Implementation of a noise-robust quantum algorithm for multivariate polynomial factorization

Iñigo Perez [1,2] and Lian-Ao Wu [1,2,3]

[1]*Department of Physics, University of the Basque Country, UPV/EHU, 48080 Bilbao, Spain*
[2]*EHU Quantum Center, University of the Basque Country, UPV/EHU, 48011 Bilbao, Spain*
[3]*Ikerbasque, Basque Foundation for Science, 48011 Bilbao, Spain*

We implement in an IBM quantum computer a quantum algorithm for multivariate polynomial factoring and propose a noise-avoiding protocol to distill the experimental results in the presence of noise. This algorithm uses single-qubit quantum state tomography (QST) processes to factor a specific type of multivariate polynomials. In one-to-one correspondence, it encodes each multivariate polynomial to one quantum state. While the validity of the algorithm is experimentally verified, the quality of the final results is subjected to the decoherence levels of the preparation of the quantum states. In this paper we propose a protocol to ensure the validity of factors found by our algorithm in the presence of such decoherence and noise. This method might be, in fact, part of a larger class of methods based on that same premise and useful outside the implementation of this specific algorithm. In combination with the noise robustness of the single-qubit QST, our factorization algorithm performs perfectly, even reversing the effects of weak noise, for the second- to fifth-order polynomial cases for which it has been implemented.

I. INTRODUCTION

Experimental quantum computing, in its present status, is still a technology with limited applications: the noisy intermediate-scale quantum (NISQ) devices of today are far from being the mature quantum computers needed for useful implementation of the algorithms that gave fame to the field [1,2]. However, studies of quantum computation have notably progressed since the seminal publications in the early 1980s [3–5] and the discoveries of the first quantum algorithms [1,2,6–8] during the 1990s. These earlier protocols and algorithms were successfully tested shortly after in nuclear magnetic resonance (NMR) devices [9–11], and steady advances followed until the mid-2010s [12–20]. However, it was not until the last decade that, thanks to the development of gate-model quantum computers (QCs) with a longer coherence time, cloud platform QCs have become widely available for use in investigations through projects like the superconductor-based IBMQ [21], Rigetti [22], and Google Q AI [23]; the photonic Xanadu [24]; the ion-trapping Honeywell [25] and IonQ [26]; and other similar platforms. These advances, along with improvements in NMR quantum devices, have allowed a number of previously theoretical algorithms [27–37] to become experimentally implemented [38–50] in real quantum devices. The present realizability of those theoretical advances, together with the improvement of the physical devices themselves [51,52], will certainly allow broader uses of quantum computing technologies in the future.

In this paper we show the implementation of one task that QCs are able to perform in their current NISQ technological state: the multivariate polynomial factorization algorithm formulated theoretically in [53], which allows the identification

and extraction of first-order terms of a certain class of Nth-order multivariate polynomials in $O(N)$ steps. The specific protocol developed in this paper for implementation in realistic noisy quantum systems allows us to get rid, to a certain extent, of system-bath entanglement caused by decoherence and helps us find models in which noise does not affect the crucial factorability of the target polynomial P_T. For this proof of concept we have chosen the five-qubit QC IBMQ Santiago, whose technical details are shown in Table I.

II. THE ALGORITHM

There are only a few classes of quantum algorithms which offer a speedup over classical algorithms. It is these and any new quantum algorithms which provide the main motivation for the development of quantum devices and computers. In this sense, any new quantum algorithm with speedup over its classical counterpart is desired, although one may need time to find its practical utility.

One such example, the Deutsch-Jozsa algorithm, solves a black-box problem which probably requires exponentially many queries to the black box for any deterministic classical computer but can be done with exactly one query by a quantum computer. Moreover, this quantum algorithm may be overridden by statistical pseudorandom algorithms with an exponentially small error probability [54]. In the same sense, the algorithm presented here solves factorization of a specific class of multivariate polynomials. It should be mentioned that classical algorithms such as the Lenstra-Lenstra-Lovász are able to factor certain types of polynomials using a polynomial number of queries [55]. However, any classical algorithm would need an exponentially large storage space in order to deal with the 2^N different monomials or terms of a target

TABLE I. Details of the IBMQ Santiago device at the time of the experiments [58]. Note how the average CNOT error might be misleading since it takes into account severed connections, with error equal to 1. For that reason, the two more representative CNOT error values are included.

Parameter	Value
Qubit number	5
Processor type	Falcon r4L
Basis gates	CX, ID, RZ, SX, X
Average CNOT error	5.028×10^{-1}
CNOT error 0-1	5.885×10^{-3}
CNOT error 3-4	6.258×10^{-3}
Average readout error	6.542×10^{-2}
Average T1	$81.73\,\mu s$
Average T2	$104.68\,\mu s$
Quantum volume	32

polynomial of order N. A quantum device, on the other hand, can perform our algorithm with $O(N)$ operations and, crucially, using only $O(N)$ qubits of storage. Our quantum algorithms show quantum advance in factoring polynomials, perhaps in the same way the Deutsch-Jozsa algorithm advanced solving a black-box problem.

The goal of the implemented algorithm [53] is to factor the first-order terms of homogeneous multivariate polynomials constructed as linear combinations of the set of products of two different sets of variables, which we will represent with lowercase and uppercase letters. One such target multivariate polynomial could be $P_T = 2abC - 2aBC - Abc + ABc$, which factors as $(b - B) \times (2aC - Ac)$. Then, from the expanded form of P_T, our algorithm would extract an approximation of that first-order $(b - B)$ term, leaving $f(a, A, c, C)$ to be obtained by division.

It is known, as the Solovay-Kitaev theorem [56] tells us, that any quantum state can be approximated efficiently with only a small number of available gates and an oracle. Similarly, we can also assume that the target polynomial state P_T preexists in the computer. Then, the number of steps required for a classical computer to trace the N-qubit state and to obtain the reduced density matrices is $O(2^{2N})$, whereas a quantum computer needs only the $O(N)$ steps required to perform N single-qubit quantum state tomography (QST) processes: the quantum advantage is overwhelming [57]. Even without that general oracle, however, this algorithm can be performed without loss of efficiency for those states obtainable in a number of steps proportional to its number of qubits. It is important to note that with these single-qubit QSTs one cannot obtain the complete $2^N \times 2^N$ density matrix of the whole system like one would in a complete QST process. Doing so indeed requires $O(2^{2N})$ steps. It is precisely the ability to obtain the single-qubit reduced density matrices (RDMs) without having the complete N-qubit density matrix that gives QCs the advantage in this process of our algorithm.

Quantum computing, as it is widely known, is based on the manipulation of qubits, the fundamental unit of quantum information and analogs of the bits used in classical computing. Unlike bits, which can be in only states $|0\rangle$ and $|1\rangle$, qubits are represented by complex superpositions of the

form $|P_\psi\rangle = \omega |0\rangle + \Omega |1\rangle \ : |\omega|^2 + |\Omega|^2 = 1$. This, after we choose to relate the relaxed state $|0\rangle$ to lowercase variables and the excited state $|1\rangle$ to uppercase variables, allows the qubit to describe any normalized first-order multivariate polynomial of the form $P_\psi = \omega a + \Omega A \ : |\omega|^2 + |\Omega|^2 = 1$. There is also, then, a one-to-one correspondence between N-qubit pure states and normalized Nth-order multivariate polynomials. For non-normalized target polynomials, the leading constant can be externally encoded in classical bits, such as a 32-bit float, and can then be multiplied by our output polynomial as the final step of the procedure. The third-order target polynomial of our example, $P_T = 2abC - 2aBC - Abc + ABc$, would then be encoded in the quantum state $|P_T\rangle = (2\,|001\rangle - 2\,|011\rangle - |100\rangle + |110\rangle)/\sqrt{10}$.

Ideally, we would be able to build and measure $|P_T\rangle$ perfectly. Then, for $\rho_T \equiv |P_T\rangle \langle P_T|$, if we obtained the target RDMs $\rho_T^{(i)}$ of each of the N qubits,

$$\rho_T^{(i)} \equiv \mathrm{Tr}_1 \mathrm{Tr}_2 \cdots \mathrm{Tr}_{i-1} \mathrm{Tr}_{i+1} \cdots \mathrm{Tr}_N \rho_T, \qquad (1)$$

they would have an entropy $\mathcal{S}(\rho_T^{(i)}) = 0$ if and only if the ith variable pair could be extracted as a first-order factor $f(a_i, A_i)$ from the target polynomial. This somewhat obscure statement is much clarified once one understands its source: a matrix whose entropy is zero is a matrix that is pure. Then, as a single-qubit pure matrix, it can be written as a ket-bra of some single-qubit quantum state. As we have already shown, each quantum state has a related normalized polynomial. Thus, the detection of each single-qubit RDM with $\mathcal{S} = 0$ means the existence of a first-order term in the target multivariate polynomial.

However, in a realistic scenario, single-qubit QSTs or any analogous method are used to obtain the N RDMs, which will always introduce noise, both from the built state decohering before measurement and from the finite number of runs used to obtain the $3N$ averages $\langle z\rangle^{(i)}$, $\langle x\rangle^{(i)}$, and $\langle y\rangle^{(i)}$. Then, the obtained N RDMs are not the target ideal RDMs $\rho_T^{(i)}$ themselves, but some noisy version of them: $\rho_B^{(i)}$, the built RDMs. Each single-qubit RDM is given by measuring only the corresponding single qubit:

$$\rho_B^{(i)} = \tfrac{1}{2}(\mathbb{1} + \langle x\rangle^{(i)}\sigma_x + \langle y\rangle^{(i)}\sigma_y + \langle z\rangle^{(i)}\sigma_z), \qquad (2)$$

where $\mathbb{1}$ is the 2×2 identity and $\sigma_{x,y,z}$ are the three Pauli matrices. The values $\langle z\rangle^{(i)}$, $\langle x\rangle^{(i)}$, and $\langle y\rangle^{(i)}$ are each averaged over a number of runs (typically, 1024) of measurements of the qubit i in the corresponding direction.

The difference between the idealized $\rho_T^{(i)}$ and practical $\rho_B^{(i)}$ is that the latter includes noise. Due to the noise, in reality $\rho_B^{(i)}$ will never have an entropy reliably equal to zero. Since in the idealized algorithm no noise was taken into account, it was implicitly assumed that $\rho_B^{(i)} = \rho_T^{(i)}$, so we could allow ourselves to filter all $\rho_B^{(i)}$ with $\mathcal{S}(\rho_T^{(i)}) \neq 0$. However, if the algorithm is to be implemented in a real device, noise has to be taken into account. One needs to accept RDMs with $\mathcal{S} \approx 0$ as corresponding to a separable term, not just those with exactly $\mathcal{S} = 0$, and bear in mind that the difference comes from experimental deviations.

However, the one-to-one relationship between RDMs and first-order polynomial terms is only true for pure matrices. For this reason, here we introduce a protocol to transform the

TABLE II. Coefficients of the monomials of P_S and P_T.

Monomial	P_S (expanded)	P_T (expanded)
abcd	1.0727	1
abcD	$0.1103 - 0.0075\,i$	0
abCd	$1.0598 + 0.0237\,i$	1
abCD	$0.1091 - 0.0050\,i$	0
aBcd	$0.9967 - 0.0456\,i$	1
aBcD	$0.1021 - 0.0117\,i$	0
aBCd	$0.9857 - 0.0230\,i$	1
aBCD	$0.1012 - 0.0095\,i$	0
Abcd	$-0.9977 - 0.0354\,i$	-1
AbcD	$-0.1028 + 0.0033\,i$	0
AbCd	$-0.9849 - 0.0570\,i$	-1
AbCD	$-0.1016 + 0.0010\,i$	0
ABcd	$-0.9285 + 0.0095\,i$	-1
ABcD	$-0.0954 + 0.0075\,i$	0
ABCd	$-0.9175 - 0.0111\,i$	-1
ABCD	$-0.0944 + 0.0053\,i$	0

noisy built RDMs into matrices with $\mathcal{S}$ exactly equal to zero. We term those purified RDMs "separabilized RDMs," and we define them as follows:

$$\rho_S^{(i)} = \left| P_S^{(i)} \right\rangle \left\langle P_S^{(i)} \right| \quad : \quad \left| P_S^{(i)} \right\rangle = \frac{\omega_i \left| 0_i \right\rangle + \Omega_i \left| 1_i \right\rangle}{\sqrt{|\omega_i|^2 + |\Omega_i|^2}} \quad (3)$$

for the coefficients

$$\omega_i = \sqrt{\frac{1 + \langle z \rangle^{(i)}}{2}}, \quad \Omega_i = \frac{\langle x \rangle^{(i)} + i \langle y \rangle^{(i)}}{\sqrt{2 + 2 \langle z \rangle^{(i)}}}. \quad (4)$$

Then, the first-order polynomial term related to $\rho_S^{(i)}$ is

$$P_S^{(i)}(a_i, A_i) = \frac{\omega_i a_i + \Omega_i A_i}{\sqrt{|\omega_i|^2 + |\Omega_i|^2}}. \quad (5)$$

At this point, we have to bear in mind that $P_S^{(i)}$ should be verified as the correct factor since it has been obtained from $\rho_S^{(i)}$, an artificial matrix we have devised, and not directly from the measured $\rho_B^{(i)}$. Theoretically, a verification protocol would be to compare the coefficients of the expanded form of the obtained P_S with the coefficients of the target polynomial P_T, for which we know the expanded form only if we have it explicitly in oracle, as shown, for example, in Table II. However, the process would require us to compare 2^N numbers for an Nth-order polynomial and is not scalable. To avoid these problems we propose to process the verification using the fidelities

$$\mathcal{F}(\rho_1, \rho_2) \equiv \text{Tr}\left(\sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}}\right)^2 = \mathcal{F}(\rho_2, \rho_1) \quad (6)$$

between experimental $\rho_B^{(i)}$ and the separable RDM $\rho_S^{(i)}$, both 2×2 matrices. As a preliminary verification protocol, it uses available data from single-qubit QSTs and requires only $O(N)$ steps. If $\mathcal{F}(\rho_B^{(i)}, \rho_S^{(i)}) \approx 1$, then the separation process has barely changed the RDM, where we regard $\mathcal{F}(\rho_B^{(i)}, \rho_S^{(i)}) \approx 1$ as the first-order approximation of $\mathcal{F}(\rho_S^{(i)}, \rho_T^{(i)}) \approx 1$ so that the ith term is well separable from the rest and the polynomial term has the form of $P_S^{(i)}$. If, on the contrary, $\mathcal{F}(\rho_B^{(i)}, \rho_S^{(i)})$ is

FIG. 1. Implementation of the second-order multivariate polynomial $aB + AB$.

small, even if $S^{(i)} \approx 0$, no separable factor of the form $P_S^{(i)}$ will exist in our final polynomial.

III. IMPLEMENTATION OF TWO REPRESENTATIVE SECOND-ORDER MULTIVARIATE POLYNOMIALS IN THE PRESENCE OF DECOHERENCE

Now we test the multivariate polynomial factorization method theoretically proposed in [53] for two second-order multivariate polynomials in a real IBM QC, one factorable and one nonfactorable. These polynomials are represented by a two-qubit state each, for which they share a one-to-one correspondence, up to a normalization constant. The implementation will be built and measured using the IBM QC IBMQ Santiago. The characteristics of the device, detailed in IBMQ's documentation [58], are reproduced in Table I.

On the other hand, quantum decoherence and noise, caused by the interaction of the system with its environment, will ruin the dynamics and add additional difficulties to control. In the presence of decoherence and noise the built RDMs $\rho_B^{(i)}$ would, for instance, become nonseparable even if the ideally expected target multivariate polynomial P_T were factorable. Thanks to our confirmation protocol, in addition to the ideal-case algorithm [53], we can still distill the separable multivariate polynomial $P_S = P_S^{(1)} \times P_S^{(2)}$ from the measured $\rho_B^{(i)}$ RDMs and thus ensure that our model for the polynomial P_T retains its same factorability.

A. A factorable multivariate polynomial

It is clear that the second-order multivariate polynomial $aB + AB$ can be factored as $(a + A)B$, and its corresponding two-qubit state $(|01\rangle + |11\rangle)/\sqrt{2}$ can be separated into a multiplication of two single-qubit states. This shows that the separability of the quantum state is equivalent to the factorability of the corresponding multivariate polynomial. We now display the multivariate polynomial factorization algorithm, starting from this simple known state.

The polynomial P_T is generated via the circuit in Fig. 1, bearing in mind that qubit 0 corresponds to the first $a + A$ term, and qubit 1 corresponds to the first B.

The QST protocol for IBMQ Santiago starts with sending the circuit to the setup. After the standard 1024 runs for each axis Z, X, and Y, we obtain the expectation values $\langle z \rangle^{(i)}$, $\langle x \rangle^{(i)}$, and $\langle y \rangle^{(i)}$ shown in Table III(a).

Once we have Table III(a), the density matrix $\rho_B^{(i)}$ can be directly obtained by the standard QST procedure [57] in Eq. (2). The density matrices related to our first and second

TABLE III. Measurements of the expectation values needed as inputs for Eqs. (2) and (4). (a) Measurements for the factorable second-order multivariate polynomial in Sec. III A. (b) Measurements for the nonfactorable second-order multivariate polynomial in Sec. III B. (c) Measurements for the third-order multivariate polynomial in Sec. IV A. (d) Measurements for the fourth-order multivariate polynomial in Sec. IV B. (e) Measurements for the fifth-order multivariate polynomial in Sec. IV C.

(a) Factorable second-order multivariate polynomial		
	First term (q1)	Second term (q0)
$\langle z \rangle^{(i)}$	0.0742	-0.9453
$\langle x \rangle^{(i)}$	0.9746	0.1387
$\langle y \rangle^{(i)}$	0.0214	-0.0625

(b) Nonfactorable second-order multivariate polynomial		
	First term (q1)	Second term (q0)
$\langle z \rangle^{(i)}$	0.1133	0.0938
$\langle x \rangle^{(i)}$	0.1523	0.1230
$\langle y \rangle^{(i)}$	-0.0039	0.0274

(c) Third-order multivariate polynomial			
	First term (q2)	Second term (q1)	Third term (q0)
$\langle z \rangle^{(i)}$	0.0273	0.1992	-0.1934
$\langle x \rangle^{(i)}$	0.9453	-0.0293	-0.0469
$\langle y \rangle^{(i)}$	0.0234	-0.0332	-0.0449

(d) Fourth-order multivariate polynomial				
	First term (q3)	Second term (q2)	Third term (q1)	Fourth term (q0)
$\langle z \rangle^{(i)}$	0.0059	-0.0351	-0.0273	0.9570
$\langle x \rangle^{(i)}$	-0.9355	0.8965	0.9609	0.2012
$\langle y \rangle^{(i)}$	-0.0332	-0.0410	0.0215	-0.0137

(e) Fifth-order multivariate polynomial					
	First term (q4)	Second term (q3)	Third term (q2)	Fourth term (q1)	Fifth term (q0)
$\langle z \rangle^{(i)}$	0.9824	0.0391	0.0430	0.1074	-0.9258
$\langle x \rangle^{(i)}$	0.0352	-0.0625	-0.0410	0.9824	0.2383
$\langle y \rangle^{(i)}$	0.0723	-0.0234	0.0566	-0.0586	0.0586

terms are

$$\rho_B^{(1)} = \begin{pmatrix} 0.5371 & 0.4873 - 0.0107i \\ 0.4873 + 0.0107i & 0.4629 \end{pmatrix} \quad (7)$$

and

$$\rho_B^{(2)} = \begin{pmatrix} 0.0273 & 0.0693 + 0.0313i \\ 0.0693 - 0.0313i & 0.9727 \end{pmatrix}. \quad (8)$$

As shown in [53] and explained in Sec. II, in the ideal case these $\rho_B^{(i)}$ RDMs would represent a separable factor of P_B if and only if their von Neumann entropies $\mathcal{S}^{(i)}$ were exactly zero. In our realistic case, however, noise has made our two $\rho_B^{(i)}$ nonseparable, as expected. The entropies of the two RDMs are shown in Table IV(a): neither of the two is exactly zero, but we can take them as close to zero since with the confirmation method we have a way to justify that choice later.

From Eq. (4), we obtain

$$P_S^{(1)} = 1.0473a + (0.9502 + 0.0209i)A \approx (a + A),$$
$$P_S^{(2)} = 0.3383b + (0.8579 - 0.3866i)B \approx B, \quad (9)$$

which is the result we expected. Moreover, as A_i variables (A and B in this $N = 2$ case) correspond to excited states, they should partially relax into a_i states (a and b, respectively)

before measurement due to the environmental noise. This effect is more pronounced for the second term since $P_T^{(2)} = B$. As we will see, this relaxation happens in general for our measurements and will be the main source of our fidelity losses, as claimed by [48].

Using Eq. (3), we calculate the density matrices associated with these polynomials,

$$\rho_S^{(1)} = \begin{pmatrix} 0.5484 & 0.4975 - 0.0110i \\ 0.4975 + 0.0110i & 0.4516 \end{pmatrix} \quad (10)$$

and

$$\rho_S^{(2)} = \begin{pmatrix} 0.1145 & 0.2903 + 0.1308i \\ 0.2903 - 0.1308i & 0.8855 \end{pmatrix}. \quad (11)$$

As we can see by comparing each pair of ith RDMs, the separabilization procedure which obtains $\rho_S^{(i)}$ from $\rho_B^{(i)}$ has only a slight changing effect. To properly quantify the results, we calculate the fidelity between the experimental $\rho_B^{(i)}$ and separable $\rho_S^{(i)}$ RDMs, as shown in Eq. (6), and obtain good matches:

$$\mathcal{F}(\rho_B^{(1)}, \rho_S^{(1)}) = 0.9887, \quad \mathcal{F}(\rho_B^{(2)}, \rho_S^{(2)}) = 0.9129. \quad (12)$$

This is the end of the process: those fidelities show that, as $\rho_S^{(i)}$ is close to $\rho_B^{(i)}$, as long as we accept the measured $\rho_B^{(i)}$,

TABLE IV. Entropies and separability diagnoses of the RDMs for multivariate polynomials. For the single-qubit density matrix of a first-order multivariate polynomial, $S_{\mathrm{MAX}} = \log 2$. (a) Entropies and separabilities of the two $\rho_B^{(i)}$ RDMs in Sec. III A. By construction, $\mathcal{S}(\rho_S^{(i)}) \equiv 0$. (b) Entropies and separabilities of the two $\rho_B^{(i)}$ RDMs in Sec. III B. By construction, $\mathcal{S}(\rho_S^{(i)}) \equiv 0$. (c) Entropies and separabilities the three $\rho_B^{(i)}$ RDMs in Sec. IV A. By construction, $\mathcal{S}(\rho_S^{(i)}) \equiv 0$. (d) Entropies and separabilities of the four $\rho_B^{(i)}$ RDMs in Sec. IV B. By construction, $\mathcal{S}(\rho_S^{(i)}) \equiv 0$. (e) Entropies and separabilities of the five $\rho_B^{(i)}$ RDMs in Sec. IV C. By construction, $\mathcal{S}(\rho_S^{(i)}) \equiv 0$.

	$\mathcal{S}^{(i)}$	$\mathcal{S}^{(i)}/S_{\mathrm{MAX}}$	Separability diagnosis
(a) $\rho_B^{(i)}$ RDMs in Sec. III A			
First term	0.0613	8.84%	Separable
Second term	0.1029	14.85%	Separable
(b) $\rho_B^{(i)}$ RDMs in Sec. III B			
First term	0.6750	97.38%	Nonseparable
Second term	0.6808	98.21%	Nonseparable
(c) $\rho_B^{(i)}$ RDMs in Sec. IV A			
First term	0.1242	17.91%	Separable
Second term	0.6722	96.97%	Nonseparable
Third term	0.6722	96.98%	Nonseparable
(d) $\rho_B^{(i)}$ RDMs in Sec. IV B			
First term	0.1414	20.39%	Separable
Second term	0.2013	29.04%	Separable
Third term	0.0950	13.70%	Separable
Fourth term	0.0605	8.72%	Separable
(e) $\rho_B^{(i)}$ RDMs in Sec. IV C			
First term	0.0424	6.12%	Separable
Second term	0.6901	99.56%	Nonseparable
Third term	0.6898	99.51%	Nonseparable
Fourth term	0.0314	4.54%	Separable
Fifth term	0.1024	14.77%	Separable

we also have to trust using $\rho_S^{(i)}$ to calculate the first-order polynomial factors $P_S^{(i)}$, so our final approximation to the target polynomial is confirmed to be $P_S = P_S^{(1)} \times P_S^{(2)}$.

We have demonstrated how our method is able to offer P_S as an approximation equally factorable to the target polynomial P_T. On the other hand, the algorithm is also capable of identifying the cases when P_T is nonfactorable. To show this, of course, we shall start with the corresponding entangled polynomial and see whether the values of $S^{(i)}$ and $\mathcal{F}(\rho_B^{(i)}, \rho_S^{(i)})$ vary in a significant manner.

B. A nonfactorable multivariate polynomial

Now we start with the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$, with the maximal von Neumann entropy $\log 2$. In this sense, we can call $P_T = ab + AB$ a maximally nonfactorable multivariate polynomial. The state is built via the circuit in Fig. 2, and the expectation values of the measurements obtained in IBMQ Santiago are shown in Table III(b). Substituting these

FIG. 2. Implementation of the second-order multivariate polynomial $ab + AB$.

expectation values into Eq. (2), we obtain the density matrices

$$\rho_B^{(1)} = \begin{pmatrix} 0.5566 & 0.0762 + 0.0020i \\ 0.0762 - 0.0020i & 0.4434 \end{pmatrix} \quad (13)$$

and

$$\rho_B^{(2)} = \begin{pmatrix} 0.5469 & 0.0615 - 0.0137i \\ 0.0615 - 0.0137i & 0.4531 \end{pmatrix}, \quad (14)$$

and they have entropies very close to the maximum, as shown in Table IV(b). This verifies that P_T is nonfactorable since such high entropies could not be produced by the noise perturbing a separable P_T.

Having concluded that P_T is nonfactorable, in a real scenario we would end our analysis since we have no separable factors whose coefficients need to be calculated. However, we can still run our protocol to see what erroneous conclusion can be reached. Having an idea of to what extent the resulting P_S is flawed is still insightful for this case study.

Using the values in Table III(b) in Eq. (2), we obtain

$$P_S^{(1)} = 0.9908a + (0.1356 - 0.0035i)A \approx a,$$
$$P_S^{(2)} = 0.9934b + (0.1118 + 0.0248i)B \approx b$$
$$\Rightarrow P_T \approx P_S \approx ab. \quad (15)$$

This result is obviously incorrect, as we know that $P_T = ab + AB$. Moreover, the obtained separated RDMs, defined in Eq. (3), have the forms

$$\rho_S^{(1)} = \begin{pmatrix} 0.9816 & 0.1343 + 0.0034i \\ 0.1343 - 0.0034i & 0.01839 \end{pmatrix} \quad (16)$$

and

$$\rho_S^{(2)} = \begin{pmatrix} 0.9867 & 0.1110 - 0.0247i \\ 0.1110 + 0.0247i & 0.0131 \end{pmatrix}, \quad (17)$$

which have nothing to do with the forms of $\rho_B^{(i)}$ obtained from the QST measurements. Their relative fidelities are far from 1:

$$\mathcal{F}(\rho_B^{(1)}, \rho_S^{(1)}) = 0.5750, \quad \mathcal{F}(\rho_B^{(2)}, \rho_S^{(2)}) = 0.5600. \quad (18)$$

We see that the confirmation method is not only able to confirm the factorability of factorable polynomials but would also be able to spot false-positive cases treated as separable when they should have not been.
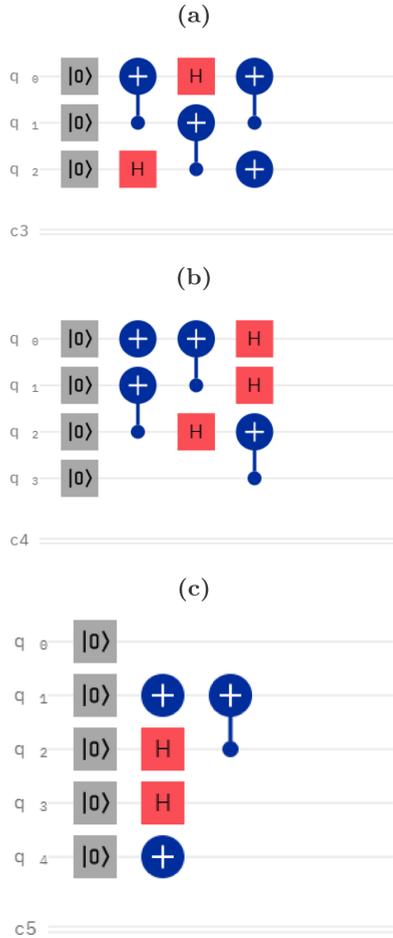
FIG. 3. Circuits used in Sec. IV that encode the (a) third-, (b) fourth-, and (c) fifth-order generated multivariate polynomials in Secs. IV A, IV B, and IV C, respectively.

IV. SCALABILITY: IMPLEMENTATION FOR HIGHER-ORDER MULTIVARIATE POLYNOMIALS IN THE PRESENCE OF NOISE

We now come to verify the scalability of our protocol. Using the IBM QC IBMQ Santiago [58] described in Table I, the protocol will be applied to third-order, fourth-order, and fifth-order multivariate polynomials in the presence of noise. The third-order and fourth-order circuits will be created randomly, without taking into account any optimization, to avoid testing the method in just the most favorable scenarios. Even if simpler versions of the circuits would make separability easier to spot in these simple cases, this will not be the case in large-scale circuits with hundreds of qubits and tens of thousands of gates, to which the method is meant to be applied in the future. The fifth-order circuit, however, has been constructed as simply as possible in order to minimize noise and thus emulate the effect of a quantum-error-correction algorithm.

A. A third-order multivariate polynomial

Let us now verify the protocol for a three-qubit case. We construct a circuit with at least one separable qubit to test the protocol. The circuit is shown in Fig. 3, and Table III(c) reflects the expectation values for the three orthogonal direc-

tions required by the QST. The experiment shows that the built RDMs are rather noisy. By calculating the entropy with those RDMs, we obtain Table IV(c).

In this realistic, noisy scenario the entropies cannot be exactly zero, as shown in Sec. II. However, there is a clear difference between the first term with much less entropy and the other two, which almost maximize their respective entropies. Our algorithm ascertains that this first term should be taken as separable from the rest of the polynomial and that the imperfectness of entropies in Table IV(a) would have been introduced by the noise in the process of building the circuit. Under this assumption we calculate the separabilized polynomial given by the only separable qubit, using Eq. (4) to obtain the coefficients of Eq. (5), and obtain

$$P_S^{(1)} = 1.0406a + (0.9574 + 0.0238i)A, \quad (19)$$

which almost restores the term $a + A$. In order to verify the validity of that term, we now have to calculate the fidelity between $\rho_B^{(1)}$ and $\rho_S^{(1)}$:

$$\mathcal{F}(\rho_B^{(1)}, \rho_S^{(1)}) = 0.9723. \quad (20)$$

As this high fidelity confirms the validity of $P_S^{(1)}$, our approximation of the target multivariate polynomial would be, then, $P_S = P_S^{(1)} \times f(b, B, c, C)$, which crucially maintains the factorability properties of the target polynomial $P_T = (a + A)(bC + Bc)$.

B. A fourth-order multivariate polynomial

We build a fourth-order multivariate polynomial using the circuit shown in Fig. 3, and the QST results are shown in Table III(d). With these expectation values we can calculate the four RDMs $\rho_B^{(i)}$ and four entropies, as shown in Table IV(d). Here, as in Table IV(c), we have obtained entropies that are far from zero. However, none of them are above or close to 90% either, so our preliminary conclusion would be that the four qubits were separable from each other on the original P_T.

Under this assumption, the four purified $P_S^{(i)}$ obtained are

$$P_S^{(1)} = 1.0352a - (0.9629 + 0.0342i)A \approx a - A,$$
$$P_S^{(2)} = 1.0355b + (0.9622 - 0.0440i)B \approx b + B,$$
$$P_S^{(3)} = 1.0059c + (0.9938 + 0.0222i)C \approx c + C,$$
$$P_S^{(4)} = 0.9947d + (0.1023 - 0.0069i)D \approx d. \quad (21)$$

Now our protocol is to check the fidelities between $\rho_B^{(i)}$ and $\rho_S^{(i)}$:

$$\mathcal{F}(\rho_B^{(1)}, \rho_S^{(1)}) = 0.9671,$$
$$\mathcal{F}(\rho_B^{(2)}, \rho_S^{(2)}) = 0.9462,$$
$$\mathcal{F}(\rho_B^{(3)}, \rho_S^{(3)}) = 0.9804,$$
$$\mathcal{F}(\rho_B^{(4)}, \rho_S^{(4)}) = 0.9890. \quad (22)$$

With these fidelities we confirm that P_S is a good approximation for P_T. Taking into account that we have taken entropies as high as almost 30% as $S^{(i)} \approx 0$, these high fidelities are

notable. Thanks to the justification protocol, the robustness of the separabilization procedure with respect to noise is clear.

For this fully factorable case, we can obtain an approximation to the whole target polynomial. From Eqs. (21), we obtain

$$P_S \approx (a - A)(b + B)(c + C)d = P_T. \qquad (23)$$

We can also compare the polynomial $P_S \equiv \prod_i P_S^{(i)}$ with the expanded form of P_T. As we can see by examining Table II, the coefficients of both fit well with each other, showing that the obtained approximation P_S not only imitates the factoring properties of P_T but is also a good numerical match.

C. A fifth-order representative multivariate polynomial

To demonstrate fifth-order multivariate polynomials we focus on a carefully chosen multivariate polynomial to understand to what extent our protocol could be refined through the improvement of the measured state. It is interesting to note that such a scheme is analogous to implementing a quantum-error-correction algorithm.

We generate $P_T = a(bC + Bc)(d + D)E$ using the simple circuit in Fig. 3. Remember that in a real-life scenario one would not have the factorization of P_T since that is precisely what we are looking for. The QST results are given in Table III(e), and RDM entropies are given in Table IV(e), which gives two clearly different entropy levels. With entropies $\mathcal{S}^{(2)}, \mathcal{S}^{(3)} > 99.5\%$, the second and third terms are not individually separable. This is an improvement with respect to the nonseparable terms in the above third-order multivariate polynomial in Sec. IV A, as shown in Table IV(c), in which entropies are dropped from 100% to lower than 97%. In the case of the separable terms we can also see an improvement: from 8.72%–29.04% in the three- and four-qubit cases to 4.54%–14.77%, the entropy range of these RDMs has been approximately halved.

The purified states for the separable terms are

$$P_S^{(1)} = 0.9992a + (0.0177 + 0.0364i)A \approx a,$$
$$P_S^{(4)} = 1.0571d + (0.9378 - 0.0559i)D \approx d + D,$$
$$P_S^{(5)} = 0.2895e + (0.9295 + 0.2286i)E \approx E. \qquad (24)$$

Results of Eq. (24) lead to the polynomial $P_S \approx a \times f(b, B, c, C) \times (d + D)E$, which is exactly the same form of the target multivariate polynomial $a(bC + Bc)(d + D)E$.

In order to quantify this closeness, we turn to our confirmation protocol. The obtained fidelities are

$$\mathcal{F}\big(\rho_B^{(1)}, \rho_S^{(1)}\big) = 0.9929,$$
$$\mathcal{F}\big(\rho_B^{(4)}, \rho_S^{(4)}\big) = 0.9950,$$
$$\mathcal{F}\big(\rho_B^{(5)}, \rho_S^{(5)}\big) = 0.9533, \qquad (25)$$

which confirm the validity of the three $P_S^{(i)}$ obtained.

As mentioned in Sec. III A, relaxed a_i terms like a barely suffer any changes, indicating the robustness of our algorithm against decoherence. However, A_i terms like E, corresponding to excited states, also suffer from relaxation. This means that experimentally, there is no symmetry between a_i and A_i terms, even though the theoretical (noiseless) version of the algo-

TABLE V. Cases when, for separable $P_T^{(i)}$, $\mathcal{F}(\rho_S^{(i)}, \rho_T^{(i)}) > \mathcal{F}(\rho_B^{(i)}, \rho_T^{(i)})$. N/A = not applicable.

	$N = 2$	$N = 3$	$N = 4$	$N = 5$
$i = 1$	Yes	Yes	Yes	Yes
$i = 2$	No	N/A	Yes	N/A
$i = 3$		N/A	Yes	N/A
$i = 4$			Yes	Yes
$i = 5$				No

rithm treats them equally and interchangeably. This means that even if the coding of a_i and A_i into relaxed and excited states of the qubit, respectively, is completely arbitrary, noise breaks that symmetry, and the choice may end up influencing the experimental results.

V. NOISE-REVERTING EFFECTS OF FIXED-PROPERTY RDMS

A remarkable tendency observed when comparing the built and separabilized RDMs with the target RDMs one would obtain in the ideal case is the following: $\rho_S^{(i)}$ seem to be of a better quality than $\rho_B^{(i)}$. In other words, the separabilization process tends to reverse the effects of the small quantities of noise that make $\rho_B^{(i)}$ different from $\rho_T^{(i)}$, leading to $\mathcal{F}(\rho_S^{(i)}, \rho_T^{(i)}) > \mathcal{F}(\rho_B^{(i)}, \rho_T^{(i)})$ in most of the studied examples, as shown in Table V.

Then, it seems that forcing our RDMs to have some properties we know they should have (in this case, the factorability of ρ_T) does not come with a cost in fidelity; on the contrary, it may well be that, for some small amounts of noise, those imposed properties improved the quality of our RDMs (here $\rho_S^{(i)}$) with respect to the freely measured $\rho_B^{(i)}$.

The two examples where this is not fulfilled, the $N = 2$, $i = 2$, and $N = 5$, $i = 5$, cases, represent terms of the form $P_T^{(i)} = A_i$ encoded into excited $|1\rangle$ states, which means they suffer maximally from relaxation. In those cases, noise is too great for the separabilization process to reverse. However, even if in those two cases $\mathcal{F}(\rho_S^{(i)}, \rho_T^{(i)}) < \mathcal{F}(\rho_B^{(i)}, \rho_T^{(i)})$, the final results are still totally valid.

VI. STATISTICAL ERROR ASSESSMENT

States obtained through QST present two different types of errors. On the one hand, they suffer the losses and decoherence inherent in physical quantum devices, as has been discussed. On the other hand, the finite size of the measurement sample used in QST allows for only certain mathematical significance. In this section the size of the latter, which is controllable, will be calculated in order to show how it is smaller than the physical noise we cannot control.

In order to quantify the effects of the mathematical uncertainty produced by the QST method itself, as opposed to the physical noise produced by the imperfections of the QC, one can calculate the width of the distribution of the results that could arise purely from the measurement of the state. The standard deviation of such a binomial distribution

is $\sigma = \sqrt{np(1-p)}$ for a number n of runs and a probability p of measuring the first eigenstate. Both from the formula and intuitively, we understand that for eigenstates of the measured direction that width is zero. One example of this is measuring state $|0\rangle$ on the z axis: it will always give a measurement of $\langle z \rangle = -1 \pm 0$. The maximum width is achieved when $p = 0.5$, as in the case of $(|0\rangle + |1\rangle)/\sqrt{2}$. Here the chances of measuring each eigenstate are equal, which gives a symmetric binomial distribution. For 1024 runs this standard deviation is 16, so the value of our measurement will be $\langle z \rangle = 0 \pm {}^{16}/_{1024}$. Keeping the error at one significant figure, $\langle z \rangle = 0.00 \pm 0.02$. To translate this measurement error into the error of the coefficients of the terms of the polynomial we can apply the usual error-propagation formula over Eq. (4),

$$\sigma_\omega = \left| \frac{\partial \omega}{\partial \langle z \rangle} \right| \sigma_z = \frac{1}{4}\sqrt{p/n}, \tag{26}$$

which has its maximum at $p = 1$. For $n = 1024$, $\sigma_\omega^{\mathrm{MAX}} = {}^1/_{128} \approx 0.008$. That value, or 0.01 for terms normalized to $\sqrt{2}$ like $a + A$, is the maximum error that arises from QST.

Most of the obtained $P_S^{(i)}$ differ from their $P_T^{(i)}$ by more than the maximum deviation $\sigma_\omega^{\mathrm{MAX}}$, which shows that $n = 1024$ runs is enough for our purposes and that physical noise plays a role in the final results of our implementation. However, as $\sigma_\omega \propto {}^1/\sqrt{n}$, statistical noise can be reduced, increasing the run sample size if needed.

VII. CONCLUSIONS

Our experiments confirm that, using the noise-avoiding protocol presented in this paper, our Nth-order multivariate polynomial factorization algorithm [53] can be successfully implemented in IBM QCs. We are able to overcome the noise introduced by the quantum circuits and obtain results close to the ideal factorization. This is the case even for multivariate polynomial terms of the form A_i, encoded into excited $|1\rangle$ states, that partially relax into a_i states before measurement, which represent the noisiest scenarios [48]. Thanks to the implementation protocol, for all the presented target polynomials P_T we are able to discern the individual separability of all

qubits of the target state and provide a close approximation P_S to those first-order factorable terms of the target polynomial. We are able to do this in $O(N)$ steps, just as in the ideal case of the theoretical algorithm [53]. This approximation P_S is factorable for all originally separable qubits, by construction, retaining the main property of the target polynomial P_T the algorithm is trying to analyze.

The protocol that allows the implementation of the algorithm in the nonideal case is based on the controlled modification of the measured state. The modified density matrix, upon which known properties of the target state are imposed, tends to actually get closer to the target density matrix under limited enough noise. Due to the general nature of the method, it can be implemented outside the ambit of this specific algorithm in those cases when certain properties of the target state are known.

Quantum-error-correction methods [48,49] that preserve the shape of the built state, keeping it close to the target noiseless state, are easily combined with our polynomial factorization quantum algorithm since they are applied to the construction of the state itself before measurements, improving the input of the QST and so improving the quality of our algorithm's predictions. Due to the asymmetry between excited and relaxed qubits, it would also be relevant to choose the correct encoding for each problem: the less excitation there is in the target state, the less relaxation decoherence it will suffer. The protocol proposed in this paper ensure the validity of our algorithm in the presence of decoherence and noise.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, NW Washington, DC, 1994).

[2] L. K. Grover, in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing—STOC '98* (ACM Press, New York, NY, 1998).

[3] Y. Manin, *Vychislimoe i nevychislimoe* (Sovetskoe radio, Moscow, 1980).

[4] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[5] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[6] R. J. D. Deutsch, Proc. R. Soc. London, Ser. A **439**, 553 (1992).

[7] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).

[8] P. W. Shor, SIAM Rev. **41**, 303 (1999).

[9] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).

[10] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).

[11] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 883 (2001).

[12] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B **11**, 1085 (1997).

[13] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[14] P. Zanardi, Phys. Rev. A **57**, 3276 (1998).

[15] D. A. Lidar and K. B. Whaley, Decoherence-free subspaces and subsystems, in *Irreversible Quantum Dynamics*, Lecture Notes

in Physics, Vol. 622, edited by F. Benatti and R. Floreanini (Springer, Berlin, Heidelberg, 2003).

[16] D. A. Lidar and L.-A. Wu, Phys. Rev. A **67**, 032313 (2003).

[17] A. Mizel, Phys. Rev. A **70**, 012304 (2004).

[18] A. Mizel, D. A. Lidar, and M. Mitchell, Phys. Rev. Lett. **99**, 070502 (2007).

[19] J. Jing, L.-A. Wu, M. Byrd, J. You, T. Yu, and Z.-M. Wang, Phys. Rev. Lett. **114**, 190502 (2015).

[20] P. V. Pyshkin, D.-W. Luo, J. Jing, J. Q. You, and L.-A. Wu, Sci. Rep. **6**, 37781 (2016).

[21] IBM Quantum superconducting platform, https://quantum-computing.ibm.com/services?services=systems.

[22] Rigetti superconducting platform, https://www.rigetti.com/what-we-build.

[23] Google Quantum AI superconducting platform, https://quantumai.google/quantum-computing-service.

[24] Xanadu photonic platform, https://www.xanadu.ai/hardware.

[25] Honeywell ion-trap platform, https://www.honeywell.com/us/en/company/quantum/quantum-computer.

[26] IonQ ion-trap platform, https://ionq.com/.

[27] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[28] P. Zanardi, Phys. Rev. A **63**, 012301 (2000).

[29] M. S. Byrd and D. A. Lidar, Phys. Rev. Lett. **89**, 047901 (2002).

[30] S. Bose, Phys. Rev. Lett. **91**, 207901 (2003).

[31] L.-A. Wu, M. S. Byrd, and D. A. Lidar, Phys. Rev. Lett. **89**, 127901 (2002).

[32] M. S. Byrd, D. A. Lidar, L.-A. Wu, and P. Zanardi, Phys. Rev. A **71**, 052301 (2004).

[33] L.-A. Wu and D. Lidar, Quantum Inf. Process. **5**, 69 (2006).

[34] L.-A. Wu, G. Kurizki, and P. Brumer, Phys. Rev. Lett. **102**, 080405 (2009).

[35] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).

[36] E. Farhi, J. Goldstone, and S. Gutmann, arXiv:1411.4028.

[37] T. Xin, Phys. Rev. A **102**, 052410 (2020).

[38] J. Jing and L.-A. Wu, Sci. Rep. **3**, 2746 (2013).

[39] J. Jing, L.-A. Wu, J. Q. You, and T. Yu, Phys. Rev. A **88**, 022333 (2013).

[40] X.-D. Cai, C. Weedbrook, Z.-E. Su, M.-C. Chen, M. Gu, M.-J. Zhu, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **110**, 230501 (2013).

[41] S. Barz, I. Kassal, M. Ringbauer, Y. O. Lipp, B. Dakić, A. Aspuru-Guzik, and P. Walther, Sci. Rep. **4**, 6115 (2014).

[42] J. Pan, Y. Cao, X. Yao, Z. Li, C. Ju, H. Chen, X. Peng, S. Kais, and J. Du, Phys. Rev. A **89**, 022313 (2014).

[43] Z.-M. Wang, M. S. Byrd, J. Jing, and L.-A. Wu, Phys. Rev. A **97**, 062312 (2016).

[44] J. Jing, M. S. Sarandy, D. A. Lidar, D.-W. Luo, and L.-A. Wu, Phys. Rev. A **94**, 042131 (2016).

[45] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Nature (London) **536**, 63 (2016).

[46] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe, Nat. Commun. **8**, 1918 (2017).

[47] C. Flühmann, T. L. Nguyen, M. Marinelli, V. Negnevitsky, K. Mehta, and J. P. Home, Nature (London) **566**, 513 (2019).

[48] B. Pokharel, N. Anand, B. Fortman, and D. A. Lidar, Phys. Rev. Lett. **121**, 220502 (2018).

[49] B. G. Markaida and L.-A. Wu, Sci. Rep. **10**, 18846 (2020).

[50] U. Skosana and M. Tame, Sci. Rep. **11**, 16599 (2021).

[51] A. Mizel, M. W. Mitchell, and M. L. Cohen, Phys. Rev. A **63**, 040302(R) (2001).

[52] A. Mizel, M. W. Mitchell, and M. L. Cohen, Phys. Rev. A **65**, 022315 (2002).

[53] L.-A. Wu and M. S. Byrd, Quantum Inf. Process. **8**, 1 (2009).

[54] D. Simon, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society, NW Washington, DC, 1994), pp. 116–123.

[55] H. W. J. Lenstra, A. K. Lenstra, and L. Lovász, Math. Ann. **261**, 515 (1982).

[56] C. M. Dawson and M. A. Nielsen, arXiv:quant-ph/0505030.

[57] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).

[58] Details of IBMQ Santiago, https://quantum-computing.ibm.com/services?services=systems&system=ibmq_santiago.