Article:
Frembs, M., Roberts, S., Campbell, E.T. et al. (2023) Hierarchies of resources for measurement-based quantum computation. New Journal of Physics, 25 (013002). ISSN: 1367-2630

https://doi.org/10.1088/1367-2630/acaee2

Hierarchies of resources for measurement-based quantum computation

IOP Publishing New J. Phys. 25 (2023) 013002 https://doi.org/10.1088/1367-2630/acaee2

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
20 April 2022

REVISED
7 November 2022

ACCEPTED FOR PUBLICATION
28 December 2022

PUBLISHED
9 January 2023

PAPER

Hierarchies of resources for measurement-based quantum computation

Markus Frembs[1,*], **Sam Roberts**[2], **Earl T Campbell**[3,4] and **Stephen D Bartlett**[2]

[1] Centre for Quantum Dynamics, Griffith University, Gold Coast, QLD 4222, Australia
[2] Centre for Engineered Quantum Systems, School of Physics, The University of Sydney, Sydney, NSW 2006, Australia
[3] Department of Physics & Astronomy, University of Sheffield, Sheffield S3 7RH, United Kingdom
[4] Riverlane, Cambridge CB2 3BZ, United Kingdom
[*] Author to whom any correspondence should be addressed.

E-mail: m.frembs@griffith.edu.au

Keywords: measurement-based quantum computation, contextuality, nonlocality, Clifford hierarchy

Abstract

For certain restricted computational tasks, quantum mechanics provides a provable advantage over any possible classical implementation. Several of these results have been proven using the framework of measurement-based quantum computation (MBQC), where nonlocality and more generally contextuality have been identified as necessary resources for certain quantum computations. Here, we consider the computational power of MBQC in more detail by refining its resource requirements, both on the allowed operations and the number of accessible qubits. More precisely, we identify which Boolean functions can be computed in non-adaptive MBQC, with local operations contained within a finite level in the Clifford hierarchy. Moreover, for non-adaptive MBQC restricted to certain subtheories such as stabiliser MBQC, we compute the minimal number of qubits required to compute a given Boolean function. Our results point towards hierarchies of resources that more sharply characterise the power of MBQC beyond the binary of contextuality vs non-contextuality.

1. Introduction

Quantum computation promises many advantages over classical computations, including the ability to efficiently solve certain problems, such as factoring, where no efficient classical algorithms are currently known. What drives this quantum advantage?

Contextuality offers a potential answer to this question, as it has been found to be an important resource for quantum computation in a variety of settings [1–13]. Roughly speaking, contextuality is the impossibility of assigning pre-determined outcomes to all potential measurements of a quantum system in a way that is independent of other, simultaneously performed measurements [14]. In the case of locally performed measurements on a composite system as considered in this work, contextuality reduces to nonlocality. Contextuality is a common notion of non-classicality. Notably, contextuality plays a central role in a recent seminal result showing a provable quantum advantage for a class of shallow quantum circuits over their classical counterparts [15] (later extended to the noisy setting in [16]). While the class of problems solvable with such circuits is not motivated by practical applications, it provides a proof of principle that quantum advantages over classical computation are possible, and highlights quantum contextuality as a key resource.

Despite this evidence for the role of contextuality as a resource for quantum advantage, a finer characterisation of this resource is largely missing. We address this problem by asking a related question: how non-classical is quantum computation? This is similar to the study of the extent to which quantum mechanics violates certain Bell inequalities, yet with an explicit emphasis on computation and computationally relevant resource constraints.

In this paper, we study the computability of Boolean functions in the framework of measurement-based quantum computation (MBQC) [17–19], observing that many of the relevant results in the literature

including references [15, 20] are readily and naturally formulated within the measurement-based framework. For simplicity, we focus on non-adaptive MBQC with linear side-processing, where contextuality provides the sharpest known separation between classical and quantum computation [13, 21]. We outline this setup in section 1.1 below.

Within this setting, we further consider the interplay between the following two resource aspects: the amount of magic (non-Clifford operations, see section 1.2) necessary and the number of qubits required for the computation of a given Boolean function. Already in this limited framework, the classification of Boolean functions under these resources points towards a rich structure beyond the classical paradigm, which under the physical restrictions considered is restricted to the computation of linear functions only [21]. We summarise our main results and provide an overview to the structure of the paper in section 1.3.

1.1. The setting

In this section, we define our restricted framework of MBQC. An MBQC consists of a correlated quantum resource state, and a control computer with restricted computational power. The quantum resource state consists of N local subsystems—or parties—each of which consists of a qubit and measurement device that exchanges classical information with the control computer once. The control computer is responsible for selecting the measurement settings for each local subsystem, and for processing the measurement outcomes into useful computational outputs. Importantly, the power of the control computer is limited: we consider control computers that can only compute linear functions, and as such are not even classically universal[5]. This notion of MBQC is known as $l2$-MBQC (where the $l2$ stands for mod-2 linear side-processing) and is based on the model of Anders and Browne [20]. The following definition is based on references [13, 21]. (See [8] for a more general notion of MBQC.)

Definition 1. A $l2$-MBQC with classical input $\mathbf{i} \in \mathbb{Z}_2^n$ and classical output $o \in \mathbb{Z}_2$ consists of N qubit subsystems, jointly prepared in the state $|\psi\rangle$, each of which receives an input $c_k(\mathbf{i}) \in \mathbb{Z}_2$ from the control computer, performs a measurement $M_k(c_k(\mathbf{i}))$, and returns a measurement outcome $m_k \in \mathbb{Z}_2$, for $k = 1, \ldots, N$[6]. The inputs and computational output satisfy the following conditions:

(a) The computational output $o \in \mathbb{Z}_2$ is a linear function of all measurement outcomes $\mathbf{m} = (m_1, \ldots, m_N)^\intercal \in \mathbb{Z}_2^N$[7],

$$o = \sum_{k=1}^{N} m_k \mod 2.$$

(b) Local measurements $M_k(c_k)$ have eigenvalues $(-1)^{m_k}$. The measurement settings $\mathbf{c} = (c_1, \ldots, c_N)^\intercal \in \mathbb{Z}_2^N$ are linear functions of the classical input $\mathbf{i} = (i_1, \ldots, i_n)^\intercal \in \mathbb{Z}_2^n$ and the measurement outcomes $\mathbf{m}$ via

$$\mathbf{c} = T\mathbf{m} + P\mathbf{i} \mod 2, \tag{1}$$

for some $T \in \mathrm{Mat}(N \times N, \mathbb{Z}_2)$ and $P \in \mathrm{Mat}(N \times n, \mathbb{Z}_2)$.

(c) For a suitable ordering of the parties $1, \ldots, N$ the matrix T in equation (1) is lower triangular with vanishing diagonal. If $T = 0$ the $l2$-MBQC is called non-adaptive.

We remark that definition 1 describes a single run of the computation, corresponding to a given input $\mathbf{i} \in \mathbb{Z}_2^n$. Evaluation on more than one input requires access to multiple, identical copies of the same MBQC. In this sense, we say that a $l2$-MBQC is deterministic whenever the output in multiple runs of the MBQC is a deterministic function of the inputs, $o(\mathbf{i})$ for $\mathbf{i} \in \mathbb{Z}_2^n$. More generally, in the non-deterministic (probabilistic) case every input specifies a probability distribution over the outputs. We will mostly restrict ourselves to deterministic $l2$-MBQC (with the exception of theorem 4). Moreover, we will focus on the non-adaptive case. The latter is a natural restriction for the study of contextuality (nonlocality) as a resource in MBQC [22], since adaptivity generally allows to reproduce any nonlocal correlations (see also Remark 1 in [21]).

[5] The restriction to linear side-processing greatly simplifies the analysis of contextuality as a resource in MBQC. While nonlinear side-processing is not required for universal MBQC, one may consider relaxing this restriction in future studies in order to quantify any advantage of (MB)QC over universal classical computation in practical settings.

[6] Throughout, we will use boldface for vectors.

[7] In general, one can apply any linear post-processing to the measurement outcomes. However, since MBQC can, in particular, model constant and linear functions, it is sufficient to restrict the post-processing to the (mod 2)-linear sum of local measurement outcomes. Moreover, since a multi-output Boolean function can be decomposed into multiple single-output Boolean functions, restricting our analysis to a single output bit is not restriction.

Nevertheless, more flexible restrictions on adaptivity can still lead to interesting classes of algorithms such as shallow circuits in [15]. We briefly discuss the adaptive case in appendix H. Finally, we note that definition 1 is readily generalised to qudit systems, but requires care in the definitions of the higher-dimensional measurements allowed within the framework. Many of our results generalise to qudit systems of prime dimension, yet additional technicalities arise; to simplify presentation we only consider the qubit case in the main body of the text.

1.2. The stabiliser subtheory

We denote the group of Pauli operators on N qubits as $\mathcal{P}_N$. Throughout, we label the local computational basis states as $|q\rangle$ for $q \in \{0,1\}$. An important class of operators is given by the Clifford hierarchy.

Definition 2. The Clifford hierarchy on N qubits is defined recursively by setting $\mathcal{C}_N^1 = \mathcal{P}_N$, and letting the k'th level $\mathcal{C}_N^k$ be given by

$$\mathcal{C}_N^k = \{U \in \mathcal{U}((\mathbb{C}^2)^{\otimes N}) \mid UPU^\dagger \in \mathcal{C}_N^{k-1}\ \forall P \in \mathcal{P}_N\}. \tag{2}$$

Notably, the second level $\mathcal{C}_N^2$ is the normaliser of the Pauli group and is known as the *Clifford group*. Any state that can be obtained by applying a gate from the Clifford group to a computational basis state is known as a *stabiliser state*. Note that in the setting of the Clifford hierarchy, it is natural to model the classical control in definition 1 in the form of unitary conjugation on some fixed measurement setting.

Definition 3. We say a MBQC belongs to level-D if the local measurement settings are of the form of

$$M_k(c_k) = U_k(c_k) M_k(0) U_k^{-1}(c_k), \tag{3}$$

where $M_k(0) \in \mathcal{P}_1$ is some fixed measurement, $U_k(c_k) \in \mathcal{C}_1^D$, and where the resource state is a stabiliser state.

When the $l2$-MBQC belongs to level-2, the MBQC belongs to the stabiliser subtheory, and is classically efficiently simulable by the Gottesman–Knill theorem [23, 24]. Level-3 MBQCs are universal for quantum computation (in the adaptive case), with the scheme based on cluster states [18] being a well-known example. The restriction on resource states being stabiliser states is without loss of generality—one can additionally allow resource states that are obtained by applying a Dth level gate to a stabiliser state, in close analogy with the paradigm of stabiliser quantum computing supplemented by magic state injection.

In the context of MBQC, it is convenient to express the output of the computation in terms of a polynomial. Namely, every Boolean function $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ is given by a polynomial from the ring $\mathbb{Z}_2[x_1, \ldots, x_n]$ in n variables $x_1, \ldots, x_n \in \mathbb{Z}_2$. This representation is known as the algebraic normal form.

1.3. Summary of results

In this paper, we study the computability of Boolean functions in non-adaptive $l2$-MBQC under various resource constraints. Below, we summarise our main results, and outline the structure of the rest of the paper.

1.3.1. Contextuality

We begin by recalling that any Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ can be computed within non-adaptive, deterministic $l2$-MBQC [22] (see theorem 2 in section 2). In the classical setting, only linear functions are computable. Thus, nonlinearity indicates the presence of quantumness in the form of contextuality [13, 21]. The proof of this result relies on operators outside the Clifford group, i.e. outside the second level in the Clifford hierarchy; moreover, it generally requires an exponential (in the degree of f, expressed as a polynomial) number of qubits. This suggests a finer classification in terms of the Clifford hierarchy, which we present in section 3, and the number of qubits ('qubit count') required to implement a given Boolean function in the non-adaptive case, presented in section 4[8]. A natural starting point for these considerations is the stabiliser sub-theory, where resource states are stabiliser states and operators are restricted to the second level in the Clifford hierarchy.

1.3.2. Stabiliser theory

In the case of $l2$-MBQCs belonging to level-2 (i.e. stabiliser MBQCs), we show the computable functions (in non-adaptive MBQC) to be heavily restricted: in the deterministic case, only quadratic functions can be computed (see theorem 3), while in the probabilistic case, the success probability (see definition 4) to compute a given Boolean function is bounded by its non-quadraticity (see definition 5), i.e. the Hamming distance to the nearest quadratic function (see theorem 4). These results are presented in section 3.1.

[8] In the adaptive case, one must also consider the time required to implement a given function (see appendix H).

Moreover, we find that in the deterministic case, a quadratic function can be implemented using $\mathrm{rk}(f)+1$ qubits only, where $\mathrm{rk}(f)$ denotes the rank of the matrix corresponding to the quadratic terms of f (see theorem 6).

1.3.3. Clifford hierarchy

Despite being non-classical (contextual), the above mentioned results (theorem 3 and theorem 4) show that computation within non-adaptive stabiliser $l2$-MBQC is limited[9]. A natural way to extend the stabiliser case is via the Clifford hierarchy. In section 3.2, we consider what non-Clifford resources are required to implement a given Boolean function within $l2$-MBQC. The main result of this section, theorem 5 shows that operations from the Dth level in the Clifford hierarchy are required whenever a non-adaptive, deterministic $l2$-MBQC computes a polynomial of degree D.

1.3.4. Qubit count

While we can compute the minimal number of qubits in the stabiliser case, i.e. for quadratic functions (see theorem 6 in section 4.1), generalising this result beyond the stabiliser case is challenging. In section 4.2, we consider an approach based on Greenberger-Horne-Zeilinger (GHZ) states, which (by the proof of theorem 2) provide a universal resource for function computation in non-adaptive, deterministic $l2$-MBQC[10]. We characterise the number of qubits required to compute an arbitrary Boolean function in terms of the minimal number of Fourier components (see theorem 7). Similar optimisation problems arise in circuit synthesis [26–30].

In addition, we employ the discrete Fourier transform to obtain upper bounds on the qubit count for certain highly symmetric functions, which turn out to be optimal in some cases, e.g. for δ-functions corollary 2. As an immediate consequence, we conclude that the number of qubits required to implement a Boolean function f in non-adaptive, deterministic $l2$-MBQC is far from monotonic in the degree of f (see corollary 3), thus further hinting at a rich substructure of contextuality beyond the results in references [7, 13].

Finally, we discuss possible avenues towards related and future research in section 5.

2. Every Boolean function has a representation as contextual MBQC

In this section we prove theorem 2, that non-adaptive $l2$-MBQC is complete. That is, for any function $f:\mathbb{Z}_2^n\to\mathbb{Z}_2$ there exists an $l2$-MBQC with output function $o(\mathbf{i})=f(\mathbf{i})$ for all inputs $\mathbf{i}\in\mathbb{Z}_2^n$. This is in sharp contrast to the classical regime, which is restricted to linearity—nonlinear computation is an indicator of quantum contextuality [13, 21]. The proof strategy is to first construct $l2$-MBQCs that compute the n-bit δ-function which evaluates to 1 on the all-zero input string, and evaluates to zero otherwise (alternatively, the n-bit AND-function). Linearly composing the output of many such parallel $l2$-MBQCs can then be used to compute any function. In fact, our proof is easily generalised to qudits of prime dimension (see appendix C).

We begin by defining the resource state and the measurement operators relevant for this construction. We take the resource state to be given by the N-qubit GHZ state

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle^{\otimes N}+|1\rangle^{\otimes N}). \tag{4}$$

This is a mild restriction, since the GHZ state in equation (4) will prove to be a universal resource for non-adaptive, deterministic $l2$-MBQC in theorem 2 below (see also [22, 31]). More generally, in section 3 we will define a hierarchy for $l2$-MBQC by restricting the allowed operations to certain levels in the Clifford hierarchy and the resource state to a stabiliser state (see definition 3). Note also that the GHZ state is a stabiliser state. Finally, in section 4 we will analyse the qubit count for $l2$-MBQC with a GHZ resource state.

Next, recall from definition 1 that each party performs one of two measurements $M_k(c_k)$ determined by a single input $c_k\in\mathbb{Z}_2$. Moreover, we require that M_k has (non-degenerate) eigenvalues $(-1)^q$, $q\in\mathbb{Z}_2$, i.e. $M_k^2=1$. We define the following canonical measurement operators

$$X(\mathrm{e}^{i\pi\vartheta})|q\rangle=\mathrm{e}^{i\pi(1-2q)\vartheta}|q\oplus 1\rangle. \tag{5}$$

In matrix (gate) representation, these operators take the form

$$X(\mathrm{e}^{i\pi\vartheta})=\begin{pmatrix}0 & \mathrm{e}^{-i\pi\vartheta}\\ \mathrm{e}^{i\pi\vartheta} & 0\end{pmatrix}. \tag{6}$$

[9] Note that for d odd prime, the stabiliser formalism is in fact non-contextual [25]. At least in this case, we can take it as the lowest level of such a hierarchy.

[10] Note however, that GHZ states are not universal for MBQC in general.

The inputs c_k to the measurement devices thus specify $M_k(c_k) = X_k(e^{i\pi\vartheta(c_k)})$ and are themselves determined in a linear way from the computational input $\mathbf{i} \in \mathbb{Z}_2^n$ and other measurement outcomes $m_k \in \mathbb{Z}_2$ according to the general setup in definition 1. (Note that in the non-adaptive case, $c_k = c_k(\mathbf{i})$ is a linear functions of the inputs only.)

The output function of the *l*2-MBQC, $o(\mathbf{i}) = \oplus_{k=1}^N m_k$, arises as the parity of the individual measurement outcomes on local qubits. The resource state $|\psi\rangle$ is a $+1$-parity eigenstate of the operator $\otimes_{k=1}^N X_k(0)$. On the other hand, we can easily construct operators for which $|\psi\rangle$ is a (-1)-parity eigenstate. For instance, consider the prototypical Anders–Browne 3-qubit example, where $M_k(0) = X_k(0) = X_k$ and $M_k(1) = X_k(e^{i\frac{\pi}{2}}) = Y_k$. Note that this choice of local measurements solves the following set of four linear equations $\sum_{k=1}^3 c_k(i_1, i_2) \cdot \vartheta_k = o(i_1, i_2)$, where $i_1, i_2 \in \mathbb{Z}_2$, $\vartheta_k = \frac{1}{2}$, and $c_1(i_1, i_2) = i_1$, $c_2(i_1, i_2) = i_2$, $c_3(i_1, i_2) = i_1 \oplus i_2$, and $o(i_1, i_2) = i_1 i_2 \oplus i_1 \oplus i_2$.

In fact, this example is representative of the general case. More precisely, for deterministic *l*2-MBQC the computation can be expressed in terms of the phase parameters in the local measurement operators of equation (5).

Theorem 1. *The output function $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ of a non-adaptive, deterministic l2-MBQC with a GHZ resource state, is given by the linear sum of angles $\vartheta_k \in \mathbb{R}$, corresponding to local measurement operators in equation (5),*

$$o(\mathbf{i}) = \sum_{k=1}^{N} c_k(\mathbf{i})\vartheta_k \pmod 2 \quad \forall \mathbf{i} \in \mathbb{Z}_2^n. \tag{7}$$

Proof (sketch). Using that the GHZ state $|\psi\rangle$ is a parity eigenstate of the global measurement operators $M(\mathbf{i}) = \otimes_{k=1}^N M_k(c_k(\mathbf{i}))$, one shows that the most general form for local measurements M_k is given by equation (6). Equation (7) then follows by mere re-writing $|\psi\rangle$ in terms of the eigenbases of the M_k. For details, see appendix A. □

We note that theorem 1 is closely related to results obtained in a slightly different context in [32] (see section 5.3).

Finding an implementation to compute o as a *l*2-MBQC thus reduces to finding a set of (linear) functions c_k and real parameters $\vartheta_k \in \mathbb{R}$, which satisfies the required parity conditions in equation (7). We first construct an *l*2-MBQC that computes the n-bit δ-function $\delta : \mathbb{Z}_2^n \to \mathbb{Z}_2$ defined by

$$\delta(\mathbf{i}) := \begin{cases} 1 & \text{if } \mathbf{i} = 0 \\ 0 & \text{otherwise} \end{cases}. \tag{8}$$

We remark that the n-bit δ function is an important and ubiquitous function—up to linear pre- and post-processing it is equivalent to the n-bit AND function. We have the following lemma.

Lemma 1. *The n-bit δ-function can be implemented on $N = 2^n - 1$ qubits within non-adaptive, deterministic l2-MBQC.*

Proof (sketch). We prove this in appendix B, by giving an explicit measurement scheme acting on a GHZ state. □

We remark that a similar result has previously been obtained in [22]. Here, we gave a constructive proof in terms of the operators in equation (6). Moreover, our technique generalises to qudits of prime dimension (for details, see appendix C).

In particular, we note that lemma 1 recovers the main example of Anders and Browne [20] (up to linear side-processing) for $n = 2$ with $\vartheta_k = \frac{1}{2}$, such that $M(0) = X$ and $M(1) = Y$.

The n-bit δ-function along with linear side-processing is sufficient to allow for the evaluation of arbitrary functions. In particular, one can decompose any function into a linear combination of delta functions, each of which admits an *l*2-MBQC. The outputs of these *l*2-MBQCs can be linearly combined to give the desired output, as in the following theorem.

Theorem 2 ([22]). *For any Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ there exists a non-adaptive l2-MBQC that deterministically evaluates it.*

Proof (sketch). This follows directly from lemma 1 and the fact that every function can be written as a sum of δ-functions $f(\mathbf{i}) = \sum_{\mathbf{j} \in \mathbb{Z}_2^n} f_\mathbf{j} \delta(\mathbf{i} - \mathbf{j})$, $f_\mathbf{j} \in \mathbb{Z}_2$ for all inputs $\mathbf{i} \in \mathbb{Z}_2^n$. □

The number of qubits in the implementation of the δ-function is $N = 2^n - 1$, which is optimal (see [22]). We explore the question of optimality for arbitrary Boolean functions in more detail in section 4, as well as other resource aspects related with *l*2-MBQC.

3. Boolean functions as MBQC - (dependence on) Clifford hierarchy

In this section, we study the implementation of Boolean functions in $l2$-MBQC, restricted to the stabiliser subtheory where only Pauli operators can be measured. In the deterministic, non-adaptive case such $l2$-MBQCs admit a simple description, namely the entire computation can be expressed as a set of eigenvalue equations that relate the inputs and outputs of the computation as follows:

$$\bigotimes_{k=1}^{N} U_k(c_k(\mathbf{i}))M_k(0)U_k^{-1}(c_k(\mathbf{i}))|\psi\rangle = (-1)^{o(\mathbf{i})}|\psi\rangle \quad \forall \mathbf{i} \in \mathbb{Z}_2^n. \tag{9}$$

In section 3.1, we prove that any quadratic Boolean function can be computed within the stabiliser formalism. Conversely, any non-quadratic function requires gates from higher levels in the Clifford hierarchy. In fact, the degree of a Boolean function in $l2$-MBQC relates to the phase terms in local measurement operators of the form in equation (6), which in turn put a bound on the necessary level in the Clifford hierarchy. We make this precise in section 3.2.

3.1. Quadratic Boolean functions and stabiliser formalism

The qubit stabiliser formalism is contextual. For instance, the prototypical Anders–Browne NAND-gate computes a quadratic Boolean function. It is natural to ask whether stabiliser $l2$-MBQC can realise any polynomial $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$. However, this is not the case. In fact, non-adaptive, deterministic stabiliser MBQC is limited to quadratic Boolean functions.

Theorem 3. *Every non-adaptive, deterministic, level-2 (i.e. stabiliser) $l2$-MBQC computes a quadratic function. Conversely, every quadratic function is computed by a non-adaptive, deterministic, level-2 $l2$-MBQC.*

Proof (sketch). The first implication follows by noting that $(-1)^{o(\mathbf{i})}M(\mathbf{i})$ is in the stabiliser of the resource state of the MBQC for all $\mathbf{i} \in \mathbb{Z}_2^n$. Quadraticity of f is then a consequence of the (Abelian) group structure of the stabiliser. For details, see appendix D. The converse direction follows from equation (B1) in appendix B that every quadratic function can be computed in level-2 MBQC. In particular, as the delta function on two bits can be computed within stabiliser $l2$-MBQC, any quadratic monomial can be computed. Finally, any quadratic function can be computed by taking linear combinations of quadratic and linear terms via linear post-processing. □

For the probabilistic case, we need two additional concepts: the *success probability* for a MBQC and the *non-quadraticity* of a Boolean function.

Definition 4 (success probability). Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean function, and let A be a MBQC, which implements f with probability $p(\mathbf{i})$ on inputs $\mathbf{i} \in \mathbb{Z}_2^n$. We define the average success probability by $P_{\text{succ}} = \sum_{\mathbf{i}\in\mathbb{Z}_2^n} p(\mathbf{i})/2^n$.

Assume a deterministic MBQC computing function g is used to approximate the function f, then the success probability is $P_{\text{succ}} = 1 - d_{\text{H}}(f,g)/2^n$ where $d_{\text{H}}(f,g) := |\{\mathbf{i} \in \mathbb{Z}_2^n \mid f(\mathbf{i}) \neq g(\mathbf{i})\}|$ denotes the Hamming distance between f and g. Clearly, $P_{\text{succ}} = 1$ if and only if $f = g$. In order to compute the success probability for general functions, we measure how far it is from being quadratic (see e.g. [33]).

Definition 5 (non-quadraticity). Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean function. Then the non-quadraticity of f is given by

$$\mathcal{NQ}(f) := \min\{d_{\text{H}}(f,q) : q : \mathbb{Z}_2^n \to \mathbb{Z}_2 \text{ quadratic}\}. \tag{10}$$

It then follows as a corollary of theorem 3 that

Corollary 1. *Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be an arbitrary Boolean function. The maximum success probability to approximate f by a Boolean function using non-adaptive, deterministic, level-2 (i.e. stabiliser) $l2$-MBQC is*

$$P_{\text{succ}} = 1 - \frac{\mathcal{NQ}(f)}{2^n}. \tag{11}$$

Proof (sketch). The proof of this simply follows by noting that theorem 3 entails the MBQC must compute some quadratic function q with success probability $1 - d_{\text{H}}(f,q)$. The maximum success probability is achieved by choosing q to minimise the Hamming distance d_{H}, which is the non-quadraticity of f. □

Usually, a non-adaptive, level-2 $l2$-MBQC does not yield deterministic outputs. Still, corollary 1 remains true also in the probabilistic case. In other words, when restricted to stabiliser measurements (and stabiliser states), the best approximation to a given Boolean function is always achieved with a deterministic $l2$-MBQC.

Theorem 4. *Let $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ be an arbitrary Boolean function. The maximum success probability of computing f in (probabilistic) non-adaptive, level-2 (i.e. stabiliser) l2-MBQC is*

$$P_{\text{succ}} = 1 - \frac{\mathcal{NQ}(f)}{2^n}. \tag{12}$$

Proof (sketch). As with theorem 3, the proof exploits the group structure of the stabiliser in order to construct a deterministic MBQC performing at least as well as a probabilistic one. For details, see appendix E. □

In particular, this says that if f is not quadratic then the success probability will be less than one, and we cannot demonstrate 'strong' nonlocality (contextuality) for this function. As a concrete case study, consider example 2 in [34] that is an 8-bit input Boolean function with $\mathcal{NQ}(f) = 68$. This entails an optimal success probability of $P_{\text{succ}} = 47/64 \approx 0.734375$.

Note also that the bound in theorem 4 is strict since for the stabiliser formalism deterministic strategies are always optimal. However, it is not clear whether this is always the case. In particular, a similar problem arises from the well-known CHSH inequality. While quantum correlations violate the classical bound, they cannot win the related CHSH nonlocal game with certainty. This is different to the problem studied here, where the restriction is not on the number of qubits involved but on the level in the Clifford hierarchy of the gates used in equation (3). Nevertheless, this example shows that the MBQC which best approximates a given Boolean function need not be a deterministic one.

3.2. Beyond quadratic functions

Theorem 3 shows that in the non-adaptive case, non-Clifford operations are required to evaluate general (non-quadratic) Boolean functions f. In this section, we establish the necessity of operations belonging to higher levels in the Clifford hierarchy depending on the degree of f.

We utilise a characterisation of the Clifford hierarchy due to Zeng *et al* [35]. We define a set of operations known as semi-Clifford operations [35, 36].

Definition 6 (semi-Clifford hierarchy). We say a gate $U \in \mathcal{C}_N^k$ is a kth level semi-Clifford gate (on N qubits) if $U = C_1 D C_2$ where $C_1, C_2 \in \mathcal{C}_N^2$ are Clifford gates, and $D \in \mathcal{C}_N^k$ is diagonal. We label the set of kth level semi-Clifford gates (on N-qubits) as $\mathcal{SC}_N^k$.

In other words, gates in the semi-Clifford hierarchy are those that are diagonal up to Clifford operations. Note in the above that $D \in \mathcal{C}_N^k$ necessarily, as for any $U \in \mathcal{C}_N^k$ one can verify that $C_1 U C_2 \in \mathcal{C}_N^k$ $\forall C_1, C_2 \in \mathcal{C}_N^2$ [35].

Theorem 5. *Every non-adaptive, deterministic, level-D l2-MBQC computes functions of degree at most D. Conversely, every function of degree D is computed by a non-adaptive, deterministic, level-D l2-MBQC.*

Proof (sketch). For the first implication, we use the fact that single qubit Clifford hierarchy operators are semi-Clifford operators (see [35]), in order to express the measurement operators in the MBQC as a conjugated Pauli operator by a diagonal Clifford hierarchy-operator. The result then follows from the characterisation of the diagonal Clifford hierarchy in [37]. For details, see appendix F. For the converse direction, we use equation (B1) in appendix B to construct the delta function on D-bits, which saturates the bound. Any function can then be computed as a linear combination of D-bit or fewer delta functions. □

Theorem 5 generalises theorem 3. If a non-adaptive $l2$-MBQC belonging to some level in the Clifford hierarchy computes a polynomial of degree D, then it at least belongs to level-D in the Clifford hierarchy.

We remark that the analogous problem for qudits is open. In our argument we used the fact that the semi-Clifford hierarchy is equal to the Clifford hierarchy for single qubits, $\mathcal{SC}_1^k = \mathcal{C}_1^k$, which has not been shown to hold for general qudits (see [38] for a more comprehensive discussion). For prime qudits it is conjectured that all Clifford hierarchy gates are semi-Clifford, and has been proven true for the third-level gates [38]. We also remark that certain gates do not belong to any finite level in the Clifford hierarchy. For qubits, an example is the square root of the Hadamard, $\sqrt{H}$. For qudits an example is the phase gate $D_3 = \text{diag}(1, 1, -1)$.

4. Boolean functions as MBQC - (dependence on) qubit count

In this section, we search for the minimal number of qubits, also known as qubit count, needed to implement a Boolean function $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ in non-adaptive, deterministic $l2$-MBQC.

Definition 7. Let $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$. We call a non-adaptive $l2$-MBQC which deterministically implements f *optimal*, if no other non-adaptive $l2$-MBQC exists which deterministically implements f on fewer qubits. The

minimal number of qubits over all possible resource states is denoted by $R(f)$, while $R_{\mathrm{GHZ}}(f)$ denotes the minimal number of qubits when restricted to the n-qubit GHZ state in equation (4).

Note first that we have the freedom to manipulate f by any invertible linear transformation on the inputs via pre-processing P. The resource cost R should therefore be an invariant under affine transformations. We thus define an equivalence relation on all functions with signature $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ under affine transformations as follows,

$$f \leftrightarrow f' :\Longleftrightarrow \exists P \in \mathrm{Mat}(n\times n, \mathbb{Z}_2),\ \mathrm{rk}(P) = n :\ f'(\mathbf{i}) = f(P\mathbf{i}) \quad \forall \mathbf{i} \in \mathbb{Z}_2^n. \tag{13}$$

Furthermore, in section 2 we have seen how the n-bit δ-function can be implemented as a non-adaptive $l2$-MBQC on $N = 2^n - 1$ qubits[11]. Hence, given an arbitrary Boolean function $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$, one way to implement it is by naively adding all terms in the sum $f(\mathbf{i}) = \sum_{\mathbf{j}\in\mathbb{Z}_2^n} f_{\mathbf{j}}\delta(\mathbf{i}-\mathbf{j})$ with $f_{\mathbf{j}} \in \mathbb{Z}_2$ for all $\mathbf{i} \in \mathbb{Z}_2^n$. However, the minimal number of qubits is only subadditive in this as well as its polynomial representation. To see this, we again consider the stabiliser case first.

4.1. Qubit count in stabiliser *l*2-MBQC

Recall that only quadratic functions can be computed deterministically using stabiliser $l2$-MBQCs. We now find the minimal number of qubits to do so. Consider a quadratic Boolean function

$$f(\mathbf{x}) = \sum_{i=1}^{n} l_i x_i + \sum_{i<j} q_{i,j} x_i x_j \pmod 2, \quad l_i, q_{i,j} \in \mathbb{Z}_2 \tag{14}$$

and define a symmetric matrix $Q(f)$ such that $Q_{i,i} = 0$ and $Q_{i,j} = Q_{j,i} = q_{i,j}$. We denote by $\mathrm{rk}(f)$ the $\mathbb{Z}_2$-rank of Q.

Theorem 6. *Let $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a quadratic Boolean function. Let f be expressed as*

$$f(\mathbf{x}) = \sum_{i=1}^{n} l_i x_i + \sum_{i<j} q_{i,j} x_i x_j \pmod 2, \quad l_i, q_{i,j} \in \mathbb{Z}_2 \tag{15}$$

Then f can be deterministically computed as a non-adaptive, level-2 (i.e. stabiliser) $l2$-MBQC on $R(f) = \mathrm{rk}(f) + 1$ qubits, where $\mathrm{rk}(f)$ is the $\mathbb{Z}_2$-rank of the symmetric matrix $Q(f)$.

Proof (sketch). The result is a straightforward application of the main theorem in [39]. For details, see appendix G. □

Theorem 6 replicates the Anders–Browne result as a special case, where $o(i_1, i_2) = i_1 i_2 \oplus i_1 \oplus i_2$ is quadratic with

$$Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{16}$$

This is a rank 2 matrix and so the theorem says it can be computed using 3 qubits.

Note that theorem 6 suggests another resource measure: by theorem 3, within the stabiliser formalism only quadratic functions can be computed; in fact, they can be computed *efficiently in the number of qubits*. Unfortunately, as a consequence of theorem 3 we cannot use arguments based on stabilisers (as in the proof of theorem 6) to understand the number of qubits as a resource also in the general case. Instead, in the next section we will apply the Fourier transform between the polynomial and $\mathbb{Z}_2$-linear representation of Boolean functions (see section 4.2.1) below to obtain a lower bound on the number of qubits for non-adaptive, deterministic $l2$-MBQCs with a GHZ resource state[12]. This turns out to be a hard problem in general, yet we show how to reproduce the bound in theorem 6, as well as other known bounds for R obtained in previous sections.

4.2. Qubit count in *l*2-MBQC using GHZ states

By comparison with optimal bounds for Bell inequalities, finding the optimal $l2$-MBQC implementing a given Boolean function is likely a difficult problem. Here, we approach this problem by fixing the resource state to be a GHZ state, which we found to be universal for non-adaptive, deterministic $l2$-MBQC in theorem 2. To this end, we will need some basic facts about the discrete Fourier transform.

[11] Note that this is the same scaling behaviour as for the n-bit $\mathrm{AND}(\mathbf{i}) = \prod_{j=1}^{n} i_j$, which is optimal by [22].

[12] Recall that by theorem 2 GHZ-states are universal for (the computation of Boolean functions) in non-adaptive, deterministic $l2$-MBQC.

4.2.1. Polynomial vs $\mathbb{Z}_2$-linear representation of Boolean functions

We introduce some tools to allow us to map between different representations of Boolean functions in $l2$-MBQC. In particular, we introduce the $\mathbb{Z}_2$-linear representation of a Boolean function, in addition to its polynomial representation. We show how to map between these representations using the discrete Fourier transform. Our analysis closely resembles the one in [40], to which we refer the reader for more details. (See also [41] for more details on Boolean function analysis.)

The polynomial representation of computational outputs is one useful way of characterising $l2$-MBQCs, as the polynomial degree places important constraints on the resources required. In order to characterise the optimal implementation of a given $l2$-MBQC, we consider another representation known as the $\mathbb{Z}_2$-linear function representation. Any Boolean function $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ can be written in the following two ways, up to an additive constant,

$$f(\mathbf{x}) = \sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}} \left(\oplus_{j=1}^n a_j x_j\right) = \sum_{\mathbf{b}\in\mathbb{Z}_2^n} D_{\mathbf{b}} \left(\prod_{j=1}^n x_j^{b_j}\right), \tag{17}$$

where $C_{\mathbf{a}} \in \mathbb{R}$, $D_{\mathbf{b}} \in \mathbb{Z}_2$ for all $\mathbf{a},\mathbf{b} \in \mathbb{Z}_2^n$, and $\oplus$ denotes addition modulo 2[13]. We focus on the first representation in terms of $\mathbb{Z}_2$-linear functions. In particular, we define the $\mathbb{Z}_2$-linear basis functions $\phi_{\mathbf{a}}(\mathbf{x}) := \oplus_{j=1}^n a_j x_j$, and monomial basis functions $\pi_{\mathbf{b}}(\mathbf{x}) := 2^{W(\mathbf{b})-1}\prod_{l=1}^n x_l^{b_l}$ for $0 \neq \mathbf{a},\mathbf{b} \in \mathbb{Z}_2^n$, $\phi_0 = \pi_0 := 1$, and where $W(\mathbf{b}) := |\{l \in \{1,\dots,n\} \mid b_l \neq 0\}|$ denotes the *Hamming weight* of $\mathbf{b} \in \mathbb{Z}_2^n$. Both sets of functions $\{\phi_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{Z}_2^n\}$ and $\{\pi_{\mathbf{b}} \mid \mathbf{b} \in \mathbb{Z}_2^n\}$ are each linearly independent and generate the space of Boolean functions on bit strings $\mathbf{x} \in \mathbb{Z}_2^n$, as will be shown below. As such, we can determine the corresponding transformation map between the coefficients $C_{\mathbf{a}}$, $D_{\mathbf{b}}$. By equation (4) in [22], $\phi_{\mathbf{a}}$ for $\mathbf{a} = (1,\dots,1) \in \mathbb{Z}_2^n$ is given by

$$\phi_{\mathbf{a}} = \oplus_{j=1}^n x_l = \sum_{0\neq\mathbf{b}\in\mathbb{Z}_2^n} (-2)^{W(\mathbf{b})-1} \prod_{l=1}^n x_l^{b_l}. \tag{18}$$

Using this, it is easy to see that we can write a given $\mathbb{Z}_2$-linear basis function $\phi_{\mathbf{a}}$ as

$$\phi_{\mathbf{a}} = \sum_{0\neq\mathbf{b}\in\mathbf{a}\mathbb{Z}_2^n} (-2)^{W(\mathbf{b})-1} \prod_{l=1}^n x_l^{b_l}, \tag{19}$$

where we have defined the set $\mathbf{a}\mathbb{Z}_2^n = \{(a_1 b_1,\dots,a_n b_n) \in \mathbb{Z}_2^n \mid \forall b_i \in \mathbb{Z}_2\}$. More generally, we define the symmetric product,

$$\langle \pi_{\mathbf{b}}, \phi_{\mathbf{a}} \rangle := \begin{cases} 1 & \text{if } \mathbf{a} = \mathbf{b} = 0, \\ (-1)^{\sum_{j=1}^n a_j b_j - 1} & \text{otherwise.} \end{cases} \tag{20}$$

This defines a linear map $\mathcal{F} : \mathbb{R}^{2^n} \to \mathbb{R}^{2^n}$ with matrix coefficients $\mathcal{F}_{\pi_{\mathbf{b}}\phi_{\mathbf{a}}} := \langle \pi_{\mathbf{b}}, \phi_{\mathbf{a}} \rangle$[14]. From equation (20) it follows that $\mathcal{F}_{\phi_{\mathbf{a}}\pi_{\mathbf{b}}} = \pm 1$ and given that $\mathcal{F}$ has full rank (as a basis change) it has an inverse. In fact, for fixed dimension n and with appropriate normalisation factor $\mathcal{N} = 2^{-\frac{n}{2}}$, $\mathcal{F}$ becomes a Hadamard transform and is thus in particular orthogonal, hence, $(\mathcal{N}\mathcal{F}_{\pi_{\mathbf{b}}\phi_{\mathbf{a}}})^{-1} = \mathcal{N}\mathcal{F}_{\phi_{\mathbf{a}}\pi_{\mathbf{b}}} = \mathcal{N}\mathcal{F}_{\pi_{\mathbf{b}}\phi_{\mathbf{a}}}$. This generalises equation (18) and provides an explicit translation between the two representations of Boolean functions underlying equation (7).

More precisely, let $f = \sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}}\phi_{\mathbf{a}}$, where $(C_{\mathbf{a}})_{\mathbf{a}\in\mathbb{Z}_2^n}$ are the coefficients of f in the basis $\{\phi_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{Z}_2^n\}$, then $\mathcal{F}$ transforms these into coefficients $(D_{\mathbf{b}})_{\mathbf{b}\in\mathbb{Z}_2^n}$ in its polynomial representation $f = \sum_{\mathbf{b}\in\mathbb{Z}_2^n} D_{\mathbf{b}}(\frac{1}{2^{W(\mathbf{b})-1}}\pi_{\mathbf{b}})$,

$$f = \mathcal{F}\left(\sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}}\phi_{\mathbf{a}}\right) = \sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}} \left(\sum_{0\neq\mathbf{b}\in\mathbf{a}\mathbb{Z}_2^n} (-2)^{W(\mathbf{b})-1} \prod_{l=1}^n x_l^{b_l}\right) = \sum_{\mathbf{b}\in\mathbb{Z}_2^n}\sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}}\langle \pi_{\mathbf{b}}, \phi_{\mathbf{a}} \rangle \pi_{\mathbf{b}} = \sum_{\mathbf{b}} D_{\mathbf{b}}\pi_{\mathbf{b}}. \tag{21}$$

In particular, note that the local phases ϑ_k from equation (7) simply correspond to the coefficients $\mathbf{C}_{\mathbf{a}}$ under the mapping $\mathcal{F}^{-1}$ applied to the output function of the $l2$-MBQC (in its polynomial representation).

[13] Note that the $C_{\mathbf{a}}$ are not arbitrary real numbers, but are in fact dyadic rationals.

[14] Note that while $\mathcal{F}$ is a map between functions over bit strings $\mathbf{i} \in \mathbb{Z}_2^n$ with real coefficients, it reduces to a map between Boolean functions for appropriate $\mathbf{C}_{\mathbf{a}}$ (and $\mathbf{D}_{\mathbf{b}}$). The real coefficients corresponding to a Boolean function f are also known as the Walsh spectrum of f.

4.2.2. Optimising the qubit count

More precisely, let $f=\sum_{\mathbf{a}\in\mathbb{Z}_2^n} C_{\mathbf{a}}\phi_{\mathbf{a}}$ be a Boolean function, which is implemented (in terms of the output function) of a non-adaptive, deterministic $l2$-MBQC with a GHZ state. By theorem 1, the coefficients $C_{\mathbf{a}}$ are encoded in terms of local phases, which in turn define local measurement operators via equation (6). It follows that the minimal number of qubits required to implement f deterministically as a non-adaptive $l2$-MBQC with a GHZ state corresponds with the minimal number of terms in the $\mathbb{Z}_2$-linear representation of f.

Let $f=\sum_{\mathbf{b}\in\mathbb{Z}_2^n} D_{\mathbf{b}}\pi_{\mathbf{b}}$ be the polynomial representation of f. Then we obtain a corresponding representation in terms of $\mathbb{Z}_2$-linear functions by applying the inverse discrete Fourier transform $\mathcal{F}^{-1}$ in equation (21). As we will see in the next sections, for monomials and other highly symmetric functions this representation is already minimal in the number of non-zero coefficients in its $\mathbb{Z}_2$-linear representation, and thus in the number of qubits in the implementation as $l2$-MBQC. However, for more general Boolean functions this is no longer the case. The reason is that we may change the representation of f in terms of $\mathbb{Z}_2$-linear functions, as long as f describes the same Boolean function. To give an example, the minimal number of $\mathbb{Z}_2$-linear terms of the Boolean function $f\colon\mathbb{Z}_2^4\to\mathbb{Z}_2$, $f(\mathbf{i})=i_1i_2+i_3i_4$ arises by subtracting the term $z=4i_1i_2i_3i_4-2i_1i_2(i_3+i_4)$ from the 'naive' representation $f(\mathbf{i})=\frac{1}{2}(i_1+i_2-i_1\oplus i_2)+\frac{1}{2}(i_3+i_4-i_3\oplus i_4)$ given by adding the optimal representations of the Boolean functions i_1i_2 and i_3i_4.

More generally, for $f\colon\mathbb{Z}_2^n\to\mathbb{Z}_2$, $f(\mathbf{x})=\sum_{\mathbf{b}\in\mathbb{Z}_2^n} D_{\mathbf{b}}\left(\prod_{j=1}^n x_j^{b_j}\right)$ define the linear span of *zero polynomials*

$$Z(f)=\operatorname{span}\left\{2^m\sum_{\mathbf{b}\in\mathbb{Z}_2^n} D_{\mathbf{b}}\left(\prod_{j=1}^n x_j^{b_j}\right)\;\middle|\; n\geqslant m\geqslant 1, D_{\mathbf{b}}\in\mathbb{Z}_2\forall\mathbf{b}\in\mathbb{Z}_2^n\right\}. \tag{22}$$

In addition to the linear equivalence relation in equation (13), we have the following characterisation.

Theorem 7. *The minimal number of qubits $R_{\mathrm{GHZ}}(f)$ required to deterministically implement a given Boolean function $f\colon\mathbb{Z}_2^n\to\mathbb{Z}_2$ in non-adaptive $l2$-MBQC with a GHZ state, is the minimal number of non-zero coefficients $C_{\mathbf{a}}$ in $\mathcal{F}^{-1}(f)$ in equation (21) under the relation $f\sim f'\iff f'=f+z$, $z\in Z(f)$ of equation (22).*

Proof (sketch). From the above discussion, we know that the minimal number of qubits to implement f as a non-adaptive, deterministic $l2$-MBQC with a GHZ state corresponds to the minimal number of terms in the $\mathbb{Z}_2$-linear representation of f. Recall that $\mathcal{F}:\mathbb{R}^{2^n}\to\mathbb{R}^{2^n}$ in equation (21) is an orthogonal linear map, in particular, it has full rank. It follows that $\sum_{\mathbf{a}} C_{\mathbf{a}}\mathcal{F}(\phi_{\mathbf{a}})=\mathcal{F}(\sum_{\mathbf{a}} C_{\mathbf{a}}\phi_{\mathbf{a}})=0$ for $C_{\mathbf{a}}\in\mathbb{R}$ implies $C_{\mathbf{a}}=0$ for all $\mathbf{a}\in\mathbb{Z}_2^n$. Now let $f=\sum_{\mathbf{a}} C_{\mathbf{a}}\phi_{\mathbf{a}}=\sum_{\mathbf{a}} C'_{\mathbf{a}}\phi_{\mathbf{a}}$ such that $\mathcal{F}(\sum_{\mathbf{a}} C_{\mathbf{a}}\phi_{\mathbf{a}})=\mathcal{F}(\sum_{\mathbf{a}} C'_{\mathbf{a}}\phi_{\mathbf{a}})\pmod 2$. It follows that $\mathcal{F}(\sum_{\mathbf{a}} C_{\mathbf{a}}\phi_{\mathbf{a}})=\mathcal{F}(\sum_{\mathbf{a}} C'_{\mathbf{a}}\phi_{\mathbf{a}})+\mathbf{z}$ for some $\mathbf{z}\in\mathbb{R}^{2^n}$ with $\mathbf{z}=0\pmod 2$. Since $\{\pi_{\mathbf{b}}\}_{\mathbf{b}\in\mathbb{Z}_2^n}$ is a basis of $\mathbb{R}^{2^n}$, we conclude that $\mathcal{F}(\sum_{\mathbf{a}} C_{\mathbf{a}}\phi_{\mathbf{a}})=\mathcal{F}(\sum_{\mathbf{a}} C'_{\mathbf{a}}\phi_{\mathbf{a}})+z$ with $z\in Z(f)$. Consequently, the optimal implementation of f is given by minimising the number of terms in the $\mathbb{Z}_2$-linear representation of $\mathcal{F}^{-1}(f+z)$ over all $z\in Z(f)$[15]. □

The ambiguity in the $\mathbb{Z}_2$-linear representation of Boolean functions makes computing the qubit count in non-adaptive, deterministic $l2$-MBQC a complex task in general. Since the number of terms in equation (22) grows doubly exponentially with n, a brute force search is generally infeasible. Moreover, the existence of a general solution as in the case of quadratic functions within stabiliser $l2$-MBQC via theorem 3 seems unlikely by comparison with similar problems in circuit synthesis. For instance, the minimal number of T-gates can be related to minimal number of mod-2 linear functions with odd coefficients. Solving the latter relates to minimum distance decoding in punctured Reed–Muller codes which is hard in general [26, 27].

Nevertheless, we can use theorem 7, together with the discrete Fourier transform in equation (21), to obtain an upper bound on the qubit count. In the remainder of this section, we exemplify this analysis in two cases: the n-bit δ-function and elementary symmetric functions.

Example 1 (n-bit δ-function). Given a general output function in its polynomial representation $o(\mathbf{i})$ we may use $\mathcal{F}^{-1}$ to obtain its representation in terms of $\mathbb{Z}_2$-linear basis functions and thus study its scaling behaviour. For monomials this decomposition is optimal with respect to minimising necessary $\mathbb{Z}_2$-linear terms.

Corollary 2. *In order to implement the monomial $f\colon\mathbb{Z}_2^n\to\mathbb{Z}_2$, $f(\mathbf{x})=\prod_{j=1}^n x_j$ in non-adaptive, deterministic $l2$-MBQC with a GHZ resource state one requires no fewer than $N=2^n-1$ qubits, i.e. $R_{\mathrm{GHZ}}(f)=N$.*

[15] We remark that for $d>2$ the minimisation over zero polynomials in equation (22) only provides an upper bound to R_{GHZ}. The reason is that the representation of the output function via $\mathbb{Z}_2$-linear terms in equation (7) breaks down for ld-MBQCs.

Proof (sketch). Note that f has degree $\deg(f) = n = W(\mathbf{b})$ for $\mathbf{b} = (1)^n := (1,\ldots,1) \in \mathbb{Z}_2^n$, hence, by equation (21) it has coefficient $\frac{1}{2^{W(\mathbf{b})-1}} = \frac{1}{2^{n-1}}$. Explicitly, the coefficients in the $\mathbb{Z}_2$-linear representation under the transformation $\mathcal{F}^{-1}$ read:

$$\mathcal{F}^{-1}\left(\prod_{j=1}^{n} x_j\right) \overset{\mathbf{b}=(1)^n}{=} \mathcal{F}^{-1}\left(\prod_{j=1}^{n} x_j^{b_j}\right) = \mathcal{F}^{-1}\left(\frac{1}{2^{W(\mathbf{b})-1}}\pi_{\mathbf{b}}\right)$$
$$= \sum_{\mathbf{a}\in\mathbb{Z}_2^n} \frac{1}{2^{W(\mathbf{b})-1}} \langle \phi_{\mathbf{a}}, \pi_{\mathbf{b}}\rangle \phi_{\mathbf{a}} = \frac{1}{2^{n-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^n} (-1)^{W(\mathbf{a})-1 \oplus_{j=1}^n a_j x_j}.$$

Since these terms are all odd multiples of $\frac{1}{2^{W(\mathbf{b})-1}}$, they can only be reduced by a zero term of degree at least n, however, there are no such terms in $Z(f)$, hence, the representation in terms of $\mathbb{Z}_2$-linear functions under the transformation $\mathcal{F}^{-1}$ is already optimal. Finally, note that the overlap with $\phi_{\mathbf{a}}$, $\mathbf{a} = 0$ can be implemented by post-processing, leaving $N = 2^n - 1$ non-zero terms. □

Corollary 2 reproduces proposition 1 in [22]. Note also that the n-bit δ-function arises from monomials by linear pre-composition in equation (13), hence, $R_{\mathrm{GHZ}}(\delta) = 2^n - 1$.

Example 2. (Elementary symmetric functions). While for monomials the transformation in equation (21) is already optimal in the number of non-zero coefficients (and thus in the number of qubits in the implementation as non-adaptive, deterministic $l2$-MBQC with a GHZ resource state), this is no longer the case for more general polynomials. Nevertheless, for certain symmetric functions the minimisation problem in theorem 7 under the equivalence relation in equation (22) simplifies.

As an example we consider elementary symmetric functions,

$$\Sigma_k^n(\mathbf{x}) = \sum_{\substack{i_1<\ldots<i_k \\ i_j\in\{1,\ldots,n\}}} x_{i_1}\ldots x_{i_k}, \qquad k \leqslant n.$$

Plugging Σ_k^n into the inverse transformation in equation (21) results in a total number of terms equal to $\sum_{l=1}^{k}\binom{n}{l}$. It turns out that we can minimise this number by (at least) $\binom{n}{k} - 1$ as follows. We add the zero polynomial $z \in Z(\Sigma_k^n)$ given by

$$z = (-2)^{n-k} x_1\ldots x_n + (-2)^{n-k-1} \sum_{\substack{i_1<\ldots<i_{n-1} \\ i_j\in\{1,\ldots,n\}}} x_{i_1}\ldots x_{i_{n-1}} + \ldots + (-2) \sum_{\substack{i_1<\ldots<i_{k+1} \\ i_j\in\{1,\ldots,n\}}} x_{i_1}\ldots x_{i_{k+1}}$$
$$= \sum_{l=0}^{n-k-1} (-2)^{n-k-l}\, \Sigma_l^n(\mathbf{x}).$$

By construction, $\mathcal{F}^{-1}(\Sigma_k^n)$ and $\mathcal{F}^{-1}(z)$ have the same (smallest) coefficient $\frac{1}{2^{k-1}}$, and we can thus compare the coefficients in their representation based on $\mathbb{Z}_2$-linear functions $\phi_{\mathbf{a}}$, $\mathbf{a} \in \mathbb{Z}_2^n$. Clearly, $\mathcal{F}^{-1}(\Sigma_k^n + z)$ contains the term $x_1 \oplus \ldots \oplus x_n$ and thus $C^{\Sigma_k^n+z}_{W(\mathbf{a})=n} = \frac{(-1)^{n-k}}{2^{k-1}}$. For the terms of length $k \leqslant m < n$, the coefficients $C^{\Sigma_k^n+z}_{W(\mathbf{a})=m}$ contain contributions from all higher degree terms in the polynomial representation of $\Sigma_k^n + z$:

$$C^{\Sigma_k^n+z}_{W(\mathbf{a})=m} = \frac{1}{2^{k-1}}(-1)^{(n-k)+(m-1)}\left(1 - \binom{n-m}{n-m-1} + \binom{n-m}{n-m-2} - \ldots + (-1)^{n-m}\right)$$
$$= \frac{1}{2^{k-1}}(-1)^{(n-k)+(m-1)}\left(\sum_{l=0}^{n-m}(-1)^l\binom{n-m}{n-m-l}\right) = 0.$$

Hence, with respect to monomials of degree $k \leqslant m$ in $\Sigma_k^n + z$, we have reduced the overall number of non-zero coefficients by $\binom{n}{k} - 1$. Note also that the coefficients of the remaining monomials of degree $1 \leqslant m < k$ are non-zero since there, the above sum is truncated and reads

$$C^{\Sigma_k^n+z}_{W(\mathbf{a})=m} = \frac{1}{2^{k-1}}(-1)^{(n-k)+(m-1)}\left(1 - \binom{n-m}{n-m-1} + \binom{n-m}{n-m-2} - \ldots + (-1)^{n-k}\binom{n-m}{k-m}\right)$$
$$= \frac{1}{2^{k-1}}(-1)^{(n-k)+(m-1)}\left(\sum_{l=0}^{n-k}(-1)^l\binom{n-m}{n-m-l}\right) \neq 0,$$

thus leaving a total of $\sum_{l=1}^{k-1}\binom{n}{l}+1$ terms in the $\mathbb{Z}_2$-linear representation, hence, $R_{\mathrm{GHZ}}(\Sigma_k^n)\leqslant\sum_{l=1}^{k-1}\binom{n}{l}+1$. Note also that: (a) $R_{\mathrm{GHZ}}(\Sigma_2^n)=\binom{n}{1}+1=n+1$ confirms theorem 6, since Σ_2^n is quadratic with $\mathrm{rk}(\Sigma_2^n)=n$ (see also proposition 2 in [22]), and (b) $R_{\mathrm{GHZ}}(\Sigma_n^n)=\sum_{l=1}^{n-1}\binom{n}{l}+1=2^n-1$ reproduces the minimal number of qubits within $l2$-MBQC for monomials in corollary 2 (see also proposition 1 in [22]). Comparing the latter, we draw the following conclusion from the above classification.

Corollary 3. *There are Boolean functions* $f,g:\mathbb{Z}_2^n\to\mathbb{Z}_2$ *such that* $\deg(f)>\deg(g)$, *yet* $R_{\mathrm{GHZ}}(f)<R_{\mathrm{GHZ}}(g)$.

Proof (sketch). This follows immediately by comparing the linear scaling (in the number of qubits) of quadratic Boolean functions according to theorem 6 with the exponential scaling of the symmetric function Σ_n^n and the n-qubit δ-function in corollary 2. For instance, $R_{\mathrm{GHZ}}(\Sigma_2^7)>R_{\mathrm{GHZ}}(\Sigma_3^3)$ despite $\deg(\Sigma_3^3)=3>2=\deg(\Sigma_2^7)$. □

In summary, we find that—unlike the contextuality threshold in [13] and the close correspondence with the Clifford hierarchy in theorem 5—the degree is not sufficient to compare Boolean functions with respect to their optimal representation in non-adaptive, deterministic $l2$-MBQC with a GHZ resource state. The computational classification of the latter thus possesses a rich substructure beyond the non-contextual case.

5. Discussion

We have assessed the ability to compute Boolean functions in non-adaptive, deterministic $l2$-MBQC under various resource restrictions. We have considered the computational power of stabiliser $l2$-MBQC, as well as $l2$-MBQC involving operations from higher levels in the Clifford hierarchy. We find that stabiliser $l2$-MBQCs can only compute quadratic functions with high probability (with the Anders and Browne example [20] being a prototypical example), while higher degree polynomials require operations from increasing levels in the Clifford hierarchy. In this way, we obtain a hierarchy of resources for non-adaptive, deterministic $l2$-MBQC beyond contextuality in [21].

In addition to the necessity of certain quantum operations in $l2$-MBQC for evaluating Boolean functions, we posed the resource-theoretic problem of determining the minimal number of qubits needed to implement a given Boolean function within non-adaptive, deterministic $l2$-MBQC. Clearly, this is an important and often limiting resource for near-term quantum devices. We characterise this problem by focusing on GHZ resource states and find that it too reveals a complex substructure to contextuality. At the heart of this is the (quantum Fourier) transformation mapping between two different representations of a Boolean function, as polynomial and as a $\mathbb{Z}_2$-linear sum. Interestingly, our characterisation closely resembles known hard problems in circuit synthesis and minimal distance coding in punctured Reed–Muller codes [26], suggesting that finding the minimal number of qubits is hard in general. Nevertheless, in certain cases the sharp bound can be found, such as for quadratic functions within stabiliser $l2$-MBQC.

Finally, we comment on some close connections and extensions of our results.

5.1. Adaptivity

The motivation for our setting was based on the recent results for shallow circuits, which constitute the first proof of a quantum–classical gap [15]. For this class of circuits, a constant depth circuit of one and two qubit gates is performed—that depends on the classical input bit string—followed by a measurement in the computational basis. Conversely, we consider a fixed unitary circuit (i.e. the resource state preparation), followed by a measurement that depends on the input bit string. This simplifies the analysis and allows us to derive strong bounds on resources in this scheme, but the same reasoning can also be applied in the adaptive case. As outlined in more detail in appendix H, within the latter the exponential scaling in qubit count, along with the necessity of non-Clifford gates for certain functions in the non-adaptive case quickly collapse. Nevertheless, one can sometimes trade off between space and time resources such as in [15]. We hope that the non-adaptive case can be leveraged to understand resource costs for more general adaptive computations.

5.2. Magic, contextuality, and cohomology

Both magic and contextuality can be classified by cohomology. In the former case, certain gates in the Dth level in the Clifford hierarchy $\mathcal{C}_N^D$ on N qubits can be classified by elements of the group cohomology $\mathcal{H}^D(\mathbb{Z}_2^N,U(1))$, following for example [42], while in the latter case, group cohomology also appears as a classifier for certain proofs of contextuality [7, 8, 43, 44]. As both magic and contextuality appear as resources for quantum computation, it is tempting to construct a unified framework for resource theories based on cohomology.

Recently, the role of magic in certain many-body systems known as symmetry-protected topological (SPT) phases[16] has been studied [46–48], whereby all states within a phase of matter possess magic. Such SPT phases have also been identified as resources for MBQC [49–54]. It would be interesting to study the role of many-body magic for computational universality, particularly with the example of [51], which is universal with only Pauli measurements. Further, it would be interesting to consider the role of contextuality in the fault-tolerant setting—particularly fault-tolerant MBQC [16, 55–59]—where non-Clifford operations require vastly more resources than Clifford operations (and indeed is the motivation for considering magic as a resource in the present setting).

Data availability statement

No new data were created or analysed in this study.

Acknowledgments

We acknowledge support from Australian Research Council via the Centre of Excellence in Engineered Quantum Systems (EQUS) Project Number CE170100009. MF was supported through a studentship in the Centre for Doctoral Training on Controlled Quantum Dynamics at Imperial College funded by the EPSRC, as well as through Grant Number FQXi-RFP-1807 from the Foundational Questions Institute and Fetzer Franklin Fund, a donor advised fund of Silicon Valley Community Foundation, and ARC Future Fellowship FT180100317. ETC's technical contributions were made while at the University of Sheffield. SDB acknowledges additional support from the Australian Research Council via Project Number DP220101771.

Appendix A. Proof of theorem 1

The proof consists of two parts: first, we prove equation (7), assuming that local measurement operators are of the form in equation (6), i.e. $M_k = X(\mathrm{e}^{i\pi\vartheta_k})$; second, we prove that measurements are necessarily of this form.

For the first part, note the relation between eigenstates of $M_k = X(\mathrm{e}^{i\pi\vartheta_k})$ and the computational basis:

$$|m_k\rangle_{\vartheta_k} = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{m_k}\mathrm{e}^{i\pi\vartheta_k}|1\rangle).$$

Conversely, the computational basis expressed in terms of eigenstates of $X(\mathrm{e}^{i\pi\vartheta_k})$ reads

$$|q_k\rangle = \frac{1}{\sqrt{2}}\mathrm{e}^{-i\pi q_k\vartheta_k}\sum_{m=0}^{1}(-1)^{q_k m_k}|m_k\rangle_{\vartheta_k}. \tag{A1}$$

We encode the choice of local measurement operators by $M_k(c_k(\mathbf{i})) = X(\mathrm{e}^{i\pi c_k(\mathbf{i})\vartheta_k})$ for linear functions $c_k : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and parameters $\vartheta_k \in [0,1)$[17]. In particular, note that $M(0) = X$. Rewriting the N-qubit GHZ resource state in equation (4) in terms eigenstates of the local measurement bases thus yields

$$\begin{aligned}
|\psi\rangle = \frac{1}{\sqrt{2}}\sum_{q=0}^{1}|q\rangle^{\otimes N} &= \frac{1}{\sqrt{2}}\sum_{q=0}^{1}\otimes_{k=1}^{N}\left(\frac{1}{\sqrt{2}}\mathrm{e}^{-i\pi q c_k(\mathbf{i})\vartheta_k}\sum_{m_k=0}^{1}(-1)^{q m_k}|m_k\rangle_{\vartheta}\right)\\
&= \left(\frac{1}{\sqrt{2}}\right)^{N+1}\sum_{q=0}^{1}\left(\sum_{\mathbf{m}\in\mathbb{Z}_2^N}(-1)^{q(\sum_{k=1}^{N}m_k - o'(\mathbf{i}))}\otimes_{k=1}^{N}|m_k\rangle_{\vartheta}\right)\\
&= \left(\frac{1}{\sqrt{2}}\right)^{N-1}\left(\sum_{\substack{\mathbf{m}\in\mathbb{Z}_2^N,\\ \oplus_{k=1}^{N}m_k = o'(\mathbf{i})}}\otimes_{k=1}^{N}|m_k\rangle_{\vartheta}\right),
\end{aligned} \tag{A2}$$

where we defined $(-1)^{o'(\mathbf{i})} = \mathrm{e}^{-i\pi q c_k(\mathbf{i})\vartheta_k}$ and we used that $|\psi\rangle$ is an eigenstate of the global measurement operators $M(\mathbf{i}) = \otimes_{k=1}^{N}M_k(c_k(\mathbf{i}))$. Finally, since the output function of the non-adaptive, deterministic $l2$-MBQC reads $o(\mathbf{i}) = \oplus_{k=1}^{N}m_k$, we find $o' = o$, hence[18],

[16] We remark that such phases are also classified by group cohomology [45].

[17] In other words, $c_k = \phi_{\mathbf{a}_k}$ with $0 \neq \mathbf{a}_k \in \mathbb{Z}_2^n$ for every $k \in \{1,\ldots,N\}$ (see section 4.2.1).

[18] A similar relation has been derived in equation (10) in [32] for three-qubit GHZ states.

$$o(\mathbf{i}) = \sum_{k=1}^{N} c_k(\mathbf{i})\vartheta_k \pmod 2.$$

We are left to show the second part: that every local measurement operator is of the form in equation (6)[19]. To see this, note that the global measurement operators $M(\mathbf{i}) = \otimes_{k=1}^{N} M_k(c_k(\mathbf{i}))$ are such that $|\psi\rangle$ is a parity eigenstate of $M(\mathbf{i})$ for all inputs $\mathbf{i} \in \mathbb{Z}_2^n$. For every $\mathbf{i} \in \mathbb{Z}_2^n$, rewrite $|\psi\rangle$ in the local eigenbases corresponding to the $M_k(c_k(\mathbf{i}))$. This yields a superposition of product states $|\mathbf{m}\rangle_{\varphi,\vartheta} = \otimes_{k=1}^{N} |m_k\rangle_{\varphi,\vartheta}$, where we again denote every product state by the Boolean vector $\mathbf{m} \in \mathbb{Z}_2^N$ such that

$$|0\rangle_{\varphi,\vartheta} = \sin(\varphi)|0\rangle + e^{\pi i\vartheta}\cos(\varphi)|1\rangle \qquad |1\rangle_{\varphi,\vartheta} = \cos(\varphi)|0\rangle - e^{\pi i\vartheta}\sin(\varphi)|1\rangle.$$

In particular, note that $|m\rangle_{\vartheta} = |m\rangle_{\frac{\pi}{4},\vartheta}$. Clearly, the product state $|\mathbf{m}\rangle_{\varphi,\vartheta}$ has parity $m := \oplus_{k=1}^{N} m_k$. Moreover, the coefficient to the product state $|\mathbf{m}\rangle_{\varphi,\vartheta}$ reads

$$_{\varphi,\vartheta}\langle \mathbf{m}|\psi\rangle = \frac{1}{\sqrt{2}}\left(\prod_{k=1}^{N}\Phi^{m_k}(\varphi_k) + (-1)^m e^{\pi i\sum_{k=1}^{N}\vartheta_k}\prod_{k=1}^{N}\Phi^{m_k\oplus 1}(\varphi_k)\right), \tag{A3}$$

where we defined $\Phi^0(\varphi_k) = \sin(\varphi_k)$ and $\Phi^1(\varphi_k) = \cos(\varphi_k)$, and the two summands correspond to the inner product between the two summands in $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ with $|\mathbf{m}\rangle_{\varphi,\vartheta}$[20].

We have a parity eigenstate if $_{\varphi,\vartheta}\langle \mathbf{m}|\psi\rangle = 0$ for all $\mathbf{m}$ with $m \neq o$ for some $o \in \mathbb{Z}_2$. We thus obtain $\frac{2^N}{2}$ constraints from equation (A3), both on absolute values and phases of the form

$$\prod_{k=1}^{N}\Phi^{m_k}(\varphi_k) + (-1)^m e^{\pi i\sum_{k=1}^{N}\vartheta_k}\prod_{k=1}^{N}\Phi^{m_k\oplus 1}(\varphi_k) = 0 \qquad \forall \mathbf{m} \in \mathbb{Z}_2^N \text{ s.t. } m \neq o. \tag{A4}$$

Clearly, the constraints on absolute values are satisfied for $\varphi = \frac{\pi}{4}$. Moreover, for $N \geqslant 3$ all solutions are of this form. First, for $N \geqslant 3$ odd, consider pairs of constraints in equation (A3) of the same parity $m = \oplus_{k=1}^{N} m_k$. Specifically, given any $\mathbf{m} \in \mathbb{Z}_2^N$ and another vector arising from $\mathbf{m}$ by flipping all bits except the one at site k. Then we have the following pair of constraints,

$$\Phi^{m_k}(\varphi_k)\prod_{k'\neq k}\Phi^{m_{k'}}(\varphi_{k'}) + (-1)^m e^{\pi i\sum_{k=1}^{N}\vartheta_k}\Phi^{m_k\oplus 1}(\varphi_k)\prod_{k'\neq k}\Phi^{m_{k'}\oplus 1}(\varphi_{k'}) = 0$$
$$\Phi^{m_k}(\varphi_k)\prod_{k'\neq k}\Phi^{m_{k'}\oplus 1}(\varphi_{k'}) + (-1)^m e^{\pi i\sum_{k=1}^{N}\vartheta_k}\Phi^{m_k\oplus 1}(\varphi_k)\prod_{k'\neq k}\Phi^{m_{k'}}(\varphi_{k'}) = 0$$

These imply $\frac{\prod_{k'\neq k}\Phi^{m_{k'}}(\varphi_{k'})}{\prod_{k'\neq k}\Phi^{m_{k'}\oplus 1}(\varphi_{k'})} = (-1)^{m+1}e^{\pi i\sum_{k=1}^{N}\vartheta_k}\frac{\Phi^{m_k\oplus 1}(\varphi_k)}{\Phi^{m_k}(\varphi_k)} = \frac{\prod_{k'\neq k}\Phi^{m_{k'}\oplus 1}(\varphi_{k'})}{\prod_{k'\neq k}\Phi^{m_{k'}}(\varphi_{k'})}$ and thus $|\sin(\varphi_k)| = |\cos(\varphi_k)|$, hence, $\varphi_k = \frac{\pi}{4}$. For N even, similar constraints yield $|\Phi^{m_k}(\varphi_k)\Phi^{m_{k'}}(\varphi_{k'})| = |\Phi^{m_k\oplus 1}(\varphi_k)\Phi^{m_{k'}\oplus 1}(\varphi_{k'})|$. For $N \neq 2$ we thus again find $\varphi_k = \frac{\pi}{4}$, since for another pair of constraints in equation (A3) also $|\Phi^{m_k}(\varphi_k)\Phi^{m_{k'}\oplus 1}(\varphi_{k'})| = |\Phi^{m_k+\oplus 1}(\varphi_k)\Phi^{m_{k'}}(\varphi_{k'})|$, hence, $\frac{|\Phi^{m_{k'}}(\varphi_{k'})|}{|\Phi^{m_{k'}\oplus 1}(\varphi_{k'})|} = \frac{|\Phi^{m_k\oplus 1}(\varphi_k)|}{|\Phi^{m_k}(\varphi_k)|} = \frac{|\Phi^{m_{k'}\oplus 1}(\varphi_{k'})|}{|\Phi^{m_{k'}}(\varphi_{k'})|}$. Finally, for all $N > 2$ we find $(-1)^{m+1}e^{\pi i\sum_{k=1}^{N}\vartheta_k} = 1$, hence, $e^{\pi i\sum_{k=1}^{N}\vartheta_k} = (-1)^{m+1} = (-1)^o$, which recovers the first part of the proof.

Appendix B. Proof of Lemma 1

Consider the resource state given by the N-qubit GHZ state $|\psi\rangle$ in equation (4) with $N = 2^n - 1$, and consider the measurement procedure $0 \to M(0) = X$ and $1 \to M(1) = X(e^{i\pi\vartheta})$ with measurements in equation (6), which we re-state here for convenience,

$$X(e^{i\pi\vartheta}) = \begin{pmatrix} 0 & e^{-i\pi\vartheta} \\ e^{i\pi\vartheta} & 0 \end{pmatrix} \qquad X(e^{i\pi\vartheta})|q\rangle = e^{i\pi(1-2q)\vartheta}|q\oplus 1\rangle.$$

As before, the measurement operators $M_k(c_k(\mathbf{i})) = X(e^{i\pi c_k(\mathbf{i})\vartheta_k})$ are specified by linear functions $c_k : \mathbb{Z}_2^n \to \mathbb{Z}_2$. In particular, we set

$$c_k(\mathbf{i}) := \phi_{\mathbf{a}}(\mathbf{i}) = \oplus_{j=1}^{n} a_j i_j, \qquad \mathbf{0} \neq \mathbf{a} \in \mathbb{Z}_2^n.$$

[19] This is essentially the same argument as the one given in the proof of theorem 4 in [32]. We add it here for completeness.
[20] Note that local measurements in the computational basis only change the resource state and can thus be neglected.

In other words, the 2^n-1 qubits in $|\psi\rangle$ are indexed by vectors $\mathbf{0}\neq\mathbf{a}\in\mathbb{Z}_2^n$. We prove that this indeed allows us to compute the n-bit δ-function in equation (8) for a suitable $\vartheta_k=\vartheta$.

Note that by symmetry the output function o can be re-written as $o(\mathbf{i})=\frac{1}{2^{n-1}}\sum_{\mathbf{a}\in\mathbb{Z}_2^n}\phi_{\mathbf{a}}(\mathbf{i})=\frac{1}{2^{n-1}}\sum_{\mathbf{a}\in\mathbb{Z}_2^n}\phi_{\mathbf{i}}(\mathbf{a})$. Since $\phi_{\mathbf{i}}:\mathbb{Z}_2^n\to\mathbb{Z}_2$ for $\mathbf{0}\neq\mathbf{i}\in\mathbb{Z}_2^n$ is a non-zero linear function, by the rank-nullity theorem, the rank of its kernel is $n-1$. In turn, it follows that the number of terms contributing to the sum $\sum_{\mathbf{a}\in\mathbb{Z}_2^n}\phi_{\mathbf{i}}(\mathbf{a})$ reads 2^{n-1} for every $0\neq\mathbf{i}\in\mathbb{Z}_2^n$, while it evaluates to zero for $\mathbf{i}=\mathbf{0}$[21]. Consequently, by fixing the parameter

$$\vartheta=2^{-(n-1)}\pmod 2\iff(\mathrm{e}^{\pi i\vartheta})^{2^{n-1}}=-1, \tag{B1}$$

we find $o(\mathbf{i})=\delta(\mathbf{i})\oplus 1$. The n-bit δ-function is then computed by straightforward post-processing.

Appendix C. Universality of non-adaptive, deterministic *ld*-MBQC with *d* prime

In this section we show that any function $f:\mathbb{Z}_d^n\to\mathbb{Z}_d$ for d prime, can be implemented using a non-adaptive, deterministic ld-MBQC. We will follow a similar strategy to the proof of theorem 2 in appendix A. We start by choosing measurement operators for prime dimension d similar to those in in equation (6), namely

$$M(0)|q\rangle:=X|q\rangle=|q\oplus 1\rangle,\qquad M(c)|q\rangle:=\theta(c)\chi^{cq^{d-1}}|q\oplus 1\rangle\quad\chi,\theta(c)\in U(1),\ 1\leqslant c\leqslant d-1.$$

If we set $\theta(c)^d=\chi^{-(d-1)c}$ we have $M(c)^d=1$ for all $c\in\mathbb{Z}_d$. With $\omega=\mathrm{e}^{\frac{2\pi i}{d}}$, we find the following eigenstates,

$$\begin{aligned}|m\rangle_{\theta(c)}&=\frac{1}{\sqrt{d}}(|0\rangle+\omega^{-m}\theta(c)|1\rangle+(\omega^{-m}\theta(c))^2\chi^c|2\rangle+\ldots+(\omega^{-m}\theta(c))^{d-1}(\chi^c)^{d-2}|d-1\rangle)\\&=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}(\omega^{-m}\theta(c))^q(\chi^c)^{(q-1)q^{d-1}}|q\rangle,\end{aligned}$$

with corresponding expressions in terms of computational basis states,

$$|q\rangle=\frac{1}{\sqrt{d}}\frac{1}{\theta(c)^q\chi^{c(q-1)q^{d-1}}}\sum_{m=0}^{d-1}\omega^{qm}|m\rangle_{\theta(c)},\quad\forall c\in\mathbb{Z}_d. \tag{C1}$$

We fix the resource state to be the N-qudit GHZ state for $N=d^n-1$,

$$|\psi\rangle=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}|q\rangle^{\otimes N}.$$

Assume that the output function $o:\mathbb{Z}_d^n\to\mathbb{Z}_d$ is encoded in the phase relations as follows

$$\prod_{1\leqslant k\leqslant d^n-1}\theta(c_k(\mathbf{i}))^q\chi^{c_k(\mathbf{i})(q-1)q^{d-1}}=\omega^{qo(\mathbf{i})}. \tag{C2}$$

Rewriting $|\psi\rangle$ in terms of the respective measurement bases via equation (C1) then yields

$$\begin{aligned}|\psi\rangle&=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\otimes_{k=1}^N\left(\frac{1}{\sqrt{d}}\frac{1}{\theta(c_k(\mathbf{i}))^q\chi^{c_k(\mathbf{i})(q-1)q^{d-1}}}\sum_{m_k=0}^{d-1}\omega^{qm_k}|m_k\rangle_{\theta(c_k)}\right)\\&=\left(\frac{1}{\sqrt{d}}\right)^{N+1}\sum_{q=0}^{d-1}\left(\omega^{-qo(\mathbf{i})}\sum_{\mathbf{m}\in\mathbb{Z}_d^N}\otimes_{k=1}^N\omega^{qm_k}|m_k\rangle_{\theta(c_k)}\right)\\&=\left(\frac{1}{\sqrt{d}}\right)^{N+1}\sum_{q=0}^{d-1}\left(\sum_{\mathbf{m}\in\mathbb{Z}_d^N}\omega^{q(\sum_{k=1}^N m_k-o(\mathbf{i}))}\otimes_{k=1}^N|m_k\rangle_{\theta(c_k)}\right)\\&=\left(\frac{1}{\sqrt{d}}\right)^{N-1}\sum_{\substack{\mathbf{m}\in\mathbb{Z}_d^N,\\ \sum_{k=1}^N m_k=o(\mathbf{i})\pmod d}}\otimes_{k=1}^N|m_k\rangle_{\theta(c_k)}.\end{aligned}$$

[21] We thank an anonymous referee for improving an earlier version of the argument.

It follows that $|\psi\rangle$ is a parity $\sum_{k=1}^{N} m_k = o(\mathbf{i}) \pmod d$ eigenstate for all operators $M(\mathbf{i})$ with $\mathbf{i} \in \mathbb{Z}_d^n$.

We thus want to show that we can satisfy the phase relations in equation (C2) for any $o : \mathbb{Z}_d^n \to \mathbb{Z}_d$ by choosing suitable linear functions for the measurement settings c_k. Similar to the case of Boolean functions in section 4.2.1, we take as a basis for the space of functions $f : \mathbb{Z}_d^n \to \mathbb{Z}_d$ all (non-zero) linear functions of the form $\phi_{\mathbf{a}}(\mathbf{i}) = \oplus_{j=1}^{n} a_j i_j$ for $\mathbf{0} \neq \mathbf{a} \in \mathbb{Z}_d^n$.

First, consider a single non-zero entry, $\mathbb{Z}_d^n \ni \mathbf{i} = (i_1, 0, \ldots, 0)$ and let $\mathbf{a}$ such that $a_1 \neq 0$. There is $(d-1)$-fold degeneracy resulting from changing $\mathbf{a}$ to $\mathbf{a}'$ such that $a_1' = r a_1$ for some $0 \neq r \in \mathbb{Z}_d$ and $a_j' = a_j$ for all $j > 2$. This degeneracy yields a the local phase factor[22]

$$\phi(q) := \prod_{c=0}^{d-1} \theta(c)^q \chi^{c(q-1)q^{d-1}} = \theta^q \chi^{\sum_{c=0}^{d-1} c(q-1)q^{d-1}} = \theta^q \chi^{\frac{d(d-1)}{2}(q-1)q^{d-1}}, \tag{C3}$$

where we set $\theta := \prod_{c=0}^{d-1} \theta(c)$. Furthermore, the number of functions $\phi_{\mathbf{a}}$ with $a_1 \neq 0$ counts $\sum_{k=0}^{n-1} \binom{n-1}{k} (d-1)^k = d^{n-1}$, hence, the overall phase factor in equation (C2) reads $\phi(q)^{d^{n-1}}$.

For the general case, we again write the output function as $o(\mathbf{i}) = \frac{1}{d^{n-1}} \sum_{\mathbf{a} \in \mathbb{Z}_d^n} \phi_{\mathbf{a}}(\mathbf{i}) = \frac{1}{d^{n-1}} \sum_{\mathbf{a} \in \mathbb{Z}_d^n} \phi_{\mathbf{i}}(\mathbf{a})$, and invoke the rank-nullity theorem to deduce the rank of the kernel of every function $\phi_{\mathbf{i}}$ to be $n-1$. The number of terms contributing to the sum $\sum_{\mathbf{a} \in \mathbb{Z}_d^n} \phi_{\mathbf{i}}(\mathbf{a})$ thus reads 0 for $\mathbf{i} = \mathbf{0}$ and $(d-1)d^{n-1}$ for every $\mathbf{0} \neq \mathbf{i} \in \mathbb{Z}_d^n$, where the first factor $(d-1)$ will result in the phase $\phi(q)$ from equation (C3), such that the overall phase is $\phi(q)^{d^{n-1}}$.

Finally, we relate this global phase factor to the local phases $\theta(c)$ and χ. Since,

$$\theta^d = \left(\prod_{c=1}^{d-1} \theta(c) \right)^d = \prod_{c=1}^{d-1} \chi^{-(d-1)c} = \chi^{-(d-1)\sum_{k=1}^{d-1} c} = \chi^{-\frac{d(d-1)^2}{2}}, \tag{C4}$$

we need to choose $\theta(c)$ for $1 \leqslant c \leqslant d-1$ such that $\theta = \chi^{-\frac{(d-1)^2}{2}}$, e.g. $\theta(c) := \chi^{-\frac{c(d-1)}{d}}$. Next, we insert equation (C4) into equation (C3) and compute the global phase factors,

$$\phi(q)^{d^{n-1}} = \left(\chi^{-\frac{(d-1)^2}{2} q} \cdot \chi^{(q-1)\frac{d(d-1)}{2} q^{d-1}} \right)^{d^{n-1}} = \begin{cases} 1 & \text{if } q = 0 \\ \chi^{-\frac{d^{n-1} d(d-1)}{2}} \left(\chi^{-d^{n-1}\frac{(d-1)}{2}} \right)^q & \text{if } 1 \leqslant q \leqslant d-1 \end{cases}.$$

We may thus set $\chi^{-\frac{d^{n-1}(d-1)}{2}} = \omega$ from which it follows that $\left(\chi^{-\frac{d^{n-1}(d-1)}{2}} \right)^d = 1$, hence, $\phi(q)^{d^{n-1}} = \omega^q$. We obtain the following output function,

$$o(\mathbf{i}) = \begin{cases} 0 & \text{if } \mathbf{i} = 0 \\ 1 & \text{if } \mathbf{i} \neq 0 \end{cases}, \tag{C5}$$

from which we compute $\delta(\mathbf{i}) = (d-1)o(\mathbf{i}) + 1$ by simple post-processing.

Finally, as in theorem 2 the result follows since every function can be written as a sum of δ-functions, $f(\mathbf{i}) = \sum_{\mathbf{j} \in \mathbb{Z}_d^n} f_{\mathbf{j}} \delta(\mathbf{i} - \mathbf{j})$, $f_{\mathbf{j}} \in \mathbb{Z}_d$ for all inputs $\mathbf{i} \in \mathbb{Z}_d^n$.

Appendix D. Proof of Theorem 3

Recall from definition 1 that a non-adaptive, deterministic, level-2 (i.e. stabiliser) *l*2-MBQC is specified by the following data: $P \in \mathrm{Mat}(N \times n, \mathbb{Z}_2)$ is the classical, linear pre-processing; $|\psi\rangle$ is an N-qubit stabiliser resource state; and $M_k(c_k(\mathbf{i}))$ is a single qubit Pauli operator for every $c_k(\mathbf{i}) = P\mathbf{i}$, input $\mathbf{i} \in \mathbb{Z}_2^n$ and $k \in \{1, \ldots, N\}$. Given a stabiliser *l*2-MBQC as above, note that the exact same measurement statistics are obtained if we instead rotate $|\psi\rangle$ by some local Clifford operations and conjugate the measurement settings by the inverse Clifford operations. Therefore, we can assume without loss of generality that $M_k(0) = X_k$ and $M_k(1) = Z_k$. We denote $M(\mathbf{c} = P\mathbf{i})$ to be the tensor product of unitaries measured in this canonical choice.

Consider the quadratic function $f(\mathbf{x}) = \sum_{i=1}^{n} l_i x_i + \sum_{i<j} q_{i,j} x_i x_j$ with associated matrix Q. We require

$$M(\mathbf{0})|\psi\rangle = (+1)|\psi\rangle \tag{D1}$$

[22] Note that we are abusing notation slightly by using modulo-d arithmetic over phases with different periods. However, as the functions are computed classically the input is always an element in $\mathbb{Z}_d$.

$$M(P\mathbf{x})|\psi\rangle = (-1)^{f(\mathbf{x})}|\psi\rangle \quad \forall \mathbf{0} \neq \mathbf{x} \in \mathbb{Z}_2^n. \tag{D2}$$

If we denote by $\mathcal{S}$ the stabiliser of $|\psi\rangle$, this can be restated as $M(\mathbf{0}) \in \mathcal{S}$ and $(-1)^{f(\mathbf{x})}M(P\mathbf{x}) \in \mathcal{S}$ for all $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}_2^n$. Under group closure of the stabiliser we have $(-1)^{f(\mathbf{x})}M(P\mathbf{x})M(\mathbf{0}) \in \mathcal{S}$. Note that $M(\mathbf{0}) = X^{\otimes N}$ and $M(P\mathbf{x})$ will be a tensor product of X and Z operators. Therefore, the product $M(P\mathbf{x})M(\mathbf{0})$ is a tensor product of the identity and Y operators, possibly with some extra phase. We define

$$Q(\mathbf{u}) := \bigotimes_{k=1}^{N} (iY)^{u_k} = i^{W(\mathbf{u})} \bigotimes_{k=1}^{N} Y^{u_k}, \tag{D3}$$

where we recall that $W(\mathbf{u}) := |\{k \in \{1,\ldots,N\} \mid u_k \neq 0\}|$ denotes the *Hamming weight* of $\mathbf{u} \in \mathbb{Z}_2^N$, and we observe that $M(P\mathbf{x})M(\mathbf{0}) = Q(P\mathbf{x})$. Therefore, $(-1)^{f(\mathbf{x})}Q(P\mathbf{x}) \in \mathcal{S}$ for all $0 \neq \mathbf{x} \in \mathbb{Z}_2^n$. In particular, for $\mathbf{x} = (1,0,\ldots)^T$ and $\mathbf{x} = (0,1,\ldots)^T$ we have $(-1)^{l_1}Q(\mathbf{p}_1) \in \mathcal{S}$, $(-1)^{l_2}Q(\mathbf{p}_2) \in \mathcal{S}$, where we write $\mathbf{p}_j$ to denote the j^{th} column of P.

Assuming the stabiliser is abelian, $Q(P\mathbf{x})$ ought to be Hermitian and so $W(P\mathbf{x}) = 0 \pmod 2$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. Next we note that we have the relation

$$Q(\mathbf{u})Q(\mathbf{v}) = (-1)^{\mathbf{u}\cdot\mathbf{v}}Q(\mathbf{u} \oplus \mathbf{v}). \tag{D4}$$

Since $(-1)^{l_1}Q(\mathbf{p}_1) \in \mathcal{S}$ and $(-1)^{l_2}Q(\mathbf{p}_2) \in \mathcal{S}$, we have $(-1)^{l_1+l_2}Q(\mathbf{p}_1)Q(\mathbf{p}_2) \in \mathcal{S}$ by group closure. Using the above relation, this entails that $(-1)^{l_1+l_2+\mathbf{p}_1\cdot\mathbf{p}_2}Q(\mathbf{p}_1 \oplus \mathbf{p}_2) \in \mathcal{S}$, where $\mathbf{p}_1.\mathbf{p}_2$ is the dot product of these vectors. However, we also know that $(-1)^{f(1,1,\ldots)}Q(P(1,1,0,\ldots,0)^T) \in \mathcal{S}$. These two results are only compatible if

$$(-1)^{l_1+l_2+\mathbf{p}_1\cdot\mathbf{p}_2} = (-1)^{l_1+l_2+q_{1,2}} \tag{D5}$$

and so $\mathbf{p}_1.\mathbf{p}_2 = q_{1,2} \pmod 2$. A similar argument shows that for all $i,j \in \{1,\ldots,n\}$ we must have

$$\mathbf{p}_i.\mathbf{p}_j = q_{i,j} \pmod 2 \tag{D6}$$

$$W(\mathbf{p}_i) = 0 \pmod 2.$$

We have so far checked inputs $\mathbf{x} \in \mathbb{Z}_2^n$ with Hamming weight $W(\mathbf{x}) \leqslant 2$. More generally, let $\mathbf{x} \in \mathbb{Z}_2^n$ be arbitrary such that $P\mathbf{x} = \bigoplus_{i=1}^n \mathbf{p}_i x_i$. For every $i \in \{1,\ldots,n\}$ with $x_i = 1$, we find $(-1)^{l_i}Q(\mathbf{p}_i) \in \mathcal{S}$ as before, hence, by group closure

$$\prod_{i=1}^{n} (-1)^{l_i x_i} Q(\mathbf{p}_i x_i) = (-1)^{\sum_{i=1}^n l_i x_i} \prod_{i=1}^{n} Q(\mathbf{p}_i x_i) \in \mathcal{S}. \tag{D7}$$

Repeated application of equation (D4) then yields

$$\begin{aligned} \prod_{i=1}^{n} Q(\mathbf{p}_i x_i) &= (-1)^{\sum_{i<j} \mathbf{p}_i.\mathbf{p}_j x_i x_j} Q\left(\bigoplus_{i=1}^{n} \mathbf{p}_i x_i\right) \\ &= (-1)^{\sum_{i<j} q_{i,j} x_i x_j} Q(P\mathbf{x}), \end{aligned} \tag{D8}$$

where in the second line we have used $\mathbf{p}_i.\mathbf{p}_j = q_{i,j}$ from equation (D6). Combining equations (D7) and (D8) gives

$$(-1)^{\sum_{i=1}^n l_i x_i + \sum_{i<j} q_{i,j} x_i x_j} Q(P\mathbf{x}) = (-1)^{f(\mathbf{x})} Q(P\mathbf{x}) \in \mathcal{S}. \tag{D9}$$

This proves that any quadratic function can be computed within non-adaptive, deterministic, level-2 $l2$-MBQC. Conversely, for any Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ the above argument shows that only its quadratic part can be computed deterministically. Hence, f can be computed by a non-adaptive, deterministic, level-2 $l2$-MBQC if and only if f is quadratic.

Appendix E. Proof of Theorem 4

In this section, we prove theorem 4, which bounds the success probability of non-adaptive, level-2 (i.e. stabiliser) $l2$-MBQC. Let $f:\mathbb{Z}_2^n\to\mathbb{Z}_2$ be a Boolean function. Then the closest Boolean function (in Hamming distance) which can be deterministically computed in non-adaptive, level-2 $l2$-MBQC is a quadratic function. Hence, the success probability is determined by the non-quadraticity of f if we restrict to deterministic $l2$-MBQC (recall corollary 1). However, it is not immediately clear that a deterministic $l2$-MBQC necessarily performs best, i.e. it maximises the success probability. Here we show that for non-adaptive, level-2 $l2$-MBQC this is indeed the case.

Let A be a non-adaptive, level-2 $l2$-MBQC that given $\mathbf{x}\in\mathbb{Z}_2^n$, outputs $f(\mathbf{x})$ with probability $p_A(\mathbf{x})$ so that

$$P_{\text{succ}}(A)=\frac{1}{2^n}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}p_A(\mathbf{x}). \tag{E1}$$

If A is probabilistic, we let $D_A:=\{\mathbf{x}\in\mathbb{Z}_2^n\mid p_A(\mathbf{x})\in\{0,1\}\}$ denote the subset of values such that the outcome is deterministic. We denote the complement by $R_A:=\mathbb{Z}_2^n\backslash D_A$, which is the random subset on which $0<p_A(\mathbf{x})<1$. If R_A is empty, A has deterministic outcomes and we can deploy corollary 1. We will show that when R_A is not empty, we can find a deterministic (non-adaptive, level-2) $l2$-MBQC $A^\star$ with $P_{\text{succ}}(A^\star)\geqslant P_{\text{succ}}(A)$.

Lemma 2. *For all* $\mathbf{x}\in R_A$, $p_A(\mathbf{x})=1/2$.

Proof (sketch). For every $\mathbf{x}\in\mathbb{Z}_2^n$, let $S(\mathbf{x})$ be the observable measured. Assuming the stabiliser state has stabiliser $\mathcal{S}$, there are two possible cases, either

(a) $S(\mathbf{x})\in\mathcal{S}$ or $-S(\mathbf{x})\in\mathcal{S}$ and so $p_A(\mathbf{x})\in\{0,1\}$ and $\mathbf{x}\in D_A$;
(b) or $S(\mathbf{x})$ anti-commutes with some element in $\mathcal{S}$ in which case $p_A(\mathbf{x})=1/2$ and $\mathbf{x}\in R_A$.

This proves the lemma. □

From lemma 2 it follows that

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n}p_A(\mathbf{x})=\frac{1}{2}|R_A|+\sum_{\mathbf{x}\in D_A}p_A(\mathbf{x})=\frac{1}{2}(2^n-2^m)+\sum_{\mathbf{x}\in D_A}p_A(\mathbf{x}), \tag{E2}$$

where we have used that $|R_A|=2^n-|D_A|=:2^n-2^m$.

Lemma 3. *For all* $\mathbf{x},\mathbf{y},\mathbf{z}\in D_A$, $\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}\in D_A$.

Proof (sketch). Consider the measurement $S(\mathbf{x})$. W.l.o.g we can assume it has the form

$$S(\mathbf{x})=\otimes_k X_k(iZ_k)^{[P\mathbf{x}]_k}, \tag{E3}$$

where P is the matrix describing the ($\mathbb{Z}_2$-linear) pre-processing (see definition 1). From this we find that

$$S(\mathbf{x})S(\mathbf{y})S(\mathbf{z})\propto\otimes_j X_j(iZ_j)^{[P(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z})]_j}=S(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}), \tag{E4}$$

where the proportionality constant can be worked out but is not important. Assuming $\mathbf{x},\mathbf{y},\mathbf{z}\in D_A$ entails that $S(\mathbf{x}),S(\mathbf{y})$ and $S(\mathbf{z})$ all commute with $\mathcal{S}$. Therefore, $S(\mathbf{x})S(\mathbf{y})S(\mathbf{z})$ must also commute with $\mathcal{S}$, and by equation (E4) we know $S(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z})$ must also commute with $\mathcal{S}$. Therefore, $\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}\in D_A$. □

We remark that this is the structure of an affine space. Recall that an affine space is a set $\{\mathbf{y}\oplus\mathbf{w}:\mathbf{y}\in L\}$ where L is a linear space and $\mathbf{w}$ is some constant shift. Let $\mathbf{w}\in D_A$ arbitrary, and define $L_A^{\mathbf{w}}=\{\mathbf{x}\oplus\mathbf{w}:\mathbf{x}\in D_A\}$. The space $L_A^{\mathbf{w}}$ is linear: from $\mathbf{x}\in L_A^{\mathbf{w}}\Rightarrow(\mathbf{x}\oplus\mathbf{w})\in D_A$ and $\mathbf{y}\in L_A^{\mathbf{w}}\Rightarrow(\mathbf{y}\oplus\mathbf{w})\in D_A$ it follows that $\mathbf{x}\oplus\mathbf{y}\in L_A^{\mathbf{w}}$ since, by lemma 3, $(\mathbf{x}\oplus\mathbf{w})\oplus(\mathbf{y}\oplus\mathbf{w})\oplus\mathbf{w}=(\mathbf{x}\oplus\mathbf{y})\oplus\mathbf{w}\in D_A$. Hence, D_A is an affine space.

Since D_A is an affine space, we can define an invertible, affine transformation $\Phi:\mathbb{Z}_2^n\to\mathbb{Z}_2^n$ such that the image $\Phi(D_A)$ corresponds to the vectors of the form $(u_1,\ldots,u_m,0,\ldots,0)\in\mathbb{Z}_2^n$. It is convenient to change the problem under this transformation, in particular, we define the new target function by $g(\Phi(\mathbf{x}))=f(\mathbf{x})$. We also define the truncated function $\tilde{g}:\mathbb{Z}_2^m\to\mathbb{Z}_2$ such that $\tilde{g}(\mathbf{u})=g(u_1,\ldots,u_m,0,\ldots,0)$.

Since A is deterministic over D_A, by theorem 3 it defines a quadratic Boolean function $\tilde{q}_A : \mathbb{Z}_2^m \to \mathbb{Z}_2$ on inputs in $\Phi(D_A)$. Clearly, the success probability (with respect to the different target functions f and g) is invariant under the transformation Φ (being a mere relabelling of inputs), hence, equation (E2) becomes

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} p_A(\mathbf{x}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} p_A(\Phi(\mathbf{x})) = \frac{1}{2}(2^n - 2^m) + (2^m - d_H(\tilde{q}_A, \tilde{g})) = \frac{1}{2}(2^n + 2^m) - d_H(\tilde{q}_A, \tilde{g}), \tag{E5}$$

where we recall that $d_H(\tilde{q}_A, \tilde{g}) := |\{\mathbf{x} \in \mathbb{Z}_2^m \mid \tilde{q}_A(\mathbf{x}) \neq \tilde{g}(\mathbf{x})\}|$ denotes the Hamming distance between $\tilde{q}_A$ and $\tilde{g}$. Next, we extend $\tilde{q}_A$ to a quadratic function on all inputs $\mathbf{x} \in \mathbb{Z}_2^n$.

Lemma 4. *Let $\tilde{g}$ be a Boolean function $\tilde{g} : \mathbb{Z}_2^m \to \mathbb{Z}_2$ with an extension $g : \mathbb{Z}_2^m \times \mathbb{Z}_2^{n-m} \to \mathbb{Z}_2$. For any quadratic function $\tilde{q}_A : \mathbb{Z}_2^m \to \mathbb{Z}_2$, we can find a quadratic function $q_A : \mathbb{Z}_2^m \times \mathbb{Z}_2^{n-m} \to \mathbb{Z}_2$ such that*

$$d_{\mathrm{H}}(q_A, g) \leqslant \frac{1}{2}(2^n - 2^m) + d_{\mathrm{H}}(\tilde{q}_A, \tilde{g}). \tag{E6}$$

Proof (sketch). The proof is recursive. We define the series of nested extension functions $g^{(j)} : \mathbb{Z}_2^{m+j} \to \mathbb{Z}_2$ such that $g^{(0)} = \tilde{g}$ and $g^{(n-m)} = g$, where $g^{(j)}(\mathbf{u}) = g^{(j+1)}(\mathbf{u}, 0)$ for all $\mathbf{u} \in \mathbb{Z}_2^{m+j}$. We will recursively define a series of quadratic functions $q_A^{(j)} : \mathbb{Z}_2^{m+j} \to \mathbb{Z}_2$ starting with $q_A^{(0)} = \tilde{q}_A$, such that $q_A^{(j)}(\mathbf{u}) = q_A^{(j+1)}(\mathbf{u}, 0)$ and $\Delta_j + q_A^{(j)}(\mathbf{u}) = q_A^{(j+1)}(\mathbf{u}, 1)$ for all $\mathbf{u} \in \mathbb{Z}_2^{m+j}$ for some constant $\Delta_j \in \mathbb{Z}_2$ to be determined. Clearly, the $q_A^{(j)}$ are all quadratic if and only if $q_A^{(0)}$ is quadratic. Furthermore,

$$\begin{aligned} d_{\mathrm{H}}\left(q_A^{(j+1)}, g^{(j+1)}\right) &= \sum_{\mathbf{u}\in\mathbb{Z}_2^{m+j}} \left[q_A^{(j+1)}(\mathbf{u}, 0) \oplus g^{(j+1)}(\mathbf{u}, 0)\right] + \sum_{\mathbf{u}\in\mathbb{Z}_2^{m+j}} \left[q_A^{(j+1)}(\mathbf{u}, 1) \oplus g^{(j+1)}(\mathbf{u}, 1)\right] \\ &= d_{\mathrm{H}}\left(q_A^{(j)}, g^{(j)}\right) + \sum_{\mathbf{u}\in\mathbb{Z}_2^{m+j}} \left[\Delta_j \oplus q_A^{(j)}(\mathbf{u}) \oplus g^{(j+1)}(\mathbf{u}, 1)\right]. \end{aligned} \tag{E7}$$

Assume the sum in the last line evaluates to N when $\Delta_j = 0$, then it evaluates to $2^{m+j} - N$ when $\Delta_j = 1$. Therefore, we can choose Δ_j such that the sum evaluates to $2^{m+j}/2$ or less. This yields

$$d_{\mathrm{H}}\left(q_A^{(j+1)}, g^{(j+1)}\right) \leqslant d_{\mathrm{H}}\left(q_A^{(j)}, g^{(j)}\right) + 2^{m+j}/2. \tag{E8}$$

Using our initial condition for $j = 0$, and applying this bound recursively we get

$$d_{\mathrm{H}}(q_A, g) = d_{\mathrm{H}}\left(q_A^{(n-m)}, g^{(n-m)}\right) \leqslant d_{\mathrm{H}}\left(q_A^{(0)}, g^{(0)}\right) + \frac{1}{2}\sum_{j=0}^{n-m-1} 2^{m+j} = d_{\mathrm{H}}(\tilde{q}_A, \tilde{g}) + \frac{1}{2}(2^n - 2^m), \tag{E9}$$

which proves the lemma. □

Since q_A from lemma 4 is quadratic, by theorem 3 we can find a non-adaptive, deterministic, level-2 $l2$-MBQC $A^\star$ (using stabiliser states) implementing q_A. Applying lemma 4 and comparing with equation (E5) we obtain

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} p_{A^\star}(\mathbf{x}) = 2^n - d_{\mathrm{H}}(q_A, g) \geqslant 2^n - d_{\mathrm{H}}(\tilde{q}_A, \tilde{g}) - \frac{1}{2}(2^n - 2^m) = \frac{1}{2}(2^n + 2^m) - d_{\mathrm{H}}(\tilde{q}_A, \tilde{g}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} p_A(\mathbf{x}), \tag{E10}$$

such that the deterministic $l2$-MBQC $A^\star$ performs at least as well as probabilistic $l2$-MBQC A. Theorem 4 thus follows from corollary 1.

Appendix F. Proof of Theorem 5

Let the $l2$-MBQC belong to level-D in the Clifford hierarchy (per definition 3). Then each measurement $M_k(c_k)$ takes the form

$$M_k(c_k) = U_k(c_k) M_k(0) U_k^\dagger(c_k), \tag{F1}$$

where $U_k(c_k) \in \mathcal{C}_1^D$ and $c_k : \mathbb{Z}_2^n \to \mathbb{Z}_2$ a linear function for all $k \in \{1, \ldots, N\}$ (see definition 1). For deterministic computation we have for each input $\mathbf{i} \in \mathbb{Z}_2^n$

$$\bigotimes_{k=1}^{N} \left[U_k(c_k) M_k(0) U_k^\dagger(c_k)\right] |\psi\rangle = (-1)^{o(\mathbf{i})} |\psi\rangle \tag{F2}$$

where $|\psi\rangle$ is the resource state and $o(\mathbf{i})$ is the computational output. From [35], we have $\mathcal{SC}_1^D = \mathcal{C}_1^D$, meaning $\exists C_k, C_k' \in \mathcal{C}_1^2$ and diagonal gates $D_k \in \mathcal{C}_1^D$ such that $U_k = C_k D_k C_k'$. Equation (9) can be rewritten as

$$\bigotimes_{k=1}^{N} \left[D_k(c_k) \tilde{M}_k(0) D_k^\dagger(c_k) \right] |\tilde{\psi}\rangle = (-1)^{o(\mathbf{i})} |\tilde{\psi}\rangle, \tag{F3}$$

where $|\tilde{\psi}\rangle = C_k^\dagger |\psi\rangle$ and $\tilde{M}(0) = \bigotimes_{k=1}^N (C_k' M_k(0) C_k'^\dagger)$. Note that $|\tilde{\psi}\rangle$ is a stabiliser state and $\tilde{M}(0)$ is a Pauli operator, which we write

$$\tilde{M}(0) = \mathrm{e}^{\frac{i\pi\beta}{2}} (X_1^{x_1} Z_1^{z_1}) \otimes \ldots \otimes (X_N^{x_N} Z_N^{z_N}), \tag{F4}$$

for $\beta \in \mathbb{Z}_4$ and $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Z}_2^N$, $\mathbf{z} = (z_1, \ldots, z_N) \in \mathbb{Z}_2^N$. Expanding $|\tilde{\psi}\rangle$ in the computational basis, we have

$$|\tilde{\psi}\rangle = \sum_{\mathbf{q} \in \mathbb{Z}_2^N} \alpha(\mathbf{q}) |\mathbf{q}\rangle \quad \text{such that} \quad |\alpha(\mathbf{q})| \in \{0, \alpha\} \ \forall \mathbf{q} \in \mathbb{Z}_2^N, \text{for some } \alpha \in \mathbb{R}, \tag{F5}$$

which follows the fact that all nonzero amplitudes of a stabiliser state in the computational basis have the same magnitude. The global measurements in the updated basis

$$\tilde{M}(\mathbf{c}) = \bigotimes_{k=1}^{N} D_k(c_k) \tilde{M}_k(0) D_k^\dagger(c_k) \tag{F6}$$

permute computational basis states up to a phase,

$$\tilde{M}(\mathbf{c}) |\mathbf{q}\rangle = \theta(\mathbf{c}, \mathbf{q}) |\mathbf{q} \oplus \mathbf{x}\rangle, \tag{F7}$$

where $\theta(\mathbf{c}, \mathbf{q}) \in U(1)$ for all $\mathbf{c}, \mathbf{q} \in \mathbb{Z}_2^N$. To satisfy equation (F3) we must have

$$\theta(\mathbf{c}, \mathbf{q}) = (-1)^{o(\mathbf{i})} \quad \forall \mathbf{q} \in \mathbb{Z}_2^N \text{ with } \alpha(\mathbf{q}) \neq 0, \ \forall \mathbf{c} \in \mathbb{Z}_2^N. \tag{F8}$$

Thus, the dependence on $\mathbf{q}$ may be dropped and we may write $\theta(\mathbf{c}) := \theta(\mathbf{c}, \mathbf{q})$, and we remark that $\mathbf{c}$ is implicitly dependent on the input $\mathbf{i}$.

To determine the allowable phases $\theta(\mathbf{c}) = (-1)^{o(\mathbf{i})}$, we utilise a classification of diagonal gates in the Clifford hierarchy from [37]. From [37], up to a global phase every single qubit diagonal operator $D_k \in \mathcal{C}_1^D$ can be written as $D_k[f_k]$ where $D_k[f_k]|q_k\rangle = f_k(q_k)|q_k\rangle$ for all $q_k \in \mathbb{Z}_2$ and where $f_k : \mathbb{Z}_2 \to U(1)$ is given by

$$f_k(q_k) = \exp\left(2\pi i \sum_{m=0}^{D} \frac{\vartheta_{m_k} q_k}{2^m} \right), \quad \text{for some } \vartheta_{m,k} \in \mathbb{Z}_{2^m} \quad \forall q_k \in \mathbb{Z}_2. \tag{F9}$$

(Specifically, this follows from theorem 2 of [37] by setting $p = 2, a = 1$. In that case, combining their equations (20) and (17) we find that the mth level of the single qubit Clifford hierarchy up to phases is generated by operators of the form $\sum_{q \in \mathbb{Z}_2} \exp\left(\frac{2\pi i}{2^m} q\right) |q\rangle\langle q|$.)

Then each $\tilde{M}_k(c_k) = D_k(c_k) \tilde{M}_k(0) D_k^\dagger(c_k)$, with $\tilde{M}_k(0) = \mathrm{e}^{\frac{i\pi\beta_k}{2}} X_k^{x_k} Z_k^{z_k}$ has an action on computational basis states as

$$\tilde{M}_k(c_k)|q_k\rangle = \exp\left[2\pi i \left(\frac{\beta_k}{4} + \frac{z_k q_k}{2} + \sum_{m=0}^{D} \frac{\vartheta_{m,k}[c_k] x_k}{2^m} \right) \right] |q_k \oplus x_k\rangle, \quad \text{for some } \vartheta_{m,k}[c_k] \in \mathbb{Z}_{2^m}, \quad \forall q_k \in \mathbb{Z}_2. \tag{F10}$$

Therein, the factors $\vartheta_{m,k}[c_k]$ are determined by the choice of gate $D_k(c_k) = \mathrm{diag}(1, \exp\left(2\pi i \sum_{m=0}^{D} \frac{\vartheta_{m,k}[c_k]}{2^m}\right))$. In particular, we may rewrite them as $\vartheta_{m,k}[c_k] = \vartheta_{m,k}[0](1 - c_k) + \vartheta_{m,k}[1] c_k$, for $\vartheta_{m,k}[0], \vartheta_{m,k}[1] \in \mathbb{Z}_{2^m}$.

Then the global phase, and thus computational output can be obtained by accumulating all local phases,

$$\tilde{M}(\mathbf{c})|\mathbf{q}\rangle = \exp\left[2\pi i \left(\frac{\beta}{4} + \sum_{k=1}^{N} \frac{z_k q_k}{2} + \sum_{m=0}^{D} \sum_{k=1}^{N} \frac{\vartheta_{m,k}[0](1 - c_k) + \vartheta_{m,k}[1] c_k x_k}{2^m} \right) \right] |\mathbf{q} \oplus \mathbf{x}\rangle, \quad \forall \mathbf{q}, \mathbf{x} \in \mathbb{Z}_2^N. \tag{F11}$$

Equating the phase in the above expression to $(-1)^{o(\mathbf{i})}$ as dictated by equation (F7) we have

$$o(\mathbf{i}) = \frac{\beta}{2} + \sum_{k=1}^{N} z_k q_k + \sum_{m=0}^{D}\sum_{k=1}^{N} \frac{\vartheta_{m,k}[0](1-c_k) + \vartheta_{m,k}[1]c_k x_k}{2^{m-1}} \pmod 2. \tag{F12}$$

Now we recall that the measurement settings may be written as $\mathbb{Z}_2$-linear basis functions $c_k = \phi_{\mathbf{a}}$ for some $\mathbf{a}_k \in \mathbb{Z}_2^n$ (where $\phi_{\mathbf{a}}$ is defined in section 4.2.1). Then using equation (19) we rewrite this function in the monomial basis

$$c_k = \sum_{0\neq\mathbf{b}\in\mathbf{a}_k\mathbb{Z}_2^n} (-2)^{W(\mathbf{b})-1} \prod_{l=1}^{n} i_l^{b_l}. \tag{F13}$$

Inserting into equation (F12), we conclude that the third term in equation (F12) contributes only if $m \geqslant W(\mathbf{b})$. Moreover, since $D \geqslant m$, and since the degree of the monomial term in equation (F13) is given by $W(\mathbf{b})$, any non-vanishing term in the output function in equation (F12) has degree at most D. This completes the proof.

Appendix G. Proof of Theorem 6

Following the terminology of the proof of theorem 3 in appendix D, we denote by $P \in \mathrm{Mat}(N \times n, \mathbb{Z}_2)$ the classical, $\mathbb{Z}_2$-linear pre-processing of a non-adaptive, deterministic, level-2 (i.e. stabiliser) $l2$-MBQC.

It follows that the qubit count equals the number of rows in P, hence, we seek a suitable P with minimal number of rows. We also recall the conditions $\mathbf{p}_i.\mathbf{p}_j = q_{i,j} \pmod 2$ and $W(\mathbf{p}_i) = 0 \pmod 2$ (see appendix D) for any non-adaptive, deterministic, level-2 $l2$-MBQC computing the quadratic function f. The latter constraints are equivalent to $Q(f) = P^T P \pmod 2$, where $Q(f)$ is the matrix associated with f in equation (14). It was shown by Lempel [39] that a solution P always exists and that the smallest number of rows of P equals $N = \mathrm{rk}(Q(f)) + 1$. This completes the proof.

Appendix H. Adaptivity

In this section, we comment further on how our results change in the presence of adaptive measurements. Adaptivity is a powerful resource for many quantum computational schemes. For universal MBQC it is essential—in general, measurement bases must be chosen based on previous measurement outcomes in order to control the randomness induced by non-deterministic measurement outcomes. For many families of quantum circuits adaptivity is also essential and they may become classically simulable in its absence, see [60] for example.

By conditioning future measurements on prior measurement outcomes, qubit count and non-Clifford resource requirements can be drastically reduced (see figure 1). To see this, we consider a general adaptive MBQC as being composed of several non-adaptive MBQCs called components (where each component does need not to have deterministic output) (see figure 2). The overall computation can be represented by a directed acyclic graph $\mathcal{G}$ called the incidence graph. Each node on the graph $\mathcal{G}$ corresponds to a non-adaptive component, and the directed edges correspond to the information flow required for adaptivity: the target node corresponds to the component that requires the output of the component corresponding to the source node.

The nodes of the graph $\mathcal{G}$ are also labelled by integers, referring to the order in which they are performed. Multiple nodes may share the same label—meaning they are performed in parallel—but the labels must strictly increase when moving along the edges. We call this list of integers the schedule $\mathcal{S}$. For an MBQC with incidence graph $\mathcal{G}$ and schedule $\mathcal{S}$, we define the depth of the computation as the largest integer in $\mathcal{S}$. We define the width of the computation as the total number of qubits in all components with a common schedule index $k \in \mathcal{S}$, maximised over all $k \in \mathcal{S}$.

The depth is how many timesteps the computation takes to perform, while the width is how many qubits are required to execute it with the prescribed schedule. Note the volume does not represent the number of qubits required to implement the MBQC. In fact, an arbitrary width w MBQC can be implemented using w qubits as not all measurements need to be executed in parallel. In general, space-time tradeoffs are possible, meaning that it may be possible to vary between the width and the depth of the MBQC. We note that shallow quantum circuits in [15] are restricted to constant depth, while non-adaptive MBQCs admit a depth-1 representation.

As a concrete example, we again consider the n-bit delta function $\delta : \mathbb{Z}_2^n \to \mathbb{Z}_2$. As shown in corollary 2, $2^n - 1$ qubits are required for its implementation in non-adaptive MBQC (i.e. width $2^n - 1$ and depth 1), as

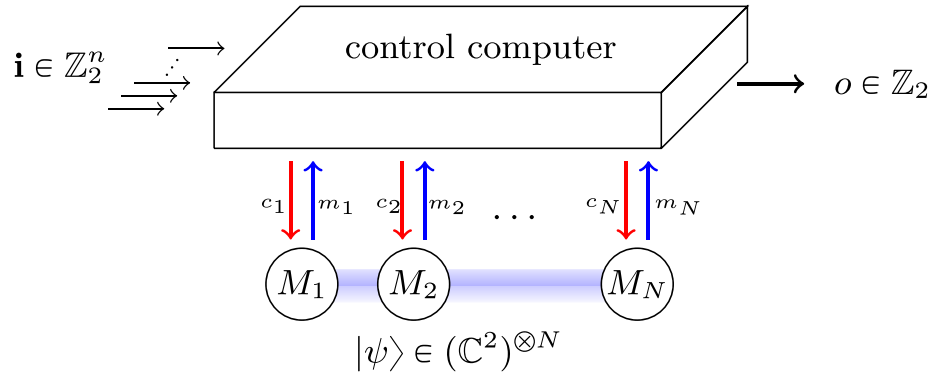

Figure 1. The schematic setup of an $l2$-MBQC defined in definition 1, from [13]. For each qubit (indexed by k) of the resource state $|\psi\rangle$, the control computer determines the measurement settings c_k as a linear function of the inputs $\mathbf{i} \in \mathbb{Z}_2^n$ and any previous measurement outcomes $m_1, \ldots, m_{k-1}$. The output $o \in \mathbb{Z}_2$ is evaluated by the control computer as the parity of all local measurement outcomes.

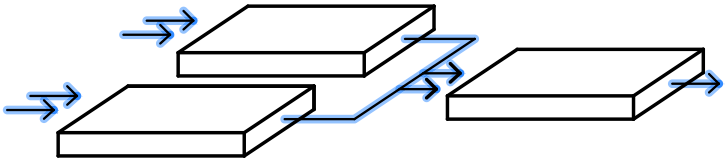

Figure 2. Sequence of non-adaptive MBQCs composed together.

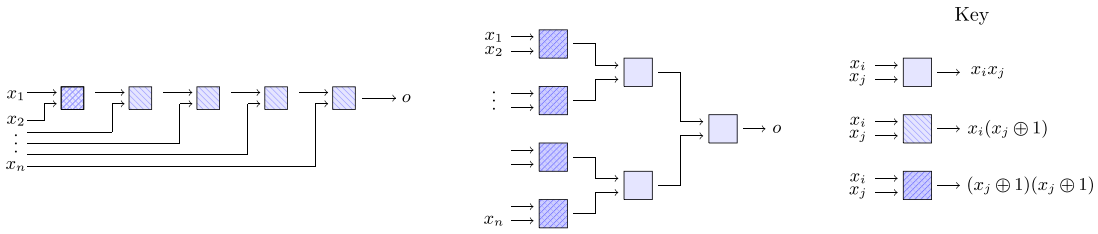

Figure 3. Linearly composed (left) and binary tree composed (middle) Anders and Browne MBQCs to compute the delta function. Each box represents an $l2$-MBQC such that the output is the product of the two inputs (up to linear pre-processing), which can be achieved with a stabiliser $l2$-MBQC using a 3-qubit GHZ state. (right) The three different Anders and Browne MBQCs required differ only by linear pre-processing.

well as non-Clifford gates belonging to the nth level in the Clifford hierarchy. Using the adaptive scheme represented in figure 3 (left), the delta function can be implemented with width 3 (meaning only 3 qubits are required), however the depth needed is n. The volume of 3 n is exponentially smaller (in n) than the non-adaptive case. Similarly, one could choose an adaptive scheme based on a binary tree, such as that depicted in figure 3 (middle). In this case, one can use $O(3n)$ qubits and a depth of $O(\log(n))$ to compute the delta function. This gives a volume of $O(3n\log(n))$.

We can verify the computational output as follows. Recall that given $\mathbf{x} \in \mathbb{Z}_2^n$, we have $\delta(\mathbf{x}) = (x_1 \oplus 1)\ldots(x_n \oplus 1)$. Then up to the appropriate linear pre-processing (specifically, the mod-2 addition of 1 to one or both inputs), we can compute this function by multiplying all the inputs together. Each Anders and Browne $l2$-MBQC can multiply pairs of inputs together using a 3-qubit GHZ state [20]. Associativity of multiplication lets us chain the $l2$-MBQCs together in different ways to achieve the same output.

ORCID iDs

Markus Frembs https://orcid.org/0000-0001-6653-4652
Sam Roberts https://orcid.org/0000-0002-4652-389X
Earl T Campbell https://orcid.org/0000-0002-5627-0021
Stephen D Bartlett https://orcid.org/0000-0003-4387-670X

References

[1] Raussendorf R 2013 Contextuality in measurement-based quantum computation *Phys. Rev.* A **88** 022322
[2] Howard M, Wallman J, Veitch V and Emerson J 2014 Contextuality supplies the 'magic' for quantum computation *Nature* **510** 351–5
[3] Bermejo-Vega J, Delfosse N, Browne D E, Okay C and Raussendorf R 2017 Contextuality as a resource for models of quantum computation with qubits *Phys. Rev. Lett.* **119** 120505
[4] Delfosse N, Guerin P A, Bian J and Raussendorf R 2015 Wigner function negativity and contextuality in quantum computation on rebits *Phys. Rev.* X **5** 021003
[5] Raussendorf R, Browne D E, Delfosse N, Okay C and Bermejo-Vega J 2017 Contextuality and Wigner function negativity in qubit quantum computation *Phys. Rev.* A **95** 052334
[6] Karanjai A, Wallman J J and Bartlett S D 2018 Contextuality bounds the efficiency of classical simulation of quantum processes (arXiv:1802.07744)
[7] Raussendorf R 2019 Cohomological framework for contextual quantum computations *Quantum Inf. Comput.* **19** 1141–70
[8] Okay C, Roberts S, Bartlett S and Raussendorf R 2017 Topological proofs of contextuality in quantum mechanics *Quantum Inf. Comput.* **17** 1135–66
[9] Veitch V, Mousavian S A H, Gottesman D and Emerson J 2014 The resource theory of stabilizer quantum computation *New J. Phys.* **16** 013009
[10] Mansfield S and Kashefi E 2018 Quantum advantage from sequential-transformation contextuality *Phys. Rev. Lett.* **121** 230401
[11] Pashayan H, Wallman J J and Bartlett S D 2015 Estimating outcome probabilities of quantum circuits using quasiprobabilities *Phys. Rev. Lett.* **115** 070501
[12] Nadish de S 2018 Logical paradoxes in quantum computation *Proc. 33rd Annual ACM/IEEE Symp. on Logic in Computer Science* (*LICS 2018*) (New York: Association for Computing Machinery) pp 335–43
[13] Frembs M, Roberts S and Bartlett S D 2018 Contextuality as a resource for measurement-based quantum computation beyond qubits *New J. Phys.* **20** 103011
[14] Kochen S and Specker E P 1967 The problem of hidden variables in quantum mechanics *J. Math. Mech.* **17** 59–87
[15] Bravyi S, Gosset D and König R 2018 Quantum advantage with shallow circuits *Science* **362** 308–11
[16] Bravyi S, Gosset D, Koenig R and Tomamichel M 2020 Quantum advantage with noisy shallow circuits *Nat. Phys.* **16** 1040–5
[17] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
[18] Raussendorf R, Browne D E and Briegel H J 2003 Measurement-based quantum computation on cluster states *Phys. Rev.* A **68** 022312
[19] Briegel H J, Browne D E, Dür W, Raussendorf R and Van den Nest M 2009 Measurement-based quantum computation *Nat. Phys.* **5** 19–26
[20] Anders J and Browne D E 2009 Computational power of correlations *Phys. Rev. Lett.* **102** 050502
[21] Raussendorf R 2013 Contextuality in measurement-based quantum computation *Phys. Rev.* A **88** 022322
[22] Hoban M J, Campbell E T, Loukopoulos K and Browne D E 2011 Non-adaptive measurement-based quantum computation and multi-party Bell inequalities *New J. Phys.* **13** 023014
[23] Gottesman D 1998 The Heisenberg representation of quantum computers (arXiv:quant-ph/9807006)
[24] Aaronson S and Gottesman D 2004 Improved simulation of stabilizer circuits *Phys. Rev.* A **70** 052328
[25] Gross D 2006 Hudson's theorem for finite-dimensional quantum systems *J. Math. Phys.* **47** 122107
[26] Amy M and Mosca M 2019 T-count optimization and Reed-Muller codes *IEEE Trans. Inf. Theory* **65** 4771–84
[27] Seroussi G and Lempel A 1983 Maximum likelihood decoding of certain Reed-Muller codes (Corresp.) *IEEE Trans. Inf. Theory* **29** 448–50
[28] Heyfron L E and Campbell E T 2018 An efficient quantum compiler that reduces T count *Quantum Sci. Technol.* **4** 015004
[29] Kissinger A and van de Wetering J 2020 Reducing the number of non-Clifford gates in quantum circuits *Phys. Rev.* A **102** 022406
[30] Heyfron L E and Campbell E 2019 A quantum compiler for qudits of prime dimension greater than 3 (arXiv:1902.05634)
[31] Werner R F and Wolf M M 2001 All-multipartite Bell-correlation inequalities for two dichotomic observables per site *Phys. Rev.* A **64** 032112
[32] Abramsky S, Barbosa R S, Carù G, de Silva N, Kishida K and Mansfield S 2018 Minimum quantum resources for strong non-locality *12th Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC 2017)* (*Leibniz Int. Proc. in Informatics (LIPIcs)*) vol 73 (Dagstuhl: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik) pp 9:1–9:20
[33] Kolokotronis N, Limniotis K and Kalouptsidis N 2007 Best quadratic approximations of cubic Boolean functions *IACR Cryptol. ePrint Arch.* **37** 2007
[34] Kolokotronis N, Limniotis K and Kalouptsidis N 2009 Best affine and quadratic approximations of particular classes of Boolean functions *IEEE Trans. Inf. Theory* **55** 5211–22
[35] Zeng B, Chen X and Chuang I L 2008 Semi-Clifford operations, structure of $C(k)$ hierarchy and gate complexity for fault-tolerant quantum computation *Phys. Rev.* A **77** 042313
[36] Gross D and Nest M 03 2008 The LU-LC conjecture, diagonal local operations and quadratic forms over $GF(2)$ *Quantum Inf. Comput.* **8** 263–81
[37] Cui S X, Gottesman D and Krishna A 2017 Diagonal gates in the Clifford hierarchy *Phys. Rev.* A **95** 012329
[38] de Silva N 2021 Efficient quantum gate teleportation in higher dimensions *Proc. R. Soc.* A **477** 20200865
[39] Lempel A 1975 Matrix factorization over GF(2) and trace-orthogonal bases of GF(2) *SIAM J. Comput.* **4** 175–86
[40] Mori R 2018 Periodic Fourier representation of Boolean functions (arXiv:1803.09947)
[41] O'Donnell R 2014 *Analysis of Boolean Functions* (Cambridge: Cambridge University Press)
[42] Yoshida B 2017 Gapped boundaries, group cohomology and fault-tolerant logical gates *Ann. Phys., NY* **377** 387–413
[43] Abramsky S and Brandenburger A 2011 The sheaf-theoretic structure of non-locality and contextuality *New J. Phys.* **13** 113036
[44] Okay C, Tyhurst E and Raussendorf R 2018 The cohomological and the resource-theoretic perspective on quantum contextuality: common ground through the contextual fraction *Quantum Inf. Comput.* **18** 1272–94
[45] Chen X, Gu Z-C, Liu Z-X and Wen X-G 2013 Symmetry protected topological orders and the group cohomology of their symmetry group *Phys. Rev.* B **87** 155114
[46] Daniel A K and Miyake A 2021 Quantum computational advantage with string order parameters of one-dimensional symmetry-protected topological order *Phys. Rev. Lett.* **126** 090505

[47] Liu Z-W and Winter A 2020 Many-body quantum magic (arXiv:2010.13817) (available at: https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.3.020333)
[48] Ellison T D, Kato K, Liu Z-W and Hsieh T H 2021 Symmetry-protected sign problem and magic in quantum phases of matter *Quantum* **5** 612
[49] Else D V, Bartlett S D and Doherty A C 2012 Symmetry protection of measurement-based quantum computation in ground states *New J. Phys.* **14** 113016
[50] Nautrup H P and Wei T-C 2015 Symmetry-protected topologically ordered states for universal quantum computation *Phys. Rev.* A **92** 052309
[51] Miller J and Miyake A 2016 Hierarchy of universal entanglement in 2D measurement-based quantum computation *npj Quantum Inf.* **2** 16036
[52] Raussendorf R, Okay C, Wang D-S, Stephen D T and Nautrup H P 2019 Computationally universal phase of quantum matter *Phys. Rev. Lett.* **122** 090501
[53] Devakul T and Williamson D J 2018 Universal quantum computation using fractal symmetry-protected cluster phases *Phys. Rev.* A **98** 022332
[54] Roberts S and Bartlett S D 2020 Symmetry-protected self-correcting quantum memories *Phys. Rev.* X **10** 031041
[55] Raussendorf R, Bravyi S and Harrington J 2005 Long-range quantum entanglement in noisy cluster states *Phys. Rev.* A **71** 062313
[56] Raussendorf R, Harrington J and Goyal K 2006 A fault-tolerant one-way quantum computer *Ann. Phys., NY* **321** 2242–70
[57] Raussendorf R and Harrington J 2007 Fault-tolerant quantum computation with high threshold in two dimensions *Phys. Rev. Lett.* **98** 190504
[58] Raussendorf R, Harrington J and Goyal K 2007 Topological fault-tolerance in cluster state quantum computation *New J. Phys.* **9** 199
[59] Brown B J and Roberts S 2020 Universal fault-tolerant measurement-based quantum computation *Phys. Rev. Res.* **2** 033305
[60] Jozsa R and Maarten V den N 2014 Classical simulation complexity of extended Clifford circuits *Quantum Inf. Comput.* **14** 633–48