Efficient Classical Simulation of the DQC1 Circuit with Zero Discord

Shalin Jose[1], Akshay Kannan Sairam[2], and Anil Shaji[1,3]

[1]School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Maruthamala PO, Vithura, Kerala, 695551, India

[2]Department of Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru, Karnataka, 560012, India

[3]Center for High Performance Computing, Indian Institute of Science Education and Research Thiruvananthapuram, Maruthamala PO, Vithura, Kerala, 695551, India

A path for efficient classical simulation of the DQC1 circuit that estimates the trace of an implementable unitary under the zero discord condition [Phys. Rev. Lett. 105, 190502 (2010)] is presented. This result reinforces the status of non-classical correlations quantified by quantum discord and related measures as the key resource enabling exponential speedups in mixed state quantum computation.

1 Introduction

Identifying the resources that allow quantum algorithms to perform certain tasks significantly faster than the best known classical ones is an increasingly important question now that small scale quantum computers are already in operation [1, 2]. The framework of quantum information theory remains incomplete without pinpointing the quantum resources responsible for this computational advantage in each case. Within the paradigm of pure state quantum computation, multipartite entanglement that grows unboundedly with the input size was proven to be a necessary resource [3]. On the other hand, the Gottesman-Knill theorem [4] showed that highly entangled stabilizer states can be simulated efficiently using classical means and therefore cannot be a resource for quantum speedup. Just the presence of large quantities of entanglement is therefore not a sufficient condition for computational speedup and quite a bit of exploration has been done on whether particular quantum circuits can be simulated classically [5, 6, 7, 8].

Shalin Jose: shaliniiser16@iisertvm.ac.in

Certain models of mixed state quantum computation, conceived in the context of NMR based experiments [9], like the DQC1 model [10], can perform specific computations exponentially faster than classical analogues. Since little, or no, entanglement is generated in the state of the quantum computer during the computation in such models, entanglement alone cannot explain the speedup [11]. The key resource enabling the quantum advantage in mixed state quantum computation remains an open question, with the variety of quantum phenomena proposed as candidate resources growing with time [12, 13, 3]. A promising candidate is quantum discord [14, 15], which will be our focus here. Demonstrating the presence of discord in the DQC1 model was one major step in establishing it's relevance as the key quantum resource [16]. However, Dakic et al. [17] conjectured that DQC1 may provide an exponential speed-up even when discord is zero, suggesting that it may not be the pertinent resource. While this conjecture has received some attention in the past [18, 19, 20] no conclusive statement about it has been made.

In this paper, we show that the zero discord DQC1 computation discussed in [17] can be simulated efficiently by classical means provided the DQC1 computation itself is feasible in the sense that an efficient, gate-based implementation of the corresponding circuit is available. Central to the DQC1 model is a large unitary matrix acting on n qubits which we are assuming can be decomposed into elementary gates. The purpose of the computation is to find the trace of this unitary. To show that an efficient classical simulation of the computation is possible, we first derive a relation between the trace of the zero-discord case unitary and it's diagonal elements implying

that measurement of certain matrix elements contain information about the trace. Adding to this, we prove that, with a tractable principle branch Hamiltonian for the corresponding unitary, there is an efficient classical algorithm for finding these matrix elements leading to the trace. Our results restores the status of quantum discord as a viable quantifier of the key resource that enables exponential speedup in mixed state quantum computation.

2 DQC1 and Quantum Discord

The DQC1 circuit shown in fig (1) consists of a single qubit of non-zero purity in the state $(\mathbb{1} + \alpha Z)/2$, coupled to an n-qubit register in completely mixed state $\mathbb{1}_n/2^n$. In the following the three Pauli spin operators are denoted by X, Y and Z respectively. It can efficiently evaluate the normalized trace of the unitary matrix U_n that acts on the n-qubit fully mixed state. As mentioned above, it is assumed that U_n is implementable in poly(n) time. This model was first introduced by Knill and Laflamme [10] and has been shown to provide exponential speed up for other related problems as well [21, 22, 23, 24]. The output state of the circuit is given as,

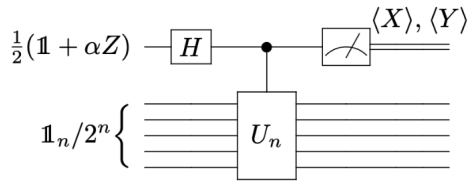

Figure 1: The DQC1 circuit for evaluating the normalized trace of the unitary U_n acting on the bottom register of n-qubits which are initialized in the fully mixed state.

$$\rho = \frac{1}{2^{n+1}}\left(\mathbb{1}_1 \otimes \mathbb{1}_n + \alpha|0\rangle\langle 1| \otimes U_n^\dagger + \alpha|1\rangle\langle 0| \otimes U_n\right)$$

The normalized trace of U_n, $\tau = \mathrm{Tr}(U_n)/2^n$, can be estimated by performing measurements of X and Y operators on the first qubit with $\tau_r = \langle\sigma_x\rangle/\alpha = \mathrm{Re}(\mathrm{Tr}(U_n)/2^n)$ and $\tau_i = \langle\sigma_y\rangle/\alpha = \mathrm{Im}(\mathrm{Tr}(U_n)/2^n)$. To estimate the trace to any fixed, desirable precision, a fixed number of repetitions of the measurements on top qubit are sufficient. This is in contrast to the resource requirement for any known classical method for evaluating the trace of the $2^n \times 2^n$ unitary U_n, all of which scale exponentially with n. The DQC1 circuit therefore achieves an exponential speedup but bipartite entanglement across the natural division between the top qubit and the rest is never generated during any step of the DQC1 algorithm. Across other bi-partitions some minimal amount of entanglement is present but it is bounded and is vanishingly small in the limit of $n \to \infty$ [25]. However finite amounts of non-classical correlations as quantified by quantum discord were observed to be present and it was proposed that such correlations may be the key quantum resource enabling the speed up [16].

2.1 Quantum Discord

For a composite quantum system AB with constituent sub-systems A and B described by the density matrices ρ_{AB}, ρ_A and ρ_B respectively, Quantum discord, $\mathcal{D}(B, A)$ captures the quantum correlations between A and B as the difference between total correlations and the purely classical correlations. Total correlations are quantified using the quantum mutual information given as,

$$\mathcal{I}(B : A) = H(\rho_B) + H(\rho_A) - H(\rho_{AB}) \qquad (1)$$

where $H(\rho) = -\mathrm{tr}(\rho \log \rho)$ is the von Neumann entropy of ρ. Classical correlations between the two subsystems are captured by,

$$\mathcal{J}(B : A) = H(B) - \tilde{H}(B|A) \qquad (2)$$

where $\tilde{H}(B|A) = \min_{\{\Pi_i^A\}} \sum_i p_i H(\rho_{B|i})$ with the minimisation of the conditional entropy $H(S|M) = \sum_i p_i H(\rho_{S|i})$ taken over all possible measurements on A. In practice, the measurements are limited to projective ones for computational simplicity. This leads to quantum discord given as,

$$\mathcal{D}(B, A) = \mathcal{I}(B : A) - \mathcal{J}(B : A)$$

We are specifically interested in the case where the state of the $n + 1$ qubits in the DQC1 circuit after the application of U_n has zero discord across top qubit versus rest division with measurements on the top qubit. In [17] it was shown that given a singular value decomposition of a state ρ_{AB} as $\sum_k c_k A_k \otimes B_k$ with A_k and B_k being operators belonging to the Hilbert spaces of A and B respectively, $\mathcal{D}(B : A)$ is zero if there exists a set of projection operators $\{\Pi_j^A\}$ such that $\sum_j \Pi_j^A A_k \Pi_j^A = A_k$. This also implies

$[A_j, A_k] = 0$. The DQC1 state after U_n can be written in the form,

$$\rho_{AB} = \frac{1}{2^{n+1}}\Big(\mathbb{1}_1 \otimes \mathbb{1}_n + \alpha X \otimes \frac{U_n + U_n^\dagger}{2} + \alpha Y \otimes \frac{U_n - U_n^\dagger}{2i}\Big), \quad (3)$$

where X, Y and Z are the three Pauli spin operators. This means that the DQC1 state after U_n is a zero discord state provided $U_n^\dagger = kU_n$ which is possible only if $U_n = e^{i\phi}O_n$ with $O_n^2 = \mathbb{1}$. In [17] it is conjectured that finding the trace of $U_n = e^{i\phi}O_n$ efficiently using classical means may not be possible for all such unitaries while DQC1 can still perform the task efficiently thereby implying that discord (which is zero) cannot be a quantifier for the key resource behind exponential quantum speedup.

The question of classical simulation of the zero discord DQC1 model is now reduced to trace estimation of the restricted class of unitary matrices with $U_n^\dagger = kU_n$. We show in the following that U_n is sufficiently restricted with O_n being involutory, that it is possible to estimate its trace classically in an efficient manner as long as U_n is also assumed to be efficiently implementable as it should be for any realistic DQC1 circuit.

3 Trace Estimation

Estimation of the global phase of U, if any, will be discussed separately. First we focus on finding the magnitude of the trace of U setting $\phi = 0$. Note that we have dropped the subscript n from the operators U and O in the following for simplifying the notation. The Hermitian Unitary matrix O has $\det(O) = \pm 1$ and eigenvalues $\lambda_j = \pm 1$ so that,

$$\mathrm{Tr[O]} = N_+ - N_-, \quad (4)$$

where N_+ and N_- are the number of eigenvalues of O equal to $+1$ and -1 respectively. The Hermitian unitary O can always be written as $O = V^\dagger DV$, where D is a diagonal matrix with $+1$ and -1 as entries while V is a Haar-random unitary. Since the Haar measure is invariant under permutation of rows and columns [26, p. 138], we assume that D has been rearranged through a suitable permutation of rows and columns with all the -1 entries clubbed together at the top so that we can write it in the form $D = \mathrm{diag}[-1, -1, .., 1, 1]$. With this rearrangement, the q^{th} diagonal element of O is,

$$O_{qq} = \sum_k |v_{qk}|^2 d_k = \sum_{k>n_{-1}} |v_{qk}|^2 - \sum_{k\le n_{-1}} |v_{qk}|^2, \quad (5)$$

where $d_k \in [1, -1]$ denote the diagonal entries of D and $v_{qk} = \langle q|V|k\rangle$ with $|q\rangle$ and $|k\rangle$ being the (permuted) computational basis vectors. We now

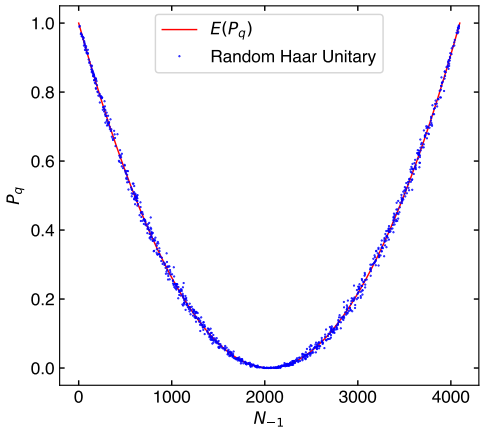

Figure 2: Probability, P_q of measuring $|00\cdots00\rangle$ at the output of a randomly generated 12-qubit zero discord unitary, when $|00\cdots0\rangle$ is the input state is plotted against N_-. Also shown as the solid line (red) is the analytic expression for the expectation value of P_q from Eq. (9). We see that the numerically obtained points are distributed around the expected value with small variance.

consider the expectation value of O_{qq} with respect to the Haar probability measure μ_N over the unitary group $\mathcal{U}_N$ with $N = 2^n$. For any measurable function f over $\mathcal{U}_N$, the expectation value is defined as $\mathbb{E}(f) = \int_{V\in\mathcal{V}_N} f(V)d\mu_N(V)$. The following results from Proposition 4.2.3 of [26] applies to any Haar-random unitary:

$$\begin{aligned} \mathbb{E}(|v_{ij}|^2) &= \frac{1}{N}, \\ \mathbb{E}(|v_{ij}|^4) &= \frac{2}{N(N+1)}, \\ \mathbb{E}(|v_{ij}|^2|v_{ij'}|^2) &= \frac{1}{N(N+1)}, \quad (j \neq j'). \end{aligned} \quad (6)$$

Using the equations above, we obtain,

$$\mathbb{E}(O_{qq}) = \frac{N_+ - N_-}{N}, \quad (7)$$

which is nothing but the normalised trace of O. If any computational basis state $|q\rangle$ is inserted as the input into the bottom half of the zero-discord

DQC1 circuit, then the probability of obtaining the same state as output is given by,

$$\begin{aligned} P_q =& |\langle q|U_N|q\rangle|^2 = O_{qq}^2 \\ =& \Big(\sum_k |u_{qk}|^2 d_k\Big)\Big(\sum_l |u_{ql}|^2 d_l\Big) \\ =& \sum_{k,l\le N_-} |v_{qk}|^2|v_{ql}|^2 - \sum_{k>N_-,l\le N_-} |v_{qk}|^2|v_{ql}|^2 \\ & - \sum_{l>N_-,k\le N_-} |v_{qk}|^2|v_{ql}|^2 + \sum_{k,l>N_-} |v_{qk}|^2|v_{ql}|^2 \end{aligned} \tag{8}$$

Using Eq. (6) we obtain,

$$\mathbb{E}(P_q) = \mathbb{E}(O_{qq}^2) = \frac{1}{N+1} + \frac{(N_+ - N_-)^2}{N(N+1)}. \tag{9}$$

From Eqs. (5), (7), (8) and (9) we observe the following about the zero discord case. The magnitude, apart from an overall phase, of the normalized trace of U_N can be obtained from $\mathbb{E}(O_{qq})$ only and $O_{qq}^2 = P_q$ is an observable quantity. Furthermore, with respect to the Haar measure, O_{qq} is a random variable distributed with variance, $\Delta(O_{qq}) = \mathbb{E}(O_{qq}^2) - [\mathbb{E}(O_{qq})]^2 \sim 1/N$, for large N. The means that when the number of qubits in the bottom register of DQC1 circuit is moderately big so that $N = 2^n$ is large, the estimate of O_{qq} obtained from P_q is equal to $\mathcal{E}(O_{qq})$ with very high confidence level. We can see this from Fig. 2, where the probability of obtaining the state $|00\cdots00\rangle$ at the output end of the DQC1 circuit, corresponding to the same state as input, is plotted as a function of N_- for randomly generated 8-qubit ($N = 256$) zero discord unitaries. Also shown in the figure is $\mathbb{E}(P_{00\cdots00})$ from Eq. (9) written as a function of only N_- using $N_+ = N - N_-$.

In the discussion above we require the unitary V in $V^\dagger DV$ to be Haar random for Eq. (9) to hold and for P_q to converge to a parabola with respect N_{-1} as in Fig. 2. This raises the following question. What if the the DQC1 unitary is highly structured and from inspection itself it is suspected that V is not a typical Haar random unitary. This question can be addressed by noting that changing V does not change the eigenvalues of O or the trace of O. Furthermore the $V^\dagger DV$ form allows us to pad the given implementation of the unitary with layers of gates on either side with corresponding layers being adjoint of each other without changing the $V^\dagger DV$ form. By randomly choosing the gates in these padding layers we can make the unitary sandwiching D effectively Haar-random. Since we are adding only finite number of layers, the padding does not increase the computational complexity of our classical simulation. In order to demonstrate that such a procedure can work, we start from a randomly chosen D and see the behavior of P_q when V is built-up in stages using randomly generated circuit layers consisting of gates from a universal gate. We denote the number of layers in V with m. We see that for small m, the unitary V is more structured and the corresponding P_q has a large scatter around the parabolic

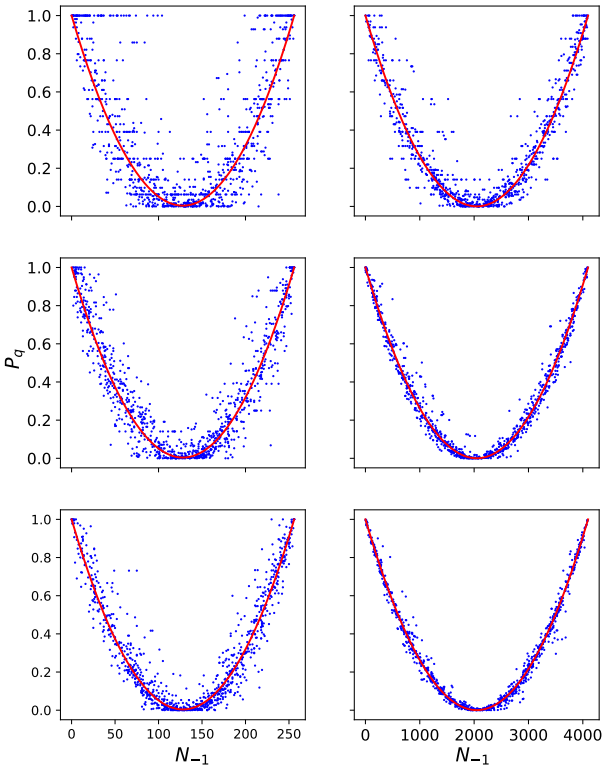

Figure 3: Probability, P_q of measuring $|00\cdots00\rangle$ at the output of a randomly generated n-qubit zero discord unitary, with $|00\cdots0\rangle$ as the input state, plotted against N_{-1}. The solid line (red) is the analytical expression for the expectation value of P_q from Eq. (9) while the dots (Blue) are the numerical obtained data points. For the plots on the left, $n = 8$ and for those on the right, $n = 12$. The unitary is of the form $V^\dagger DV$ where V consists of m layers, each constructed using sets of commuting gates randomly from the Clifford + T gate set. The first, second and third rows correspond to $m = 4$, $m = 8$ and $m = 12$ layers respectively. We see that as m increases the convergence of the values to the expected parabolic curve improves. Further, the convergence is better for larger N for a given m.

curve expected from Haar-random V. With the addition of more layers the probability converges to the expected parabola as observed in Fig. 3. Comparing similar computations for the 8-qubit and 12-qubit cases, we also observe that a higher number of qubits require fewer layers for better convergence. This behavior becomes useful in the next section where the BCH formula is applied to find an effective Hamiltonian. With increasing number of qubits, application of the BCH formula become computationally challenging but some of the difficulty can be offset if the number of layers required to construct V is smaller. Note that, so far, in the numerical computations considered, the matrix D is a $2^N \times 2^N$ matrix with randomly placed 1 and -1 values along the diagonal and need not always have an efficient implementation as a circuit consisting of one and two qubit gates (see Appendix A).

4 Classical Simulation

We assume that the input unitary U we are considering in the zero-discord case be describable classically as a quantum circuit with Poly(n) elementary gates and not as a matrix representation of U [19]. If the DQC1 circuit itself is not efficiently implementable as a quantum computation then the question whether it can perform a task using exponentially faster than best known classical circuit is ill-defined. Resource counting in such scenarios must take into consideration the exponential cost in terms of time and energy required to realize all the gates required for implementing the circuit and this cost will grow exponentially if the circuit is not efficiently implementable. The celebrated Solovay-Kitaev theorem informs us that even if a specific unitary is not efficiently implementable, it can always be approximated to any desired accuracy with those that can be implemented efficiently [27, 28] and so we restrict our attention to only such implementable unitaries. This means that even if one happens to be interested in a DQC1 computation that involves a zero-discord unitary that is not efficiently implementable then one can approximate the computation using a suitable unitary that is implementable. Operationally this implies that restricting our attention only to implementable zero-discord unitaries in the following can be done without loss of generality.

For implementable unitaries we assume that the quantum circuit using any preferred universal set of quantum gates [29, 30] is available. Multiplying the gates together as matrices to find the unitary carries exponential computational cost and cannot be done. However our objective is served if a few of the diagonal entries of the unitary can be sampled efficiently. Using these values we can compute the sample mean $\langle U_{qq}^2 \rangle = \langle O_{qq}^2 \rangle \sim P_q$ and use it as an estimate of P_q. As can be seen from 2 if we know the value of P_q which is on the y-axis, we can find N_{-1} from the x-axis. The two possible values of N_{-1} corresponding to each P_q give the normalized trace of U up to an overall factor of -1 which can further be disambiguated using the available circuit implementation of U. We outline below how a few diagonal elements of U can be sampled efficiently using classical means. The method we propose does have one caveat though, which we will point out as we go along.

The first step, if not already done, is to rearrange the gates of the given circuit implementation of U into groups of mutually commuting gates acting simultaneously on the n-qubit register. For concreteness we further assume that U is implemented using the universal gate set (Clifford + T) consisting of the three gates,

$$\mathrm{Hd} = e^{i\frac{\pi}{2}\left[\mathbb{1} - \frac{X+Z}{\sqrt{2}}\right]},\ T = e^{i\frac{\pi}{8}[\mathbb{1}-Z]},$$
$$\mathrm{CNOT} = e^{i\frac{\pi}{4}[\mathbb{1}-Z]\otimes[\mathbb{1}-X]},$$

where Hd denotes the Hadamard gate. Note that each of these gates can be written in the form $e^{ih_k^{(j)}}$ where $h_k^{(j)}$ are one- or two-local strings of Pauli operators multiplied by appropriate numerical coefficients. After the grouping the circuit has $m+1$ layers with each layer containing all the gates that can act simultaneously. Out of these one layer would correspond to the overall global phase with $e^{i\phi\mathbb{1}}$ as the gate on every one of the qubits. We can read off the overall phase from this layer and focus on the remaining m layers. The unitary transformation corresponding to the j^{th} layer of the circuit can be written as $O^{(j)} = e^{i\sum_k h_k^{(j)}} \equiv e^{iH^{(j)}}$, where $H^{(j)}$ are sums of products of Pauli operators with each $H^{(j)}$ having a Poly(n) terms.

The DQC1 unitary, O (modulo the global phase) can be written in terms of its circuit rep-

resentation as

$$O = \prod_{j=0}^{m-1} O^{(m-j)} = \prod_{j=0}^{m-1} e^{iH^{(m-j)}} \equiv e^{iH}, \quad (10)$$

The operator H is in general difficult to find and the problem of mapping a given quantum circuit to a local Hamiltonian is quite well studied [31, 32]. However, here we have the additional advantage that O, is an involution (Hermitian) with $O^2 = \mathbb{1}$. The operator H has to be constructed from $H^{(j)}$ through a judicious application of the Baker-Campbell-Hausdorff (BCH) formula [33]. Details of the convergence of the BCH expansion for the type of U considered and its numerical exploration is included in Appendix A. The operator H is again a sum of Pauli strings. We can now identify $O = V^\dagger D V = e^{iH}$ so that

$$D = V e^{iH} V^\dagger = e^{iVHV^\dagger}, \quad (11)$$

is a diagonal matrix with $+1$ and -1 as entries. The operator $VHV^\dagger$ therefore can be considered as a diagonal matrix with 0 and π appearing as entries wherever $+1$ and -1 appears along the diagonal of D respectively. Hence we have,

$$D = -\frac{2}{\pi} VHV^\dagger + \mathbb{1}^{\otimes n}, \quad (12)$$

which leads to,

$$O = V^\dagger D V = -\frac{2}{\pi} H + \mathbb{1}^{\otimes n}. \quad (13)$$

The matrix O is essentially the sum of the the same set of Poly(n) one- and two-local Pauli strings appearing in the Hamiltonian scaled by $-2/\pi$. We now have to compute a fixed number of diagonal elements of O to find the normalized trace of U as discussed earlier. Since H is sum of Pauli strings, each of which are also typically sparse matrices [34, 35], this involves computing the diagonal elements at a fixed position of each these terms essentially just by inspection of the Pauli strings that are involved. As the number of terms in H are Poly(n) albeit with a large multiplicative factor, computing a fixed number of elements O_{qq} can be done classically in an efficient manner [36], thereby completing our construction. In Appendix A.3, we have tested the algorithm and show that efficient classical computation of the trace of randomly generated zero-discord unitaries acting on n qubits is possible for $n = 15$ and $n = 18$. An important caveat in our discussion is that since $H \sim \log O$, H is not, in general single valued. The key relationship in Eq. (13) holds only if H belongs to the principal branch of the $\log O$ function. The construction of H from the circuit decomposition of O has to be such that at each step this condition is maintained. While it appears to be possible to do this in the case of the types of zero-discord unitaries we have numerically explored with number of qubits ranging up to 20, whether it can be done in general without having to evaluate $VHV^\dagger$ and looking at its 2^n diagonal elements remains an open question beyond the scope of the present work.

4.1 Schmidt Rank

In [37], the Schmidt rank of the final state of the DQC1 circuit for a random implementable unitary was shown to scale exponentially as $2^{n/2}$ proving that classical simulation of the state using the approach in [5] is not possible. For the implementable Hermitian unitaries we consider, the action of the unitary on a pure state $|\psi\rangle$ of Schmidt rank 1 is given by Eq. (13) as essentially left multiplication by a sum of Pauli operators with degree of locality bounded by the order of the BCH truncation. The Lieb-Robinson bound [38] tells us that each of the terms in the sum can increase the Schmidt rank of the state only by a fixed amount that is independent of n and dependent only of the degree of locality of the operator. Since the number of terms in the sum is bounded by Poly(n) we find that Schmidt rank of the output state of the zero discord DQC1 state is also bounded by Poly(n) indicating that methods from [5] may also be adopted to simulate the DQC1 circuit in this case.

5 Conclusions

Equations (7) and (13) captures the key reasons that allow for an efficient classical simulation of the zero discord DQC1 circuit when U is implementable. The first reason was that the magnitude of the normalized trace can be found from any diagonal element of O. The arguments that lead to Eq. (7) can be generalized even when U has more than two distinct eigenvalues and it can generate discord in the DQC1 circuit. However,

we note that the convergence of O_{qq} to $\mathbb{E}(O_{qq})$ is better if the number of distinct eigenvalues of U are less in number. This is because even if we are nominally replacing $|v_{qk}|^2$ with $\mathbb{E}(|v_{qk}|^2) = 1/N$ to get Eq. (7), what we are actually doing is replacing $\sum_k |v_{qk}|^2$ with $N_\pm/N$ which is much better approximation when $N_\pm \gg 1$. This effect can be observed in Fig. 2 where the agreement between the theoretical curve and numerically obtained data points for $N = 4096$ is better in the middle ($N_\pm \sim 2048$) and at the ends where either N_+ or N_- dominates. In the limit of the number of distinct eigenvalues of U becoming equal to N, no such additional averaging will be possible and O_{qq} can become a good estimate of its expectation value only by virtue of the law of large numbers which applies only for very large N. In comparison, the steps that lead to Eq. (12) and Eq. (13) are not possible if U has more than two distinct eigenvalues. This means that the techniques presented here cannot be extended to do efficient classical simulations of DQC1 circuit when U generates discord between the fully mixed quantum register and the top qubit.

In conclusion, we have proposed a classical algorithm using which we can efficiently estimate the trace of an implementable zero-discord unitary, in effect, reproducing the statistics of a zero discord DQC1 circuit using Poly(n) classical resources. We have shown that the conjecture made in Ref. [17] that the zero discord DQC1 case may furnish an argument against considering quantum discord as a key resource behind mixed state quantum computing is not true when U is implementable. There remains one caveat to the method we presented that needs to be fully addressed. Our results do not furnish a clinching argument in favor of considering quantum discord and other related measures which quantify nonclassical correlations other than entanglement in mixed states as the key resource either but it considerably strengthens the argument and more importantly, restores quantum discord as one of the main contenders for such consideration.

Acknowledgments

This work was supported by the the Department of Science and Technology, Government of India through a grant under the National Quantum Mission (Hub for Quantum Computation) and the Ministry of Education through the STARS grant MoE-STARS/STARS-2/2023-0809. The authors would also like to thank John George Francis for useful comments on the computational aspects of this work.

References

[1] Frank Arute et al. “Quantum supremacy using a programmable superconducting processor”. Nature **574**, 505–510 (2019).

[2] Davide Castelvecchi. “Ibm releases first-ever 1,000-qubit quantum chip”. Nature **624**, 238 (2023).

[3] Richard Jozsa and Noah Linden. “On the role of entanglement in quantum-computational speed-up”. Proc. Roy. Soc. London. Ser. A: Math. Phys. and Engg. Sci. **459**, 2011–2032 (2003).

[4] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. Phys. Rev. A **70**, 052328 (2004).

[5] Guifré Vidal. “Efficient classical simulation of slightly entangled quantum computations”. Phys. Rev. Lett. **91**, 147902 (2003).

[6] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. “Simulation of quantum circuits by low-rank stabilizer decompositions”. Quantum **3**, 181 (2019).

[7] Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. “Estimating outcome probabilities of quantum circuits using quasiprobabilities”. Phys. Rev. Lett. **115**, 070501 (2015).

[8] Andrew Jackson, Theodoros Kapourniotis, and Animesh Datta. “Partition-function estimation: Quantum and quantum-inspired algorithms”. Phys. Rev. A **107**, 012421 (2023).

[9] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. “Separability of very noisy mixed states and implications for nmr quantum computing”. Phys. Rev. Lett. **83**, 1054–1057 (1999).

[10] E. Knill and R. Laflamme. “Power of one bit of quantum information”. Phys. Rev. Lett. **81**, 5672–5675 (1998).

[11] David A. Meyer. "Sophisticated quantum search without entanglement". Phys. Rev. Lett. **85**, 2014–2017 (2000).

[12] Juan Bermejo-Vega, Nicolas Delfosse, Dan E Browne, Cihan Okay, and Robert Raussendorf. "Contextuality as a resource for models of quantum computation with qubits". Phys. Rev. Lett. **119**, 120505 (2017).

[13] Victor Veitch, Christopher Ferrie, David Gross, and Joseph Emerson. "Negative quasi-probability as a resource for quantum computation". New J. Phys. **14**, 113011 (2012).

[14] Harold Ollivier and Wojciech H. Zurek. "Quantum discord: A measure of the quantumness of correlations". Phys. Rev. Lett. **88**, 017901 (2001).

[15] Leah Henderson and Vlatko Vedral. "Classical, quantum and total correlations". J. Phys. A: Math. Gen. **34**, 6899 (2001).

[16] Animesh Datta, Anil Shaji, and Carlton M Caves. "Quantum discord and the power of one qubit". Phys. Rev. Lett. **100**, 050502 (2008).

[17] Borivoje Dakić, Vlatko Vedral, and Časlav Brukner. "Necessary and sufficient condition for nonzero quantum discord". Phys. Rev. Lett. **105**, 190502 (2010).

[18] Animesh Datta and Anil Shaji. "Quantum discord and quantum computing—an appraisal". Int. J. Quant. Info. **9**, 1787–1805 (2011).

[19] Jiajun Ma, Benjamin Yadin, Davide Girolami, Vlatko Vedral, and Mile Gu. "Converting coherence to quantum correlations". Phys. Rev. Lett. **116**, 160407 (2016).

[20] Bryan Eastin. "Simulating concordant computations" (2010). arXiv:1006.4402.

[21] David Poulin, Robin Blume-Kohout, Raymond Laflamme, and Harold Ollivier. "Exponential speedup with a single bit of quantum information: Measuring the average fidelity decay". Phys. Rev. Lett. **92**, 177906 (2004).

[22] Emanuel Knill and Raymond Laflamme. "Quantum computing and quadratically signed weight enumerators". Inf. Process. Lett. **79**, 173–179 (2001).

[23] Peter W. Shor and Stephen P. Jordan. "Estimating jones polynomials is a complete problem for one clean qubit". Quant. Info. Comput. **8**, 681–714 (2008).

[24] Sergio Boixo and Rolando D Somma. "Parameter estimation with mixed-state quantum computation". Phys. Rev. A **77**, 052320 (2008).

[25] Animesh Datta, Steven T. Flammia, and Carlton M. Caves. "Entanglement and the power of one qubit". Phys. Rev. A **72**, 042316 (2005).

[26] Fumio Hiai and Dénes Petz. "The semicircle law, free random variables and entropy". Number 77 in Mathematical Surveys and Monographs. American Mathematical Society. (2000).

[27] A Yu Kitaev. "Quantum computations: algorithms and error correction". Russian Math. Surveys **52**, 1191 (1997).

[28] Christopher M. Dawson and Michael A. Nielsen. "The solovay-kitaev algorithm" (2005). arXiv:quant-ph/0505030.

[29] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. "Elementary gates for quantum computation". Phys. Rev. A **52**, 3457–3467 (1995).

[30] Adriano Barenco. "A universal two-bit gate for quantum computation". Proc. R. Soc. Lond. **449:**, 679—-683 (1995).

[31] Alastair Kay. "Perfect, efficient, state transfer and its application as a constructive tool". Int. J. Quant. Info. **08**, 641–676 (2010).

[32] Daniel Nagaj. "Universal two-body-hamiltonian quantum computing". Phys. Rev. A **85**, 32330 (2012).

[33] Rüdiger Achilles and Andrea Bonfiglioli. "The early proofs of the theorem of campbell, baker, hausdorff, and dynkin". Archive for History of Exact Sciences **66**, 295–358 (2012).

[34] Dorit Aharonov and Amnon Ta-Shma. "Adiabatic quantum state generation and statistical zero knowledge". In Proceedings of the

Thirty-Fifth Annual ACM Symposium on Theory of Computing. Page 20–29. STOC '03New York, NY, USA (2003). Association for Computing Machinery.

[35] Seth Lloyd. "Universal quantum simulators". Science **273**, 1073–1078 (1996).

[36] Maarten Van Den Nest. "Simulating quantum computers with probabilistic methods". Quantum Info. Comput. **11**, 784–812 (2011).

[37] Animesh Datta and Guifre Vidal. "Role of entanglement and correlations in mixed-state quantum computation". Phys. Rev. A **75**, 042310 (2007).

[38] Elliott H. Lieb and Derek W. Robinson. "The finite group velocity of quantum spin systems". Comm. Math. Phys. **28**, 251–257 (1972).

[39] Mona Arabzadeh, Mahboobeh Houshmand, Mehdi Sedighi, and Morteza Saheb Zamani. "Quantum-logic synthesis of hermitian gates". J. Emerg. Technol. Comput. Syst.**12** (2016).

[40] Mahboobeh Houshmand, Morteza Saheb Zamani, Mehdi Sedighi, and Mona Arabzadeh. "Decomposition of diagonal hermitian quantum gates using multiple-controlled pauli z gates". J. Emerg. Technol. Comput. Syst.**11** (2015).

[41] Shihao Zhang, Junda Wu, and Lvzhou Li. "Characterization, synthesis, and optimization of quantum circuits over multiple-control Z-rotation gates: A systematic study". Phys. Rev. A **108**, 022603 (2023).

[42] Jonathan Welch, Alex Bocharov, and Krysta M. Svore. "Efficient approximation of diagonal unitaries over the clifford+t basis". Quantum Info. Comput. **16**, 87–104 (2016).

[43] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information: 10th anniversary edition". Cambridge University Press. Cambridge (2010).

[44] Ken M. Nakanishi, Takahiko Satoh, and Synge Todo. "Decompositions of multiple controlled-z gates on various qubit-coupling graphs". Phys. Rev. A **110**, 012604 (2024).

[45] Nicolas Loizeau, J. Clayton Peacock, and Dries Sels. "Codebase release 1.5 for PauliStrings.jl". SciPost Phys. Codebases-Pages 54–r1.5 (2025).

A Computing H

The results of our numerical exploration of repeated applications of the BCH formula for obtaining H as a sum of a large, but Poly(n) number of Pauli strings is summarized below. The first challenge is to identify or generate efficiently implementable unitaries with corresponding gate-based quantum circuits which have only ± 1 as its eigenvalues. We outline a means of addressing this problem and following that the convergence of the BCH based approach and the number of Pauli strings in H are discussed.

A.1 Circuit Implementation for a Hermitian Unitary

The task of generating random Hermitian Unitary Circuits is a non-trivial problem. To understand why, we look at the decomposition of a Hermitian Unitary provided in [39]. The Unitary is broken into three main parts by writing the unitary as $U = WDW^{\dagger}$. The central part of the circuit is the circuit decomposition of the diagonal D and it is sandwiched by rotation gates and their corresponding conjugate gates on either side. The complexity of constructing a general diagonal Hermitian unitary scales exponentially in n as shown in [40, 41], where the well-known decomposition of multi-control C^kZ gates into $O(n^2)$ elementary gates [29] is used. But this method [29] relies heavily on performing arbitrary single-qubit rotations for the exact decomposition which is challenging to implement experimentally. It may be noted that fault tolerant implementation of single-qubit rotations are typically not possible as well [42]. To switch to a universal gate set such as the Clifford + T gate set, requires applying the Solavey Kiteav Theorem and for multi-controlled Z rotations, C^kZ, exact decomposition is only known up to $k = 2$ [43, 44]. Due to this, we choose to construct our circuit for the diagonal part D using randomly placed Z, CZ and CCZ gates only. On the left side of these gates we place m layers of gates with each layer consisting of a collection of mutually commuting gates chosen from a universal gate set like Clifford + T. On the right side, there are again m layers placed in reverse order with each layer consisting of the conjugates of the gates on the corresponding layer on the right side. Though this need not encompass the entire set of Hermi-

tian Unitaries that are implementable efficiently on a quantum computer, we use this subset of Hermitian Unitaries to explore the convergence of repeated application of the BCH formula and the number of terms in H.

A.2 Baker-Campbell-Hausdorff Convergence

We are interested in answering the question of how one arrives at the Hamiltonian, H of the full Unitary efficiently, given the gate decomposition of the circuit. If that step can be achieved we can apply Eq. (10) from the main text and calculate the normalized trace for a given circuit implementation of a Hermitian Unitary. To do this, we apply the BCH formulae to the set of random Hermitian circuits generated as described in the previous section and estimate how closely the Hamiltonian and the corresponding unitary approximation converges to the required unitary. The sandwich structure of the circuit, allows us to use the following form for the BCH formula with the pattern of coefficients appearing it leading to easier computations:

$$e^{-sA}e^{B}e^{sA} = \exp\left(B + s[A,B] + \frac{s^2}{2!}[A,[A,B]] + \frac{s^3}{3!}[A,[A,[A,B]]] + \dots\right) \tag{14}$$

The gates that are part of the diagonal matrix at the center all commute with one another and they are contained in the e^B operator. The above expansion is repeatedly applied for each layer with truncation up to the specified order to estimate the final approximate Hamiltonian $H_{(1)}$ of the circuit. We note that the eigenvalues of $H_{(1)}$ are equal to 0 or π only modulo 2π. We discuss the special case where the eigenvalues are set to 0 or π separately. The L_2 norm of the difference between the exact U and the approximate Unitary, given by $\epsilon_u = |U - \exp iH_{(1)}|$, is plotted in Fig.(3) by varying different parameters such as n, m and the order of truncation. This is done for gate sets, Clifford + T and Toffoli + Hadamard. We find that the convergence to the expected Unitary varies only slightly with the gate set but they exhibit similar patterns. We also see that it converges around the truncation order 60 for $n = 8, 10$ for almost all the sampled circuits while for $n = 12$ it converges for most

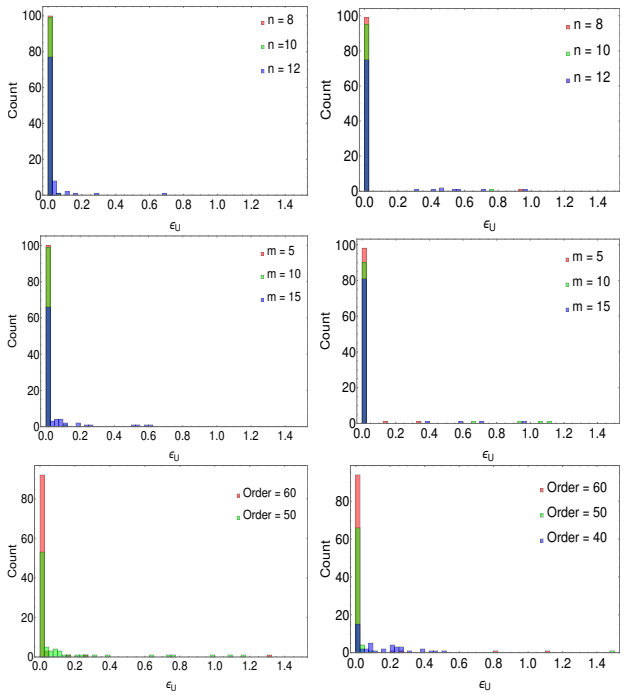

Figure 4: The L_2 norm of the difference between the exact unitary and the unitary constructed from a Hamiltonian obtained using the BCH formula is plotted. For the plots on the left-hand side the expansion of the unitary was in terms of the gate set (CNOT + H + T) and on the right-hand side it was expanded using (Toffoli + H). The first, second and third rows shows convergence of the L_2 norm under BCH expansion for varying numbers of qubits, different number of layers in the circuit implementation of the unitary and the order of BCH truncation respectively. The sample size is 100 for each plot and the order of the BCH truncation for the first two rows is 60.

of the samples. We can expect it to converge for higher values of n though we could only go up to 12 qubits as the computation gets heavy. The Unitary is also seen to converge faster for fewer number of layers as is expected.

A.3 Classical Simulation

The algorithm proposed was tested for a few randomly generated Hermitian unitary circuits using the method proposed in Appendix A.2. For generating zero-discord unitaries required for verifying the algorithm, we have reverse-calculated the principle branch Hamiltonian using Eq. (12) for a randomly selected sequence of diagonal gates that constitute D. The BCH expansion was then employed for each additional layer of gates (which are part of V and $V^\dagger$ respectively) on either side. Fig. 5 shows a comparison between the exact and

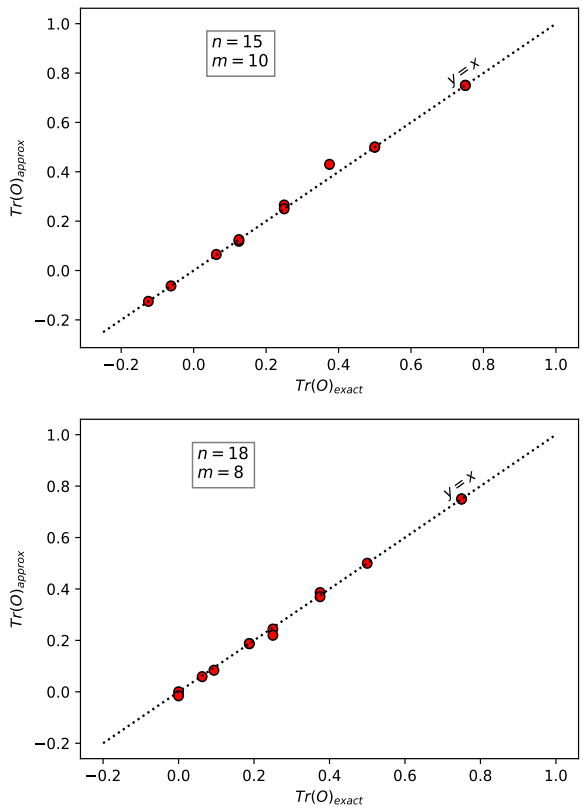

Figure 5: Normalized trace for randomly generated hermitian unitary circuits for $n = 15$ and 18 with $m = 10$ and 8 respectively is computed using the classical simulation algorithm and plotted (red dots). For each data point, 500 randomly selected diagonal elements of the unitary are average over. The data points have substantial overlap since many of the randomly generated unitaries have the same trace. The dotted line denotes the actual values of the traces and we see that the algorithm performs very well.

approximate trace values for $n = 15$ and $n = 18$ for $m = 10$ and $m = 8$ respectively. The averaging is performed on 500 randomly generated D matrices. The computation was done in Julia using the PauliStrings.jl [45]. Since the D matrices were constructed using a limited set of gates, namely, Z, CZ and CCZ, many of the matrices generated had the same trace. Similar calculations were done for $n = 20$ whose results are not included, since we were able to perform only up to $m = 6$ in most cases. We observe that complexity of calculating the effective Hamiltonian via the BCH expansion increases with the number of layers m on either side of the center block. This is because, although the number of Pauli terms in the effective Hamiltonian is Poly(n), the polynomial could be of a high order depending on the layers being applied.

A.4 Scaling of number of terms of H

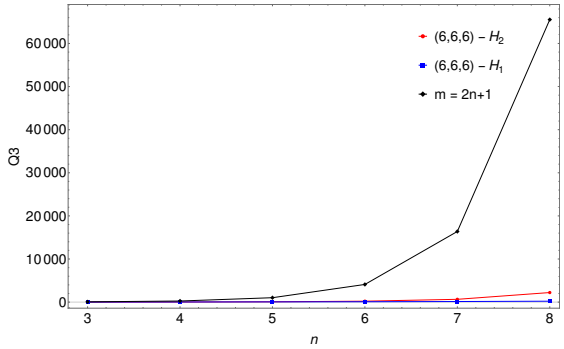

Figure 6: The third Quartrile $(Q3)$ of the distribution of the number of Pauli strings in the Hamiltonian decomposition as a function of the number of qubits n. H_1 and H_2 are blue and red lines plotted for $(n_{ccz}, n_{cz}, n_z) = (6, 6, 6)$ respectively while the black line indicates the case of random circuit Hamiltonians. The sample size is 1000 for each n.

The classical trace estimation method outlined here depends on the number of Pauli strings that make up the Hamiltonian operator and it would fail if the number scales exponentially in n. Therefore, we obtain numerical estimates for the number of terms in the Hamiltonian operators $H_{(1)}$ and $H_{(2)}$ corresponding to the same Hermitian unitary given in Fig. 5. Here, $H_{(2)}$ is the Hamiltonian that satisfies Eq. (9) of the main text and has eigenvalues 0 or π only. Therefore, $H_{(2)}$ also reflects the growth of the number of terms in O as given in Eq. (10) of the main text. A comparison is shown between Hermitian circuits and randomly generated circuits in Fig. 6. The Hermitian circuit is constructed as described above. For random circuits, we have fixed $m = 2n + 1$ layers and decomposed its matrix logarithm into a Pauli string summation. We have sampled 1000 circuits for each n. Although we cannot exactly determine the order of the growth rate of the number of terms in $H_{(2)}$ for Hermitian circuits, it is much slower compared to the number of terms in the randomly generated circuits which grow as $O(4^n)$. $H_{(1)}$ is also plotted for comparison, as it is known to scale as a polynomial in n by the nature of its construction. This would suggest that the Hamiltonian description of the Hermitian unitary operators and therefore the output state of such unitaries can be computed classically using far fewer resources with increasing number of qubits compared to a randomly generated unitary and its corresponding Hamiltonian.