On the cost of evaluating Boolean functions on a Non-adaptive Measurement-based Quantum Computer

Michael de Oliveira[1,2,3], Luís S. Barbosa[2,3], Ernesto F. Galvão[1]

[1] International Iberian Nanotechnology Laboratory
[2] University of Minho
[3] INESC TEC

Motivation

Measurement-based quantum computation (MBQC) is a known universal model. Its non-adaptive version ($\text{NMQC}_{\oplus}$) draws power from quantum correlations on an entangled resource, aided by a limited parity-2 classical computer. $\text{NMQC}_{\oplus}$ clarifies the computational role of correlations, the required resources, and control. Additionally, it suggests experiments associated with demonstrations of quantum non-locality and contextuality.

Definitions

NMQC⊕ model

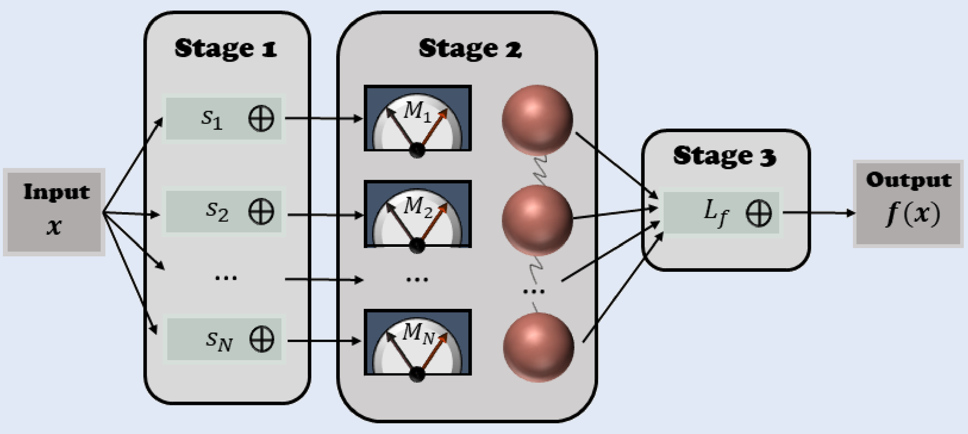
$\text{NMQC}_{\oplus}$ computations can be divided into three stages:

1. A linear pre-processing stage, that computes a Boolean value $s_i = L_i(x)$ based on the input string $x \in \{0,1\}^n$ for each measurement, with a linear function $L_i(x)$.
2. A measurement stage, where one of two dichotomic measurement operators

$$M_i(s_i) = \cos(\theta_i + s_i\phi_i)\sigma_x + \sin(\theta_i + s_i\phi_i)\sigma_y$$

will be applied on each qubit of an n-qubit resource state.
3. A linear post-processing stage, where all the outcomes from the measurements (m_i) are added modulo two

$$f(x) = L_f(m_1, m_2, ..., m_n) = \bigoplus_{i=1}^{n} m_i \; .$$



Theorem 1. [1] [Adapted] There is a measurement assignment/set of instructions for the $\text{NMQC}_{\oplus}$ model such that any Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be evaluated deterministically, using a 2^n-qubit generalized GHZ state.

The problem

Determining the linear functions which select measurement bases that are stabilizers of the GHZ state, such that for all $x \in \{0,1\}^n$,

$$\left\langle \Psi^k_{GHZ} \right| \otimes_{i=1}^{k} M_i(L_i(x)) \left| \Psi^k_{GHZ} \right\rangle = (-1)^{f(x)} \; .$$

This translates to a search problem for a multi-linear polynomial ($\text{poly}_f(x)$),

$$\left\langle \Psi^k_{GHZ} \right| \otimes_{i=1}^{k} M_i(L_i(x)) \left| \Psi^k_{GHZ} \right\rangle = \cos\Big(\underbrace{\sum_{i=1}^{k} \theta_i + \phi_i L_i(x)}_{\text{poly}_f(x)} \Big)$$

Questions

- How to find the measurement assignments/set of instructions to evaluate a Boolean function deterministically?
- What are the minimum resources necessary for the deterministic evaluation of Boolean functions?

Reduced Fourier Construction

We propose a new construction to determine a correct multi-linear polynomial for any Boolean function f, with the following process,

$$\begin{aligned} \text{poly}_f(x) &= \pi * \sum_{S\subseteq[n]} c_S * \mathcal{RF}\Big(\prod_{i\in S} x_i\Big) \\ &= \pi * \Big(\mathcal{RF}\Big(\prod_{i\in S_1} x_i\Big) + ... + \mathcal{RF}\Big(\prod_{i\in S_t} x_i\Big)\Big) \\ &= \text{poly}_1(x) + \text{poly}_2(x) + ... + \text{poly}_n(x) \equiv f(x) \; . \end{aligned}$$

using the RF transformation,

$$\mathcal{RF} = \begin{bmatrix} \binom{n}{0} & \cdots & \binom{n}{i} & \cdots \\ \binom{n-1}{0} & \cdots & -\binom{n-1}{1} + \binom{n-1}{2} & \cdots \\ \binom{n-2}{0} & \cdots & \binom{n-2}{0} - 2\binom{n-2}{1} + \binom{n-2}{2} & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ (-1)^0\binom{n}{n} & \ldots & (-1)^i\binom{n}{n-i} & \ldots \end{bmatrix}$$

with their entries defined as follows,

$$rf_{i,j} = \begin{cases} \sum_{k=0}^{i} (-1)^k \binom{j}{k}\binom{n-j}{i-k}, & i < j,\ i+j <= n \\ \sum_{k=0}^{j} (-1)^k \binom{j}{k}\binom{n-j}{i-k}, & i >= j,\ i+j < n \\ \sum_{k=j+i-n}^{j} (-1)^k \binom{j}{k}\binom{n-j}{i-k}, & i >= j,\ i+j >= n \\ \sum_{k=0}^{n-j} (-1)^{i-k} \binom{j}{i-k}\binom{n-j}{k}, & i < j,\ i+j > n \end{cases}$$

Example

For the function $g : \{0,1\}^3 \to \{0,1\}$, defined as

$$g(x_1, x_2, x_3) = x_1 * x_2 \oplus x_2 * x_3 \; .$$

In order to compute the Fourier coefficients, the $\mathcal{RF}$ transform will be applied to simplified value vectors [2],

$$\mathcal{RF} \underbrace{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}}_{v_{x_1 * x_2}} = \begin{bmatrix} 1/4 \\ -1/4 \\ 1/4 \end{bmatrix} \; , \; \mathcal{RF} \underbrace{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}}_{v_{x_2 * x_3}} = \begin{bmatrix} 1/4 \\ -1/4 \\ 1/4 \end{bmatrix} \; .$$

Afterward, these are used to generate the respective multi-linear polynomial,

$$\text{poly}_g(x) = \frac{1}{2}x_1 + x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1 \oplus x_2 - \frac{1}{2}x_2 \oplus x_3 \; .$$

This specific polynomial translates to a 5-qubit GHZ state, the linear functions $L_1(x) = x_1$, $L_2(x) = x_2$, $L_3(x) = x_3$, $L_4(x) = x_1 \oplus x_2$, and $L_5(x) = x_2 \oplus x_3$.
Additionally, the corresponding measurement operators are
$M_1(s_1) = (\neg s_1)\sigma_x + s_1\sigma_y$, $M_2(s_2) = (\neg s_2)\sigma_x - s_2\sigma_x$, $M_3(s_3) = (\neg s_1)\sigma_x + s_3\sigma_y$, $M_4(s_4) = (\neg s_4)\sigma_x - s_4\sigma_y$, and $M_5(s_5) = (\neg s_5)\sigma_x - s_5\sigma_y$.

Symmetric Boolean functions

Symmetric Boolean functions (SBF) have an ANF representation of the following form, for all $x \in \{0,1\}^n$,

$$f^{sym}(x) = c_0 \oplus c_1 * C^1 \oplus c_2 * C^2 \oplus ... \oplus c_d * C^d = \bigoplus_{k=0}^{d} c_k * C^k$$

where C^k terms represent the complete symmetric function (CSF) of dimension k, defined for all $x \in \{0,1\}^n$ as

$$C^k(x) = \bigoplus_{i_1=1}^{n-k+1} x_{i_1} \Big(\bigoplus_{i_2=i_1+1}^{n-k+2} x_{i_2} \big(\; ... \; \big(\bigoplus_{i_N=i_{k-1}+1}^{n} x_{i_N} \big)\big)\Big),$$

with $|x| = n$.

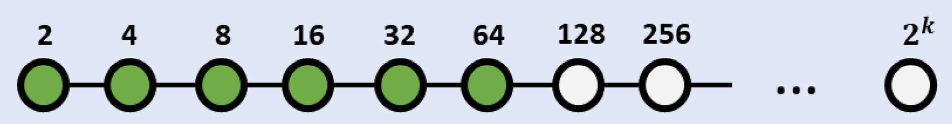
CSF construction

Any SBF can be obtained by composing elements of the CSF set which have degrees that are powers of two, i.e. for all $x \in \{-1,1\}^n$

$$\text{poly}_{f^{sym}}(x) = \sum_{k=0}^{d} c_k \Big(\prod_{r\in R_k} \mathcal{GC}\Big(C^r(x)\Big)\Big), \; \sum_{r\in R_k} 2^r = k$$

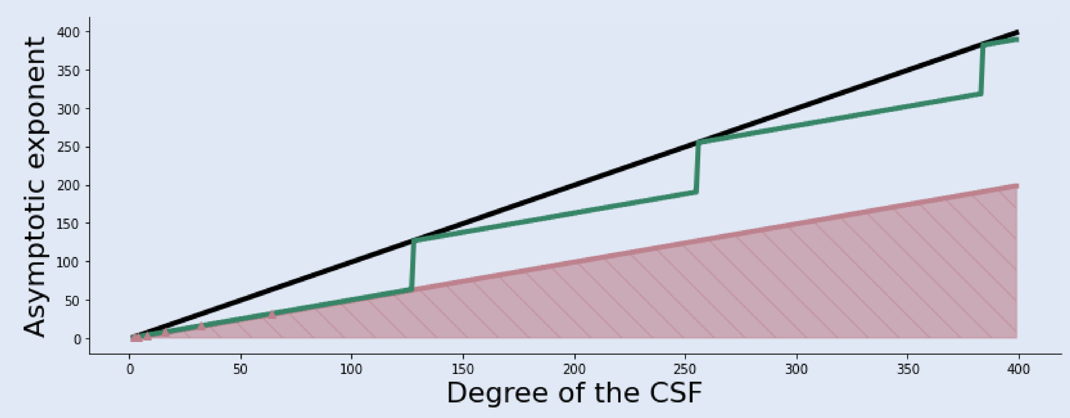
CSF polynomials

$$\text{poly}_{C^k}(x) = \frac{\pi}{2^{k-1}} \Bigg(\sum_{j=1}^{\frac{k}{2}+1} \binom{n - k/2 - j}{k/2 - j}$$
$$(-1)^j * \Bigg(\sum_{S_i\subseteq[n],|S_i|=j} \bigoplus_{i\in S_i} x_i - \sum_{S_i\subseteq[n],|S_i|=n-j+1} \bigoplus_{i\in S_i} x_i \Bigg)\Bigg)$$



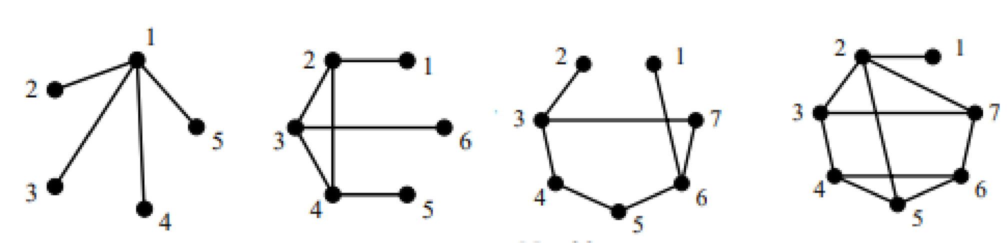
Conjecture 1. The number of qubits in a GHZ state necessary for the deterministic evaluation of a CSF C^k, with an n bit input string and a symmetric measurement assignment, scales as $\Omega(n^{k/2-1})$.

Asymptotic qubit count



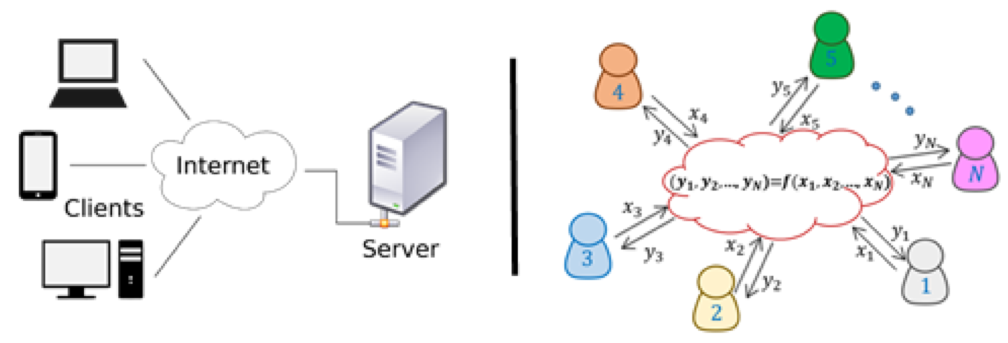
Extentions

$\text{NMQC}_{\oplus}$ computations could be extended to stabilizer states [3],



Applications

Design new protocols for secure delegated computations and secure multi-party computations [4, 5],



Acknowledgment

This work is financed by National Funds through the FCT - Fundação para a Ciência e a Tecnologia, I.P. (Portuguese Foundation for Science and Technology) within the project IBEX, with reference PTDC/CCI-COM/4280/2021, and the by the H2020-FETOPEN Grant PHOQUSING (GA no.:899544).

References

[1] Matty J Hoban, Earl T Campbell, Klearchos Loukopoulos, and Dan E Browne. Non-adaptive measurement-based quantum computation and multi-party Bell inequalities. *New Journal of Physics*, 13(2):23014, feb 2011.

[2] A Canteaut and M Videau. Symmetric Boolean functions. *IEEE Transactions on Information Theory*, 51(8):2791–2811, 2005.

[3] M Hein, J Eisert, and H J Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69(6):62311, jun 2004.

[4] Vedran Dunjko, Theodoros Kapourniotis, and Elham Kashefi. Quantum-Enhanced Secure Delegated Classical Computing. *Quantum Info. Comput.*, 16(1–2):61–86, jan 2016.

[5] Marco Clementi, Anna Pappa, Andreas Eckstein, Ian A Walmsley, Elham Kashefi, and Stefanie Barz. Classical multiparty computation using quantum resources. , 96(6):62317, dec 2017.