Contextuality as a Resource in Measurement-Based Quantum Computation

Markus Frembs

Imperial College London

Oxford, 4-6 July 2019

Why contextuality for quantum computation?

- Kochen Specker theorem: contextuality as genuine quantum feature
- interesting for quantum computation: few observables enough to prove contextuality
- measurement-based quantum computation (MBQC): harness correlations in state-dependent proofs of contextuality

The prototypical example

Consider the observables XXX, XYY, YXY, YYX and the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle) \in \mathbb{C}^8$.

$$XXX|\psi\rangle = -|\psi\rangle \qquad XYY|\psi\rangle = -|\psi\rangle$$
$$YXY|\psi\rangle = -|\psi\rangle \qquad YYX|\psi\rangle = +|\psi\rangle$$

This can be turned into a computation: let $\mathbf{i} = (i_1, i_2) \in \mathbb{Z}_2^2$ and define local functions, $f_1(\mathbf{i}) = i_1$, $f_2(\mathbf{i}) = i_2$, $f_3(\mathbf{i}) = i_1 \oplus i_2$ selecting measurements via $0 \to X$, $1 \to Y$. Denote the local measurement outcomes by $s_k \in \mathbb{Z}_2$ and define the output $o(\mathbf{i}) := \sum_{k=1}^{3} s_k$, then

$$o(\mathbf{i}) = i_1 i_2 \oplus 1 = \mathrm{NAND}(\mathbf{i})$$

Contextuality $\to$ nonlinear correlations

Note that the computation in f_k and $o = \sum_{k=1}^{3} s_k$ are mod-2 linear, however, $o(\mathbf{i})$ is a $\mathbb{Z}_2$-nonlinear function.

The Setup - Qubits

A temporally flat $l2$-MBQC with input string $\mathbf{i} \in \mathbb{Z}_2^n$ and output $o(\mathbf{i}) \in \mathbb{Z}_2$ consists of the following components:

- an N qubit system where the overall resource state is represented by $|\psi\rangle \in (\mathbb{C}^2)^{\otimes N}$
- a set of measurement settings $q_k = f_k(\mathbf{i})$ for some $\mathbb{Z}_2$-linear functions $f_k : \mathbb{Z}_2^n \to \mathbb{Z}_2$.
- a set of measurements M_k, each with two possible eigenvalues $(-1)^{s_k}$, where $s_k \in \mathbb{Z}_2$ is the measurement outcome and such that $M_k(q_k) = U_k^{q_k} M_k(0) U_k^{-q_k}$ is a projective representation of $\mathbb{Z}_2$;
- the computational output is a linear function of the measurement outcomes $\mathbf{s} = (s_1, \cdots, s_N) \in \mathbb{Z}_2^N$,

$$o(\mathbf{i}) = \sum_{j=1}^{N} c_j s_j \mod 2, \quad c_j \in \mathbb{Z}_2.$$

(In adaptive $l2$-MBQC the f_k may also depend on previous measurement outcomes s_j, $j < k$.)

MBQC with Qubits

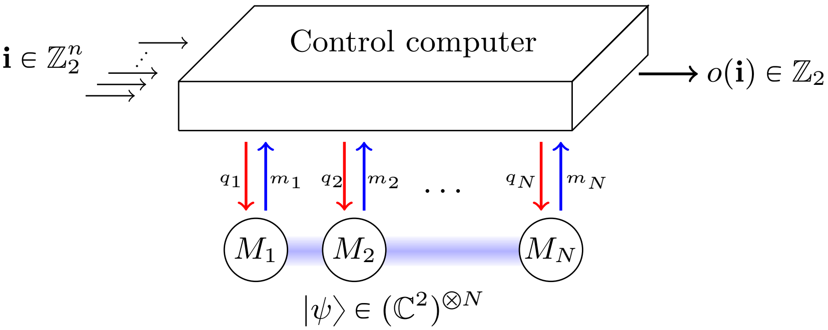

Figure: Schematic for temporally flat $l2$-MBQC.

Remark

With a suitably chosen resource state, such as (qubit) cluster states, this model is universal for quantum computation.

Contextuality in MBQC with Qubits

In [Rau13] and [ABM17] the following was proven.

deterministic $l2$-MBQC

Let M be an *adaptive* $l2$-MBQC which deterministically evaluates the Boolean function $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$. If $o(\mathbf{i})$ is $\mathbb{Z}_2$-nonlinear, then M is strongly contextual.

probabilistic $l2$-MBQC

Let M_{p_S} be an *adaptive* $l2$-MBQC that probabilistically evaluates a $\mathbb{Z}_2$-nonlinear Boolean function $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ with success probability $p_S > 1 - \mathrm{NCF}(e_o)\nu(o)$, then M_{p_S} is contextual.

What about qudits?

Is there a similarly close connection between contextuality and function computation in ld-MBQC?

The Setup - Qudits

A temporally flat *ld*-MBQC with input string $\mathbf{i} \in \mathbb{Z}_d^n$ and output $o(\mathbf{i}) \in \mathbb{Z}_d$, consists of the following components:

- an N qudit system where the overall resource state is represented by $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$
- a set of measurement settings $q_k = f_k(\mathbf{i})$ for some $\mathbb{Z}_d$-linear functions $f_k : \mathbb{Z}_d^n \to \mathbb{Z}_d$.
- a set of measurements M_k, each with d possible eigenvalues ω^{s_k}, where $\omega = e^{\frac{2\pi i}{d}}$ and $s_k \in \mathbb{Z}_d$ is the measurement outcome, and such that $M_k(q_k) = U_k^{q_k} M_k(0) U_k^{-q_k}$ is a projective representation of $\mathbb{Z}_d$;
- the computational output is a linear function of the measurement outcomes $\mathbf{s} = (s_1, \cdots, s_N) \in \mathbb{Z}_d^N$,

$$o(\mathbf{i}) = \sum_{j=1}^{N} c_j s_j \mod d, \quad c_j \in \mathbb{Z}_d.$$

(In adaptive ld-MBQC the f_k may also depend on previous measurement outcomes.)

MBQC with Qudits

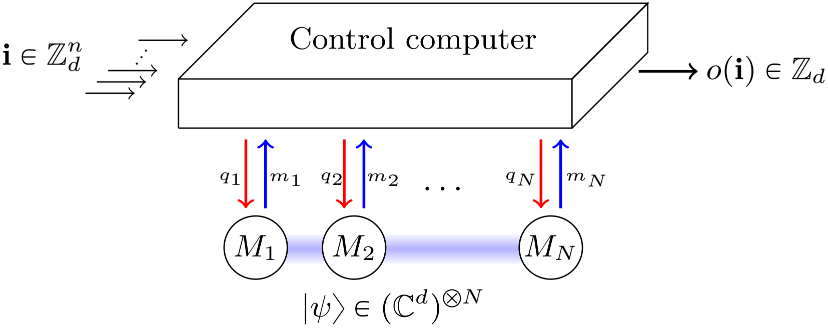

Figure: Schematic for temporally flat *ld*-MBQC.

Symplectic Structure of Qudit Stabilizer Formalism

Let $\mathcal{P}_d^{\otimes N}$ denote the N-fold tensor product of the qudit Pauli group generated by elements $\langle X_k, Z_k, \omega \mathbb{1}_k \rangle$ where $X_k|q_k\rangle = |q_k + 1\rangle$, $Z_k|q_k\rangle = \omega^{q_k}|q_k\rangle$ and $\omega = \frac{2\pi i}{d}$ is a d-th root of unity.

For $\mathbf{v} = (\mathbf{a}, \mathbf{b})^T \in \mathbb{Z}_d^{2N}$ and $\tau^2 = \omega$ one defines Weyl operators $W_\mathbf{v} := \tau^{-\mathbf{a}\cdot\mathbf{b}}(Z^{a_1} \otimes \cdots \otimes Z^{a_N})(X^{b_1} \otimes \cdots \otimes X^{b_N})$.
Then the following relation holds,

$$W_\mathbf{v} W_\mathbf{w} = \omega^{[\mathbf{v},\mathbf{w}]} W_\mathbf{w} W_\mathbf{v}.$$

The Clifford group $\mathcal{C}_N(d) \subset \mathcal{U}(\mathcal{H}_d^{\otimes N})$ is the automorphism group of the Pauli group $\mathcal{P}_d^{\otimes N}$, i.e., $VPV^\dagger \in \mathcal{P}_d^{\otimes N}$ for all $P \in \mathcal{P}_d^{\otimes N}$, $V \in \mathcal{C}_N(d)$.

In particular, there is a subgroup $\sigma\mathcal{C}_N(d) \subset \mathcal{C}_N(d)$ such that for all $V \in \mathcal{C}_N(d)$: $V = UW_\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}_d^{2N}$, and for all $U \in \sigma\mathcal{C}_N(d)$:

$$UW_\mathbf{v}U^\dagger = W_{C_U\mathbf{v}}, \quad C_U \in \mathrm{Sp}_{2N}(\mathbb{Z}_d)$$

A nonlinear, noncontextual example - I

Given the Weyl commutation relations and the action of Clifford operators on Paulis by conjugation one computes:

$$
\begin{aligned}
&V^{f(\mathbf{i})}\ W_{\mathbf{v}}\ V^{-f(\mathbf{i})} \\
&\quad = (UW_{\mathbf{x}})^{f(\mathbf{i})}\ W_{\mathbf{v}}\ (UW_{\mathbf{x}})^{-f(\mathbf{i})} \\
&\quad = (UW_{\mathbf{x}})^{f(\mathbf{i})-1}\ W_{C_U\mathbf{x}}\ W_{C_U\mathbf{v}}\ W_{-C_U\mathbf{x}}\ (W_{-\mathbf{x}}U^{-1})^{f(\mathbf{i})-1} \\
&\quad = (W_{C_U\mathbf{x}}\ \cdots\ W_{C_U^{f(\mathbf{i})}\mathbf{x}})\ W_{C_U^{f(\mathbf{i})}\mathbf{v}}\ (W_{-C_U^{f(\mathbf{i})}\mathbf{x}} \cdots\ W_{-C_U\mathbf{x}}) \\
&\quad = \omega^{\left[C_U\mathbf{x}, C_U^{f(\mathbf{i})}\mathbf{v}\right]+\left[C_U^2\mathbf{x}, C_U^{f(\mathbf{i})}\mathbf{v}\right]+\ \cdots\ +\left[C_U^{f(\mathbf{i})}\mathbf{x}, C_U^{f(\mathbf{i})}\mathbf{v}\right]} W_{C_U^{f(\mathbf{i})}\mathbf{v}} \\
&\quad = \omega^{\sum_{k=0}^{f(\mathbf{i})-1}[\mathbf{x}, C_U^k\mathbf{v}]} W_{C_U^{f(\mathbf{i})}\mathbf{v}}
\end{aligned}
$$

Remark

For $C_U = \mathbb{1}$ the exponent is linear in $f(\mathbf{i})$.

A nonlinear, noncontextual example - II

Consider the generalised phase gate,

$$S = \sum_{q=0}^{d-1} \tau^{q^2} |q\rangle\langle q| \ \in \ \sigma\mathcal{C}_1(d), \qquad C_S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and the $N = 2d$ qudit state,

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} |q\rangle^{\otimes 2} |q+1\rangle^{\otimes 2} \cdots |q+d-1\rangle^{\otimes 2}.$$

S acts on X by $S^k X S^{-k} = \tau^{-k} Z^k X$. For $f_k(\mathbf{i}) = f(\mathbf{i})$ it thus holds

$$\bigotimes_{k=1}^{2d} \left(S^{f(\mathbf{i})} W_{\mathbf{v}} S^{-f(\mathbf{i})} \right)_k |\psi\rangle = |\psi\rangle, \quad \mathbf{v} = (0,1)^\mathsf{T}.$$

A nonlinear, noncontextual example - III

On the other hand, for $V = SW_{\mathbf{x}}$, $\mathbf{x} = (0, -1)^\mathsf{T}$ one finds,

$$[\mathbf{x}, C_S^k \mathbf{v}] = k.$$

Hence, choosing $V_1 = (SW_{\mathbf{x}})_1$, $V_k = S_k$ one is left with,

$$o(\mathbf{i}) = \sum_{k=0}^{f(\mathbf{i})-1} [\mathbf{x}, C_S^k \mathbf{v}] = \frac{f(\mathbf{i})(f(\mathbf{i}) - 1)}{2}.$$

Remark

Note that there does exist a hidden variable model for the qudit stabilizer formalism, hence, it is noncontextual.

Contextuality in MBQC with Qudits

Nevertheless, noncontextual *ld*-MBQC cannot compute an arbitrary function $o : \mathbb{Z}_d^n \to \mathbb{Z}_d$ [FRB18].

deterministic *ld*-MBQC

Let M be a *ld*-MBQC for d prime, which deterministically evaluates a function $o : \mathbb{Z}_d^n \to \mathbb{Z}_d$. If $\deg(o) \geq d$, then M is strongly contextual.

probabilistic *ld*-MBQC

Let M_{p_S} be a *ld*-MBQC for d prime, which evaluates a function $o : \mathbb{Z}_d^n \to \mathbb{Z}_d$ with success probability $p_S > 1 - \mathrm{NCF}(e_o)\nu(o)$, then M_{p_S} is contextual.

Proof Sketch - I

- **functions over finite fields**

  Let $\mathbb{F}_d$ be a finite field with d elements, $n \in \mathbb{N}$. Every function $o : \mathbb{F}_d^n \to \mathbb{F}_d$ has a polynomial representation.

- **max degree invariant under linear transformations**

  Let $L_n := \{l : \mathbb{F}_d^n \to \mathbb{F}_d \mid 0 \neq l \text{ linear}\}$ denote the set of $\mathbb{F}_d$-linear transformations on the input vector $\mathbf{i} \in \mathbb{F}_d^n$. Then for $\phi : \mathbb{F}_d \to \mathbb{F}_d$,

  $$\deg(\phi) = \deg(\phi \circ L_n).$$

- **function composition for noncontextual ld-MBQC**

  Assume there exists a hidden variable model for the ld-MBQC, then $o(\mathbf{i}) = \sum_{k=1}^{N} \phi_k(\mathbf{i})$, where $\phi_k : \mathbb{F}_d \to \mathbb{F}_d$ and thus $\deg(o) \leq d - 1$.

Proof Sketch - II

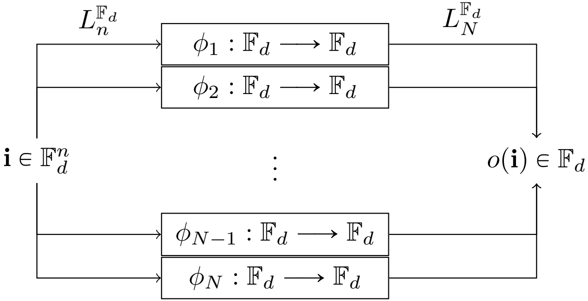

Figure: Function composition in noncontextual *ld*-MBQC.

Remark

For contextual models the functions ϕ_k do not exist independently of $\mathbf{i}$.

So far ...

- have: threshold for genuinly contextual function computation for qubits and qudits (of prime (power) dimension)
- want: distinguish between different types of contextuality

Common Goal

Classify and quantify contextuality in *ld*-MBQC

- strategy: study contextual examples from the perspective of theorems above

A nonlinear, contextual example for qutrits - I

Clearly, no such examples exist within stabilizer *ld*-MBQC.

Consider instead the following operators on a 3-dimensional system by their action on computational basis states $|q\rangle$ for $0 \leq q < 3$ and $\omega = e^{\frac{2\pi i}{3}}$,

$$X|q\rangle := |q+1\rangle,$$
$$W|q\rangle := \xi\omega^{q^2}|q+1\rangle,$$
$$V|q\rangle := \chi\omega^{-q^2}|q+1\rangle.$$

Choose $\xi^3 = \omega$, $\chi^3 = \omega^2$ then $X^3 = W^3 = V^3 = 1$. Moreover, set $\xi\chi = \omega$, e.g., $\xi = e^{\frac{2\pi i}{9}}$ and $\chi = e^{\frac{4\pi i}{9}}$.
Consider the input $\mathbf{i} = (i_1, i_2) \in \mathbb{Z}_3^2$ and $\mathbb{Z}_3$-linear functions, $f_1(\mathbf{i}) := i_1$, $f_2(\mathbf{i}) := i_2$ and $f_3(\mathbf{i}) := -i_1 - i_2$ and choose local measurements according to $0 \rightarrow X$, $1 \rightarrow W$, $2 \rightarrow V$. Finally, let the resource state be,

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle).$$

A nonlinear, contextual example for qutrits - II

We have the following identities

$$\begin{aligned} XXX|q\rangle^{\otimes 3} &= |q+1\rangle^{\otimes 3}, \\ WWW|q\rangle^{\otimes 3} &= \omega|q+1\rangle^{\otimes 3}, \\ VVV|q\rangle^{\otimes 3} &= \omega^2|q+1\rangle^{\otimes 3}, \\ \sigma(XWV)|q\rangle^{\otimes 3} &= \xi\chi|q+1\rangle^{\otimes 3} = \omega|q+1\rangle^{\otimes 3}, \quad \forall \sigma \in S_3 \end{aligned}$$

From this one readily computes the output function.

$$\begin{array}{lll} o(0,0) = 0 & o(0,1) = 1 & o(0,2) = 1 \\ o(1,0) = 1 & o(1,1) = 1 & o(1,2) = 1 \\ o(2,0) = 1 & o(2,1) = 1 & o(2,2) = 2 \end{array}$$

In fact, $o(\mathbf{i}) = 2i_1^2 i_2 + 2i_1 i_2^2 + i_1^2 + i_2^2 + i_1 i_2$.

Higher dimensional functions - I

Note that any Boolean function, $o : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, can be written in the following two equivalent ways,

$$o(\mathbf{i}) = \sum_{\mathbf{a}\in\mathbb{Z}_2^n} c_{\mathbf{a}} \left(\oplus_{l=1}^n a_l i_l\right) = \sum_{\mathbf{b}\in\mathbb{Z}_2^n} c_{\mathbf{b}} \left(\prod_{l=1}^n i_l^{b_l}\right) .$$

The coefficients of the representations are related by the discrete Fourier transform, $\mathcal{F}$. On basis elements one has,

$$\mathcal{F}(\prod_{l=1}^n x_l) = \mathcal{F}(\prod_{l=1}^n x_l^{b_l}) = \frac{1}{2^{W(\mathbf{b})-1}} \sum_{\mathbf{a}\in\mathbb{Z}_2^n} (-1)^{1-W(\mathbf{a})} \oplus_{l=1}^n a_l x_l, \quad \mathbf{b} = (1)^n$$

where $W(\mathbf{b}) := \sum_{l=1}^n b_l$ denotes the Hamming distance of $\mathbf{b} \in \mathbb{Z}_2^n$.

Higher dimensional functions - II

Importantly, the coefficients $c_{\mathbf{a}} \notin \mathbb{Z}_2$ in general. However, they can be implemented by local phases, $\chi_k = e^{\pi c_k}$,

$$(-1)^{o(\mathbf{i})+c} = \prod_{k=1}^{N} \chi_k^{f_k(\mathbf{i})},$$

In particular, this leads to:

n-dimensional AND-function

In order to implement the function $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ in flat, deterministic $l2$-MBQC, $o(\mathbf{i}) = \prod_{k=1}^{n} i_k$ one needs no fewer than $N(o) = 2^n - 1$ qubits.

What about other (Boolean) functions?

Let $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a quadratic Boolean function,

$$o(\mathbf{i}) = \sum_{j=1}^{n} l_j i_j + \sum_{j<k} q_{jk} i_j i_k, \quad l_j, q_{jl} \in \mathbb{Z}_2.$$

Let Q be the symmetric matrix with $Q_{jj} = 0$ and $Q_{jl} = Q_{lj} = q_{jl}$ and denote the $\mathbb{Z}_2$-rank of Q by $r(o)$.

Optimal implementation of quadratic functions

Let $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a quadratic Boolean function. Then o can be computed within (stabilizer) $l2$-MBQC. Furthermore, the number of qubits needed to implement the $l2$-MBQC is $N(o) = r(o) + 1$ and is minimal.

A potential resource measure ...

For $l2$-MBQC we have the following:

- quadratic functions require $N(o) = r(o) + 1$ qubits
- n-dimensional AND-function requires $N(o) = 2^n - 1$ qubits
- in general N is only subadditive, i.e., $N(o_1 + o_2) \leq N(o_1) + N(o_2)$

Resource measure?

What is the minimal number of qudits needed to implement a given function $o : \mathbb{Z}_d^n \to \mathbb{Z}_d$ in flat, deterministic ld-MBQC?

Conclusion and Outlook

- generalisation of contextuality threshold for qubits in $l2$-MBQC to qudits in ld-MBQC
- discussion of contextual ld-MBQC examples
- introduction of resource measure N

- relate to problems in circuit synthesis
- relate to (group) cohomology
- relate to Clifford hierarchy

Thank you for your attention!

S. Abramsky, R. S. Barbosa, and S. Mansfield.
Contextual Fraction as a Measure of Contextuality.
Physical Review Letters, 119(5):050504, August 2017.

M. Frembs, S. Roberts, and S. D. Bartlett.
Contextuality as a resource for measurement-based quantum computation beyond qubits.
New Journal of Physics, 20(10):103011, October 2018.

R. Raussendorf.
Contextuality in measurement-based quantum computation.
Physical Review A, 88(2):022322, August 2013.