Target circuits for data collection on Quantinuum emulator and hardware

Dominik Leichtle[*]

April 2, 2024

1 General remarks

Note that as opposed to the convention to describe the graph states in verification protocols as CZ-entangled $|+\rangle$-states, *i.e.*, in the X-Y-plane, in the following we will choose the convention to formulate all tests and protocols equivalently in the Y-Z-plane. This avoids randomization by rotations around the Z-axis which would be virtually resolved in software on Quantinuum's hardware, and rather randomizes by using rotations around the X-axis which are native in terms of Quantinuum's gate set.

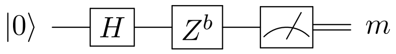
2 Secret-dependency of noise in single-qubit preparation

The formal verification and benchmarking techniques [LMKO21] that we intend to implement on Quantinuum's hardware platform must still rely on a small set of assumptions on the structure and magniture of the noise present during the execution of the protocol. This comes from the fact that the verification mechanisms are to be performed *on-chip*, *i.e.*, there is no physical separation between verifier-side and server-side quantum operations. The goal of the set of experiments in this section is to check whether these assumptions are justified, or whether the protocols require adjustment to the physical reality of the noise.

The necessary assumption for the protocol is simple: the noise present during the single-qubit preparation in the first stage of the protocol must be independent of the description of the state to be prepared. To check this condition and justify our assumptions, we want to gather information about the density matrix describing the actual single-qubit state which is prepared when the hardware is instructed to prepare a specific target state, using standard quantum state tomography.

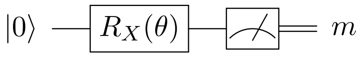
[*] dleichtl@ed.ac.uk

This following Circuit (1) prepares $|+\rangle$- and $|-\rangle$-states, depending on the choice of $b \in \{0,1\}$. Measurements are to be performed in randomly chosen Pauli-basis.



(1)

The next Circuit (2) prepares rotated states in the Y-Z-plane, for rotation angle $\theta \in \Theta = \left\{ \frac{j\pi}{4} \,\middle|\, j = 0, \ldots, 7 \right\}$. Measurements are again to be performed in randomly chosen Pauli-basis.



(2)

It is important that for each shot the parameter b (or θ, respectively), the measurement outcome m, and the measurement basis are recorded.

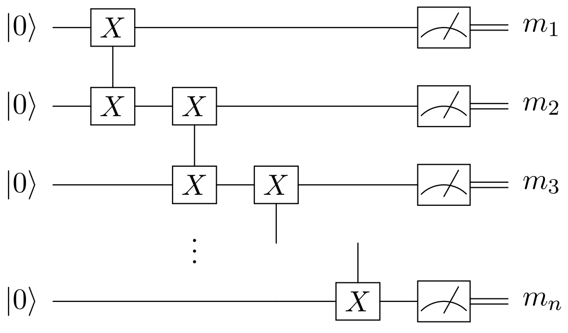
3 Noise accumulation in tests

The goal of the experiments described in this section is to gather data that allows us to make statements about how the protocol, and mainly the subroutine given by the tests, is affected by the noise. This includes getting a better understanding for how noise accumulates with a growing number of qubits and different types of resources, *i.e.*, different types of topologies for the used graph states.

The following set of experiments, ordered by growing complexity, aims at analyzing the impact of noise on the tests that are an essential part of our verification and benchmarking techniques. Each should be performed for a growing number of qubits $n = 1, 2, \ldots$ to find the cut-off point at which the noise destroys too much information in the measurement outcomes for them to be useful.

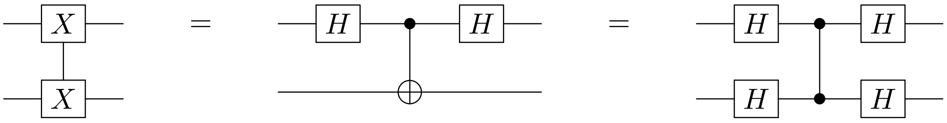
3.1 Stabilizer tests on linear cluster states

As a first and simple circuit which however already provides meaningful insight, we consider the following example of the creation of a linear cluster state, followed by a stabilizer measurement, that should allow us to extract a deterministic binary outcome in the noiseless case, and is therefore fit to start judging the impact of noise on our testing techniques.



(3)

In this circuit, the X-controlled X-gate can be rewritten as follows.



(4)

The parameters of Circuit (3) are:

- the number of qubits n,
- the (Pauli, stabilizer) measurement basis.

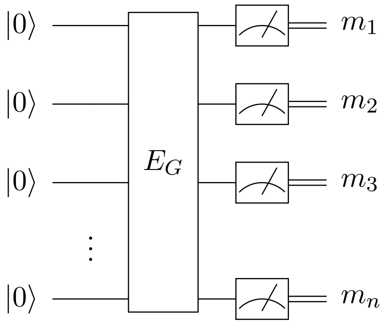
To sample a measurement basis, *i.e.*, a stabilizer of this specific graph state, proceed in the following way:

1. Sample $b_i \leftarrow_{\$} \{0,1\}$ for $i = 1, \ldots, n$, i.i.d. and uniformly at random.
2. The Pauli measurement bases are given by:
   - Measure the first qubit in the $Z^{b_1}X^{b_2}$-basis, *i.e.*, $\begin{cases} Z\text{-basis, if } b_1 = 1, b_2 = 0, \\ Y\text{-basis, if } b_1 = 1, b_2 = 1, \\ X\text{-basis, if } b_1 = 0, b_2 = 1. \end{cases}$
   - Measure the i-the qubit ($i = 2, \ldots, n-1$) in the $Z^{b_i}X^{b_{i-1} \oplus b_{i+1}}$-basis.
   - Measure the n-the qubit in the $Z^{b_n}X^{b_{n-1}}$-basis.

The data that needs to be recorded for each shot includes the number of qubits n, all measurement bases, and all measurement outcomes $\{m_i\}_{i=1,\ldots,n}$.

3.2 Generalizing the resource state

Using the stabilizer testing strategy from [KKL+22], we can generalize beyond linear cluster states and to arbitrary topologies of graph states. To this end, let $G = (V, E)$ be a graph on $|V| = n$ vertices which in the following we assume to be labeled $1, \ldots, n$ for convenience. Consider the following Circuit (5) which implements the creation of a graph state described by G, followed by a stabilizer measurement.



(5)

The entangling operation E_G creating the graph state is given by

$$E_G = \prod_{\{i,j\} \in E} XX_{i,j},$$

where $XX_{i,j}$ is defined as in Circuit 4. To sample a measurement basis, *i.e.*, a stabilizer of the graph state described by G, proceed in the following way:

1. Sample $b_i \leftarrow_\$ \{0,1\}$ for $i = 1, \dots, n$, i.i.d. and uniformly at random.
2. The Pauli measurement basis for qubit/vertex i is given by

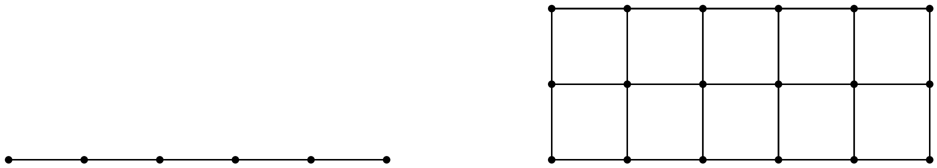
$$Z^{b_i} X^{\bigoplus_{j \in n_G(i)} b_j},$$

   where $n_G(i) = \{j \in V \mid \{i,j\} \in E\}$ is the neighborhood of vertex i.

The data that needs to be recorded for each shot includes the number of qubits n, the graph G, all measurement bases, and all measurement outcomes $\{m_i\}_{i=1,\dots,n}$.

Linear cluster state. Note that the linear cluster state from the previous section is a special case where the graph G is a line graph on n vertices.

2-dimensional cluster state. To generalize, the cluster state can be grown into the second dimension. For width k and depth m, the 2-dimensional cluster state has $n = k \times m$ vertices; its topology is depicted in Figure 1b.



(a) Linear cluster state with $n = 6$ vertices.

(b) 2-dimensional cluster state with width $k = 3$ and depth $m = 6$.

Figure 1: 1- and 2-dimensional cluster states.

Brickwork state. The brickwork state is known to be universal and convenient for translations of quantum algorithms from the circuit model to measurement-based quantum computing (MBQC). A single "brick" is depicted in Figure 2. A detailed description of the brickwork state can be found in [KKL$^+$23].

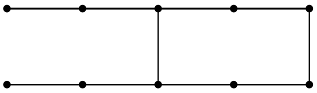
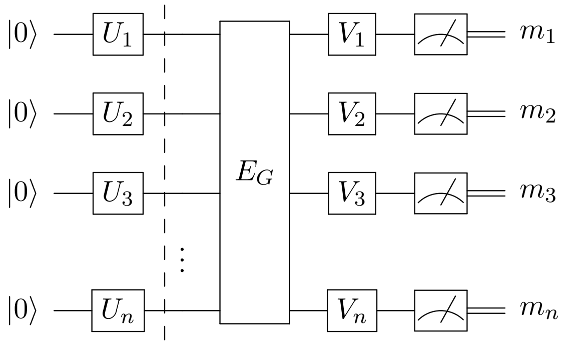


Figure 2: A single brick, building block of the family of brickwork states.

3.3 Adding randomization

To achieve its strong cryptographic guarantees, the used verification techniques and hence the benchmarking protocol in question require randomization of each qubit involved in the computation. The target computation including the randomizing unitaries U_i, V_i is depicted as Circuit 6. Note the barrier after the first layer of randomization which must guarantee that no optimizations or circuit simplifications carry over beyond to its right side.



(6)

All measurements are to be performed in the Z-basis.

To sample the circuit randomization, given as unitaries U_i, V_i, sample a Pauli measurement basis as in Section 3.2. Distinguish the following cases qubit by qubit:

1. If qubit i would have been measured in the X-basis, sample $b_i \leftarrow_{\$} \{0, 1\}$, $\theta_i \leftarrow_{\$} \Theta$, and let $U_i = Z^i H$ and $V_i = R_X(-\theta_i)$.
2. If qubit i would have been measured in the Z-basis, sample $\theta_i \leftarrow_{\$} \Theta$, $r_i \leftarrow_{\$} \{0, 1\}$, and let $U_i = R_X(\theta_i + r_i\pi)$ and $V_i = R_X(-\theta_i)$.
3. If qubit i would have been measured in the Y-basis, sample $\theta_i \leftarrow_{\$} \Theta$, $r_i \leftarrow_{\$} \{0, 1\}$, and let $U_i = R_X(\theta_i + r_i\pi + \pi/2)$ and $V_i = R_X(-\theta_i)$.

It is important to keep the randomization parameters b_i, θ_i, r_i on the record, as they are necessary for the classical postprocessing of the data set.

3.4 Dummyless stabilizer tests

The verification protocol from [KKL+23] uses only states from the X-Y-plane of the Bloch sphere (in our case this can be adapted to using only states from the Y-Z-plane), and thus allows for a simple way to reduce stochastic leakages during the qubit initialization and preparation phase, in case this would become necessary because of too strong secret-dependence of the noise on the actual hardware.

To obtain a better understanding of the impact of noise on these more specific tests, it would be interesting to gather data when the tests are drawn from a subset of the stabilizer tests from Section 3.2, namely those without X-basis measurements. For a small number of qubits, a uniform distribution of these *dummyless* stabilizer tests can be obtained from rejection sampling as follows:

1. Sample a Pauli measurement basis as in Section 3.2.
2. If all qubits are to be measured in the Y- or Z-basis, accept this test and perform it. Otherwise, discard it and go back to step 1.

For the rest of the experiment, follow the exact steps of Section 3.2.

For a larger number of qubits, there exist efficient sampling techniques for non-uniform, but useful distributions, see [KKL+23].

Circuit randomization is applied just like in Section 3.3, just that all measurements are being performed in either the Y- or the Z-basis.

References

[KKL$^+$22] Theodoros Kapourniotis, Elham Kashefi, Dominik Leichtle, Luka Music, and Harold Ollivier. Unifying quantum verification and error-detection: Theory and tools for optimisations. *arxiv:2206.00631*, 2022.

[KKL$^+$23] Theodoros Kapourniotis, Elham Kashefi, Dominik Leichtle, Luka Music, and Harold Ollivier. Asymmetric quantum secure multi-party computation with weak clients against dishonest majority. Cryptology ePrint Archive, Paper 2023/379, 2023.

[LMKO21] Dominik Leichtle, Luka Music, Elham Kashefi, and Harold Ollivier. Verifying BQP computations on noisy devices with minimal overhead. *Phys. Rev. X Quantum*, 2(040302), 2021.