exact	[PFGT20]
	impossible when $d = 2$	average case	[Ros21]
	$a \leq \exp(O(n \log n/\varepsilon))$ when $d = 7$	worst case	[Ros21]
	$a \geq n^{\Omega(1/d)}$	average case	[NPVY24]
	$a \geq n^{1+3^{-d}}$	average/worst case	**This work**
MAJORITY	$a \geq n^{\Omega(1/d)}$	average case†	[NPVY24]
	$a \geq n^{1+3^{-d}}$	average/worst case	**This work**
MOD_k	$a \geq n^{1+3^{-d}}$	worst case	**This work**

$$\deg_\varepsilon(UAU^\dagger) \leq \widetilde{O}(n^{1-3^{-d}} \ell^{3^{-d}})$$

Operator spreading 능력의 제한성 수치화

Fan-out과 ancillae를 이용한 Fan-in, 그리고 CZ를 갖지만
Deep entanglement와 high degree operator를 생성할 수 없음

$$\deg_\varepsilon(f) \leq \widetilde{O}((n+a)^{1-3^{-d}})$$

Boolean function에서의 계산 가능한 function 경계 디자인

Centre Boolean function대부분이 계산 불가능
Classical AC^0보다는 강하지만 $NC^1 - QNC^1$ 수준으로는 도달 X

Ancilla가 $n^{1+3^{-d}}$보다 작으면 PARITY 불가능
$n^{1+t}(t > 1)$정도면 PARITY 가능

The end

Thank you

for listening