

Prime number factorization using a spinor Bose–Einstein condensate inspired topological quantum computer

Emil G netay Johansen and Tapio Simula
Optical Sciences Centre, Swinburne University of Technology,
Melbourne 3122, Australia

Inspired by non-abelian vortex anyons in spinor Bose–Einstein condensates, we consider the quantum double $\mathcal{D}(\mathbb{Q}_8)$ anyon model as a platform to carry out a particular instance of Shor’s factorization algorithm. We provide the excitation spectrum, the fusion rules, and the braid group representation for this model, and design a circuit architecture that facilitates the computation. All necessary quantum gates, less one, can be compiled exactly for this hybrid topological quantum computer, and to achieve universality the last operation can be implemented in a non-topological fashion. To analyse the effect of decoherence on the computation, a noise model based on stochastic unitary rotations is considered. The computational potential of this quantum double anyon model is similar to that of the Majorana fermion based Ising anyon model, offering a complementary future platform for topological quantum computation.

Introduction:— The quest for fault-tolerant quantum computation is a substantial contemporary pursuit in science and technology [1, 2]. It is the intrinsic parallelism exhibited by quantum systems that is responsible for their extraordinary computational potential, and consequently, quantum systems could serve as an arena for simulating algorithms of exponential complexity. From an engineering point of view, the main hurdle in the construction of quantum devices is the mitigation of environmental noise that causes decoherence. The encoded quantum information becomes distorted due to decoherence, which is why error correcting protocols [3–5] are imperative for successful rectification of such distortions. However, error correcting schemes are generally very expensive to carry out. The idea of employing two dimensional systems that are intrinsically robust, such as systems exhibiting topological phases of matter [6–8], has led to a new paradigm in quantum computing known as *topological quantum computation* (TQC) [7, 9–12].

Such topologically ordered systems may be inhabited by special kinds of quasiparticles called *non-abelian anyons* [13–15], which may pave the way towards the realization of TQC. When non-abelian anyons are exchanged, their wave-function transforms according to representations of the *braid group*. This is in contrast to bosonic and fermionic wavefunctions, which transform rather trivially under the action of the permutation group. The anyonic quantum states are subject to topologically protected unitary transformations when braiding of their worldlines is performed. Such braiding of anyons serves as a possible way to implement topologically protected quantum circuits.

Notable anyon models include the Fibonacci and Ising anyons, which both belong to the family of $SU(2)_k$ models that are based on non-abelian Chern–Simons theory [10, 16–19]. All $SU(2)_k$ models are universal except for the cases $k = 2$ and $k = 4$, the former of which could potentially be realised by Majorana fermion zero mode quasiparticles [20].

Here we consider another class of anyon models known as *quantum doubles* [7, 21–24]. Specifically, we are focusing on the quantum double of the quaternion group $\mathcal{D}(\mathbb{Q}_8)$, inspired by its connection to the non-abelian vortex anyons in spinor Bose–Einstein condensates [25–29]. In particular, the unbroken high-temperature phase of an $F = 2$ spinor BEC may, through spontaneous symmetry breaking, collapse to the biaxial nematic phase [26, 30] characterised by the binary dihedral-4 group D_4^* . It is conceivable that this may further be broken down to its D_2^* subgroup, which is isomorphic to the quaternion group \mathbb{Q}_8 , considered here. The \mathbb{Q}_8 is a particularly small subgroup representing little residual symmetry, which should be beneficial for the prospect of its experimental realizability. The \mathbb{Q}_8 based quantum double model has previously been considered in [31] albeit in a different context.

In the present work, we are turning our focus to applications within quantum double TQC. We derive explicitly all pertinent information, such as particle content, fusion rules and braiding rules, for the non-abelian quantum double model $\mathcal{D}(\mathbb{Q}_8)$. We also design qubit structures (fusion trees), which are exploiting the full computational power of the model to optimize its utility. As a proof of principle demonstration, we then design and compile a quantum circuit architecture which allows us to factorize the number 15 into its prime number constituents using Shor’s algorithm [32]. Experimental realizations of Shor’s algorithm using other platforms have been studied in [33–41].

Quantum doubles based on discrete gauge groups emerge through the Higg’s mechanism by breaking particular symmetries of the initial Yang–Mills–Higg’s Lagrangian [21]. Due to the resulting discrete structure, braiding the anyons of the theory can only implement a finite set of unitary transformations, implying that the corresponding braid group is non-universal. To remedy this, measurement based fusion protocols [42, 43] could be implemented, allowing one to carry out phase gate

rotations of arbitrary angle. However, universality can only be achieved this way at the expense of sacrificing some fault-tolerance.

In the specific quantum circuit considered here, only one additional noisy gate is required, as all of the other gates can be implemented exactly within the anyon model by braiding alone. We employ a noise model based on stochastic unitary rotations to study its effect on the computational process. We also account for the error accumulation in the form of leakage from the computational subspace to its complement [43].

Quantum double of the quaternions:— Consider a condensate with spinor degrees of freedom governed by the (2+1)-dimensional non-abelian Yang–Mills–Higgs action

$$S = \int_{\mathbb{R}^{2+1}} d^3x (F_{\mu\nu}^a F_a^{\mu\nu} + (\mathcal{D}^\mu \phi)^\dagger \mathcal{D}^\mu \phi - V(\phi))$$

with $SU(2)$ symmetry, where $F_{\mu\nu}^a$ is the gauge curvature tensor, ϕ is the Higgs field, \mathcal{D} is the covariant derivative and V is the potential. We envisage the system cooling down and undergoing a symmetry breaking process to a subgroup $H \subset SU(2)$. Here we consider an ordered phase corresponding to $H = \mathbb{Q}_8$, which means that the pertinent excitations are determined by the homotopy theory of $\mathcal{D}(\mathbb{Q}_8)$. The group \mathbb{Q}_8 has eight elements and five conjugacy classes according to the partitioning $\mathbb{Q}_8 = \{\langle e \rangle, \langle \bar{e} \rangle, \langle i, \bar{i} \rangle, \langle j, \bar{j} \rangle, \langle k, \bar{k} \rangle\}$, where e is the identity and the bar denotes conjugation. The quantum double of a finite group is an algebraic construction that simultaneously involves the group and its Fourier dual [44]. The particle content of the quantum double is consequently defined by the irreducible representations of this algebra. In particular, the possible species of one type of particle, referred to as *fluxons*, are categorised according to the conjugacy classes of \mathbb{Q}_8 . Moreover, a second particle type, known as *chargeons*, also exist in the excitation spectrum, which inhabit the reciprocal space of \mathbb{R}^{2+1} and are defined by the irreducible representations of \mathbb{Q}_8 . Hence, the chargeons and fluxons are related by a generalised Fourier transform, which establishes a particle-vortex duality in the model. These two particle types can also coexist, thus forming composite objects known as *dyons*, under the condition that the chargeon group element commutes with the fluxon one, meaning that a *dyon*, denoted by $(C, \Gamma(Z_C))$, is specifically defined by a conjugacy class C and an irreducible representation of its centralizer $\Gamma(Z_C)$. The centralizers of each conjugacy class of \mathbb{Q}_8 are listed in Table I.

The group \mathbb{Q}_8 has four one-dimensional irreducible representations comprising one trivial Λ_0 and three non-trivial ones Λ_a ($a = 1, 2, 3$), in addition to one two-dimensional representation Λ_4 . The remaining centralizers have four one-dimensional irreducible representations given by one trivial, Π_0 , and three non-trivial ones Π_a ($a = 1, 2, 3$), which are simply permutations of one another. In total, $\mathcal{D}(\mathbb{Q}_8)$ has 22 particle species, comprising four pure fluxons

$$\bar{\mathbf{1}} = (\bar{e}, \Lambda_0) \quad \text{and} \quad \Phi_x = (C_x, \Pi_0), \quad (1)$$

where $x = i, j, k$, four pure chargeons

$$\rho_y = (e, \Lambda_y) \quad \text{and} \quad \Delta = (e, \Lambda_4), \quad (2)$$

where $y = 1, 2, 3$, and 14 composite dyons

$$\begin{aligned} \tilde{\Phi}_x &= (C_x, \Pi_2), \quad \bar{\rho}_y = (\bar{e}, \Lambda_y), \quad \bar{\Delta}_4 = (\bar{e}, \Lambda_4), \\ \Sigma_x &= (C_x, \Pi_1) \quad \text{and} \quad \tilde{\Sigma}_x = (C_x, \Pi_3). \end{aligned} \quad (3)$$

In addition to these particles, the pure vacuum sector is denoted by $\mathbf{1} = (e, \Lambda_0)$.

Fusion and braiding:— When two non-abelian anyons are fused their joint tensor representation branches into its irreducible orthogonal blocks, which correspond to the possible particle outcomes of the fusion. The particle types that emerge from the decomposition can be conveniently obtained using the so called Verlinde’s formula [45]

$$N_{AB\gamma}^{C\alpha\beta} = \sum_{D,\delta} \frac{S_{AD}^{\alpha\delta} S_{BD}^{\beta\delta} S_{CD}^{\gamma\delta}}{S_{eD}^{0\delta}}, \quad (4)$$

where A, B, C , and D denote conjugacy classes and $\alpha, \beta, \gamma, \delta$ label the centralizer irreducible representations. The explicit form of the modular S -matrix is provided in Supplemental Material [46]. The complete set of fusion rules are also listed in [46], and a subset of these

$$\begin{aligned} \Phi_x \otimes \Sigma_x &= \Delta \oplus \bar{\Delta}, \quad \Phi_x \otimes \Sigma_y = \Phi_z \oplus \tilde{\Phi}_z, \\ \Phi_x \otimes \Phi_x &= \mathbf{1} \oplus \bar{\mathbf{1}} \oplus \rho_x \oplus \bar{\rho}_x, \quad \Phi_x \otimes \Phi_y = \Phi_z \oplus \tilde{\Phi}_z, \\ \Sigma_x \otimes \Sigma_x &= \mathbf{1} \oplus \rho_x \oplus \bar{\rho}_y \oplus \bar{\rho}_z, \quad \Sigma_x \otimes \Sigma_y = \Sigma_z \oplus \tilde{\Sigma}_z, \end{aligned} \quad (5)$$

are required for defining our qubit Hilbert spaces.

Computational universality:— Several different anyon systems would qualify as a qubit architecture. For the purpose of demonstrating Shor’s algorithm it would make sense to design our TQC model such that its computational power is maximized. Since the specific proof of concept objective is to factor the number 15, it is tempting to base our Hilbert space on either Φ_x anyons or Σ_x anyons as both of these have four fusion outcomes, which means that only two such qudits would be required to represent the numbers from 1 to 16. However, by analyzing the topology of the resulting Hilbert space we find that universality of the model will become a major consideration.

TABLE I. Conjugacy classes C of \mathbb{Q}_8 and their corresponding centralizers $Z(C)$.

Conjugacy classes	Centralizers
$C_e = \langle e \rangle$	$Z(C_e) = \mathbb{Q}_8$
$C_{\bar{e}} = \langle \bar{e} \rangle$	$Z(C_{\bar{e}}) = \mathbb{Q}_8$
$C_i = \langle i, \bar{i} \rangle$	$Z(C_i) = \mathbb{Z}_4 = \{e, \bar{e}, i, \bar{i}\}$
$C_j = \langle j, \bar{j} \rangle$	$Z(C_j) = \mathbb{Z}_4 = \{e, \bar{e}, j, \bar{j}\}$
$C_k = \langle k, \bar{k} \rangle$	$Z(C_k) = \mathbb{Z}_4 = \{e, \bar{e}, k, \bar{k}\}$

Hopf-fibrations:— A four-level system transforms under $SU(4)$ and since this group is acting on a space with a total of $2 \cdot 4 = 8$ dimensions, the spherical surface that is being rotated is $8 - 1 = 7$ dimensional, that is, a 7-sphere S^7 . Further, it follows from Adam's theorem [47] that topological spheres of dimension 0, 1, 3, and 7 have the local structure of a fiber bundle, thus allowing us to decompose the manifold into its base space and a fiber such that $f : S^d \rightarrow S^n \times S^m$, where $d = n + m$. Such a map f is known as a Hopf fibration [48, 49] and when applied to the four-level system, it locally maps the manifold $f : S^7 \rightarrow S^4 \times S^3$, where S^4 is the base space and S^3 is the fiber. We can apply this map iteratively, which allows us to further decompose S^3 according to $f : S^3 \rightarrow S^2 \times S^1$, that is a regular 2-sphere and a circle, from which we can conclude that $S^7 \simeq S^4 \times S^2 \times S^1$, locally.

Since we consider these maps in the context of a quantum mechanical system, the S^1 degree of freedom pertains to the $U(1)$ gauge freedom, which is an experimentally unmeasurable symmetry of the amplitude. We may thus consider the projective Hilbert space, meaning that the effective topology of the manifold is $S^4 \times S^2$. Since computational universality entails that we must be able to generate a topologically dense cover over the manifold, we conclude that achieving this is much harder for a 4-level qudit than a 2-level qubit. Specifically, since qubits transform according to $SU(2)$, which rotates a $2 \cdot 2 - 1 = 3$ dimensional sphere S^3 , the effective topology is S^2 (the Bloch sphere) due to its local gauge fiber structure. Moreover, if we define a stereographic projection of S^2 onto \mathbb{R}^2 through the map $s : S^2 \rightarrow \mathbb{R}^2 \cup \infty$, we may conclude that in order to cover S^2 densely, we need to find a two-dimensional basis and make sure that we have elements of infinite order in the braid group. For a non-universal three-stranded braid group \mathbb{B}_3 , this can be achieved by supplementing the generator set with an irrational phase gate [17]. Note that for a two qubit system, which also has four levels, we have 6 anyons and thus a six-stranded braid group \mathbb{B}_6 , which has five generators, whereas a single 4-level qudit still only transforms under \mathbb{B}_3 with two generators. Consequently, it is much harder to span the complicated 4-level sphere in the qudit case due to the fewer number of generators and as a result, a less powerful braid group.

Circuit architecture:— We have arrived at the conclusion that basing our quantum circuit on anyons of the same species probably would make it difficult to implement the logic gates required in Shor's algorithm, since such systems have four levels. Moreover, calculating the braid group generators shows that the resulting group is either trivial or close to trivial. This leads to a conjecture that diversifying the qubit architecture might be a good approach for maximizing the computational power of the anyon model. Specifically, basing the individual qubits on either Σ_x or Φ_y type anyons (where $x, y = 1, 2, 3$), or a mixture of the two, yields a particularly strong model as the resulting braid group order is maximized and simul-

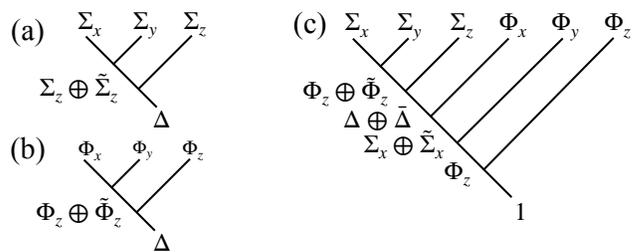


FIG. 1. (a) Qubit based on Σ anyons. (b) Qubit based on Φ anyons. (c) Two qubit anyon system based on Σ and Φ anyons.

taneously the number of non-computational basis states will be minimized, reducing the expected leakage into these states.

$\Sigma\Phi$ anyon computer:— To implement the circuit illustrated in Fig. S1 [46], four qubits are required. This can be achieved by defining three of the qubits as in Fig. 1 (a) and the last one as in Fig. 1 (b), where the controlled operations are implemented between qubits of the former kind with those of the latter. Any two qubit interaction in the circuit will thus be of the form presented in Fig. 1 (c) where all anyons are distinguishable. Note that all vertices are independent meaning that the total two qubit Hilbert space is $2^3 \cdot 1 = 8$ dimensional, which implies that we have four non-computational states in addition to the four computational ones defined by $\mathcal{H}_{\text{comp}} = \text{span}\{|\Phi_z, \Delta, \Sigma_x\rangle, |\tilde{\Phi}_z, \Delta, \Sigma_x\rangle, |\Phi_z, \Delta, \tilde{\Sigma}_x\rangle, |\tilde{\Phi}_z, \Delta, \tilde{\Sigma}_x\rangle\}$. The single qubit braid matrices σ_1 and σ_2 are

$$\begin{aligned} \sigma_1^{(\Phi_x \Phi_y)} &= \begin{pmatrix} -1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}, \quad \sigma_2^{(\Phi_x \Phi_y)} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\frac{3\pi}{4}} & e^{i\frac{5\pi}{4}} \\ e^{i\frac{5\pi}{4}} & e^{i\frac{3\pi}{4}} \end{pmatrix} \\ \sigma_1^{(\Sigma_x \Sigma_y)} &= \begin{pmatrix} e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{3\pi}{4}} \end{pmatrix}, \quad \sigma_2^{(\Sigma_x \Sigma_y)} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & -e^{i\frac{\pi}{2}} \end{pmatrix} \\ \sigma_1^{(\Sigma_x \Phi_y)} &= \begin{pmatrix} -e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \quad \sigma_2^{(\Sigma_x \Phi_y)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & e^{i\frac{\pi}{2}} \end{pmatrix}, \end{aligned}$$

which can be derived with the aid of the Supplemental Material [46]. The two qubit braids [46] can be obtained by means of graphical calculus given the information contained in the single qubit ones [10]. We proceed by making a few pertinent remarks. For a given i the braid matrices σ_i are equivalent up to a global phase factor, which implies that they have the same effective projective action. Remarkably, they also map projectively onto the Ising anyon braid matrices given by $SU(2)_2$ Chern–Simons theory. However, it is well known that the Ising anyon braids implement the Clifford group exactly, which is spanned by the Pauli matrices that form a representation of the quaternions. The 8×8 two qubit braid matrices in the six anyon encoding scheme are provided explicitly in [46], and similarly one can prove that these map projectively onto the two qubit Ising anyon braid matrices, but in the

eight anyon encoding scheme. Interestingly, many of the standard logic gates can be implemented exactly within this model, despite it being non-universal. For instance the Hadamard H and CNOT gates are $H = \sigma_2\sigma_1\sigma_2$, and $\text{CNOT} = \mathcal{P}\sigma_3^{-1}\sigma_4^{-1}\sigma_5^{-1}\mathcal{P}\sigma_3\sigma_4\mathcal{P}\sigma_3\sigma_1$, where \mathcal{P} is a projection operator that can be regarded as a map $\mathcal{P} : \mathcal{H}_{\text{full}} \rightarrow \mathcal{H}_{\text{comp}}$ projecting the full two qubit Hilbert space $\mathcal{H}_{\text{full}}$ onto the computational subspace $\mathcal{H}_{\text{comp}}$, thus containing all of the amplitude in $\mathcal{H}_{\text{comp}}$. We provide the exact compiled forms of the S -gate, the Pauli- X , the Pauli- Y , the Pauli- Z and the controlled-Pauli- Z in Supplemental Material [46]. Note that the CNOT is four dimensional while the two qubit braid matrices are eight dimensional. This means that amplitude will leak into the non-computational states when σ_3 is applied since this gate is the only one that couples the two subspaces. However, projection methods have been developed to manage the leakage, which, if successfully implemented, will have the effect of only braiding within the computational space. There also exist a subset of controlled two qubit braids known as weaves, which naturally cause very little leakage [50]. However, this weaving method is only useful when one has a vacuum sector in the fusion product and when the model is universal. Here we instead suggest to perform a projective measurement \mathcal{P} , after each σ_3 braid.

As noted, the Hadamard and the CNOT can be implemented without any compilation error, given that the leakage error correction is carried out for the CNOT, so the only gate required for the purposes of our demonstration that cannot be implemented by means of braiding alone is the controlled- $\pi/2$. To implement this gate we suggest using similar scheme as developed in [42], where a reservoir of ancillary qubits are used to set up product states $|\Psi\rangle|R_{\varphi/2}\rangle$, where $|R_{\varphi/2}\rangle$ is phase rotated by an angle $\varphi/2$, from which the phase $R_{\varphi/2}$ can be extracted. However, such a measurement protocol is susceptible to noise and therefore in the results presented in Fig. 2 we have applied stochastic unitary rotations to simulate the effect of conventional noise on the computation. The rotational angles of arbitrary elements $U \in \text{U}(4)$ are sampled from a normal distribution $N(0, \nu)$ with zero mean and variable standard deviation ν , which can be interpreted as the noise strength [17]. Assuming that this can be successfully achieved with $\varphi = \pi$, all of the logical operations required for the implementation of the Shor's algorithm quantum circuit are available.

Factorisation of 15:— The result of the simulation of Shor's algorithm corresponding to the instance $N = 15$ and $a = 11$, using our $\mathcal{D}(\mathbb{Q}_8)$ topological quantum computer simulator is shown in Fig. 2. Four different levels of noise corresponding to $\nu = 0, 0.1, 0.5, 1$ are applied to the controlled- $\pi/2$ gate, which could not be realized by

braiding alone. Figure 2 presents the probability distribution of the final state, showing two peaks with 50% amplitude each, representing the numbers 0 and 2, when no noise is applied (red curve). The trivial number 0 is a false solution but measuring 2 solves the problem as the

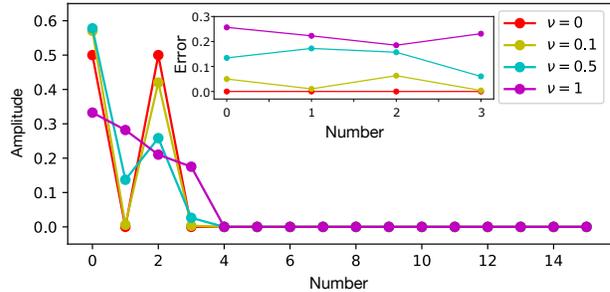


FIG. 2. Prime number factorisation of 15 using Shor's algorithm. Amplitudes of the resulting superposition when four different noise levels are applied. The inset represents the statistical error corresponding to the first four data points, 0, 1, 2, 3, with non-zero amplitude.

period can be computed as $r = \frac{2^2}{2} = 2$, which yields the prime factors $\gcd(a^{\frac{r}{2}} \pm 1, N) = \gcd(11^{\frac{2}{2}} \pm 1, 15) = 3, 5$, where $a = 11$ is chosen. Furthermore, the peaks become less distinct when the noise level is increased, eventually destroying the computation as the amplitude becomes too spread out. Each of the curves represent an average over 1000 realizations.

Conclusions:— We have presented a model of a topological quantum computer based on the quantum double of the quaternions $\mathcal{D}(\mathbb{Q}_8)$ inspired by its structural similarity to the superfluid phase that supports fractional vortices in spinor Bose–Einstein condensates as its fluxons [25]. All pertinent information of the quantum double such as particle content, fusion rules and braiding rules were derived and a qubit architecture was designed to facilitate topological quantum computation. We performed a technology demonstration of this anyon model by carrying out prime number factorisation using Shor's algorithm. The recipe of the quantum double based TQC is generic and can be applied to any laboratory superfluid having a stable ground state symmetry characterised by a discrete non-abelian gauge group, whose topological excitations include non-abelian vortex anyons.

ACKNOWLEDGMENTS

We are grateful to Joost Slingerland for generously sharing time to discuss algebraic aspects of the quantum double construction. This research was funded by the Australian Government through the Australian Research Council (ARC) Future Fellowship project FT180100020.

-
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
- [2] R. P. Feynman, Simulating Physics with Computers, *International Journal of Theoretical Physics* **21**, 467 (1982).
- [3] D. A. Lidar and T. A. Brun, *Quantum Error Correction* (Cambridge University Press, 2013).
- [4] D. Gottesman, Quantum computing: Efficient fault tolerance, *Nature (London)* **540**, 44 (2016).
- [5] D. Gottesman, *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, Vol. 68 (2010) pp. 13–58.
- [6] J. M. Kosterlitz and D. J. Thouless, Ordering, metastability and phase transitions in two-dimensional systems, *Journal of Physics C Solid State Physics* **6**, 1181 (1973).
- [7] A. Kitaev and C. Laumann, *Topological phases and quantum computation* (Oxford University Press, 2009).
- [8] X.-G. Wen, Colloquium: zoo of quantum-topological phases of matter, *Rev. Mod. Phys.* **89**, 041004 (2017).
- [9] J. K. Pachos, *Introduction to topological quantum computation* (Cambridge University Press, 2012).
- [10] B. Field and T. Simula, Introduction to topological quantum computation with non-Abelian anyons, *Quantum Sci. Technol.* **3**, 045004 (2018).
- [11] V. Lahtinen and J. K. Pachos, A short introduction to topological quantum computation, *SciPost Physics* **3** (2017).
- [12] E. C. Rowell and Z. Wang, Mathematics of topological quantum computing, *Bull. Amer. Math. Soc.* **55**, 183 (2018).
- [13] J. M. Leinaas and J. Myrheim, On the theory of identical particles, *Nuovo Cimento B Serie* **37**, 1 (1977).
- [14] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. D. Sarma, Non-Abelian anyons and topological quantum computation, *Rev. Mod. Phys.* **80**, 1083 (2008).
- [15] F. Wilczek, *Fractional statistics and anyon superconductivity*, Vol. 5 (World scientific, Singapore, 1990).
- [16] E. Witten, Quantum field theory and the Jones polynomial, *Communications in Mathematical Physics* **121**, 351 (1989).
- [17] E. G en etay Johansen and T. Simula, Fibonacci anyons versus Majorana fermions: A Monte Carlo approach to the compilation of braid circuits in $SU(2)_k$ anyon models, *PRX Quantum* **2**, 010334 (2021).
- [18] E. Fradkin, C. Nayak, A. Tsvelik, and F. Wilczek, A Chern-Simons effective field theory for the Pfaffian quantum Hall state, *Nuclear Physics B* **516**, 704 (1998).
- [19] G. V. Dunne, Course 3: Aspects of Chern-Simons Theory, in *Topological Aspects of Low Dimensional Systems*, Vol. 69, edited by A. Comtet, T. Jolicoeur, S. Ouvry, and F. David (1999) p. 177.
- [20] S. D. Sarma, M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, *npj Quantum Information* **1**, 1 (2015).
- [21] M. de Wild Propitius and F. A. Bais, *CRM-CAP Summer School on Particles and Fields '94* (Springer, 1995) pp. 353–439.
- [22] M. Gould, Quantum double finite-group algebras and their representations, *Bulletin of The Australian Mathematical Society* **48**, 275 (1993).
- [23] G. K. Brennen, M. Aguado, and J. I. Cirac, Simulations of quantum double models, *New Journal of Physics* **11**, 053009 (2009).
- [24] K. A. Dancer, P. S. Isaac, and J. Links, Representations of the quantum doubles of finite group algebras and spectral parameter dependent solutions of the Yang-Baxter equation, *Journal of Mathematical Physics* **47**, 103511 (2006).
- [25] T. Mawson, T. C. Petersen, J. K. Slingerland, and T. P. Simula, Braiding and Fusion of Non-Abelian Vortex Anyons, *Phys. Rev. Lett.* **123**, 140404 (2019).
- [26] Y. Kawaguchi and M. Ueda, Spinor Bose–Einstein condensates, *Physics Reports* **520**, 253 (2012).
- [27] Y. Kawaguchi, M. Nitta, and M. Ueda, Knots in a Spinor Bose–Einstein Condensate, *Phys. Rev. Lett.* **100**, 180403 (2008).
- [28] Y. Kawaguchi, M. Kobayashi, M. Nitta, and M. Ueda, Topological Excitations in Spinor Bose–Einstein Condensates, *Progress of Theoretical Physics Supplement* **186**, 455 (2010).
- [29] T. Simula, *Quantised Vortices; A handbook of topological excitations* (Morgan & Claypool Publishers, 2019).
- [30] D. M. Stamper-Kurn and M. Ueda, Spinor Bose gases: Symmetries, magnetism, and quantum dynamics, *Rev. Mod. Phys.* **85**, 1191 (2013).
- [31] F. A. Bais and J. C. Romers, The modular S-matrix as order parameter for topological phase transitions, *New Journal of Physics* **14**, 035024 (2012).
- [32] P. W. Shor, Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Sci. Statist. Comput.* **26**, 1484 (1997).
- [33] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance, *Nature (London)* **414**, 883 (2001).
- [34] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Demonstration of a Compiled Version of Shor’s Quantum Factoring Algorithm Using Photonic Qubits, *Phys. Rev. Lett.* **99**, 250504 (2007).
- [35] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Experimental Demonstration of a Compiled Version of Shor’s Algorithm with Quantum Entanglement, *Phys. Rev. Lett.* **99**, 250505 (2007).
- [36] A. Politi, J. C. F. Matthews, and J. L. O’Brien, Shor’s Quantum Factoring Algorithm on a Photonic Chip, *Science* **325**, 1221 (2009).
- [37] E. Mart ın-L opez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O’Brien, Experimental realization of Shor’s quantum factoring algorithm using qubit recycling, *Nature Photonics* **6**, 773 (2012).
- [38] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O’Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and J. M. Martinis, Computing prime factors with a Josephson phase qubit quantum processor, *Nature Physics* **8**, 719 (2012).
- [39] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, Realization of a scalable Shor algorithm, *Sci-*

- ence **351**, 1068 (2016).
- [40] M. Amico, Z. H. Saleem, and M. Kumph, Experimental study of Shor’s factoring algorithm using the IBM Q Experience, *Phys. Rev. A* **100**, 012305 (2019).
- [41] Z.-C. Duan, J.-P. Li, J. Qin, Y. Yu, Y.-H. Huo, S. Höfling, C.-Y. Lu, N.-L. Liu, K. Chen, and J.-W. Pan, Proof-of-principle demonstration of compiled Shor’s algorithm using a quantum dot single-photon source, *Optics Express* **28**, 18917 (2020).
- [42] C. Levaillant, B. Bauer, M. Freedman, Z. Wang, and P. Bonderson, Universal gates via fusion and measurement operations on $SU(2)_4$ anyons, *Phys. Rev. A* **92**, 012301 (2015).
- [43] C. Mochon, Anyons from nonsolvable finite groups are sufficient for universal quantum computation, *Phys. Rev. A* **67**, 022315 (2003).
- [44] T. H. Koornwinder, B. J. Schroers, J. K. Slingerland, and F. A. Bais, Fourier transform and the Verlinde formula for the quantum double of a finite group, *Journal of Physics A Mathematical General* **32**, 8539 (1999).
- [45] E. Verlinde, Fusion rules and modular transformations in 2D conformal field theory, *Nuclear Physics B* **300**, 360 (1988).
- [46] See Supplemental Material at [URL will be inserted by publisher] for details of the Shor’s algorithm and the structure of the quantum double of the quaternion group.
- [47] J. F. Adams, On the non-existence of elements of Hopf invariant one, *Ann. of Math* **72**, 20 (1960).
- [48] D. W. Lyons, An elementary introduction to the Hopf fibration, *Mathematics Magazine* **76**, 87 (2003).
- [49] R. Mosseri and P. Riberto, Entanglement and Hilbert space geometry for systems with a few qubits, *Mathematical Structures in Computer Science* **17**, 1117–1132 (2007).
- [50] L. Hormozi, G. Zikos, N. E. Bonesteel, and S. H. Simon, Topological quantum compiling, *Phys. Rev. B* **75**, 165310 (2007).
- [51] K. Rykhlinskaya and S. Fritzsche, Generation of Clebsch Gordan coefficients for the point and double groups, *Computer Physics Communications* **174**, 903 (2006).

Appendix A: Shor’s algorithm

Shor’s algorithm consists of two main parts, a quantum step followed by a classical step. The algorithm is initiated by setting up disentangled product state of two registers $|\psi\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$ of $n = 2 \cdot \lceil \log_2(N) \rceil$ qubits, where the brackets denote the *ceil* function that is rounding up the number to the closest integer and N is the number being factorised. The factor two comes from the fact that two registers are required, one in which the integers $1, 2, \dots, N$ are encoded and one which serves as a target when the controlled gates in the modular exponentiation function (MEF) is applied. The first register is then set up in an equal weight superposition by applying the Hadamard gate H to all of the n qubits in the register which results in a state

$$|\Psi\rangle = H^{\otimes n} \otimes I^{\otimes n} |\psi\rangle = \frac{1}{2^{n/2}} \left[\sum_{m=0}^{2^n-1} |m\rangle \right] \otimes |0\rangle^{\otimes n}. \quad (\text{A1})$$

Next, the quantum period finding subroutine is carried out on the full register which finds the period of the function $f(x) = a^x \pmod{N}$, where a is an integer in the interval $1 < a < N$. This part truly is at the heart of Shor’s algorithm as such a problem is inherently exponential in nature and cannot be solved efficiently by means of any classical analog. Quantum period finding can be further decomposed into two parts. First, the MEF is applied to the lower register resulting in

$$\text{MEF} : |\Psi_{\text{MEF}}\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |a^x \pmod{N}\rangle, \quad (\text{A2})$$

where after the lower register is measured, thus projecting the full Hilbert space onto a subspace spanned by the states $|x'\rangle$ resulting in the same number $a^x \pmod{N}$. The last step before the final measurement is to apply the inverse quantum Fourier transform QFT^\dagger to the top register

$$\text{QFT}^\dagger : |\tilde{\Psi}_{\text{MEF}}\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \sum_{x'} e^{-i2\pi \frac{yx'}{2^n}} |x'\rangle, \quad (\text{A3})$$

which has the effect of destructively interfering the false solutions and constructively interfering the true solutions, resulting in sharp amplitude peaks pertaining to the states that solve the problem. One of these solution candidates is measured in the very last step. Suppose that a state $|m\rangle$ was measured. Then the rest of the algorithm can be completed classically as we only have to compute $\text{gcd}(a^{\frac{m}{2}} \pm 1, N)$, where the period r can be obtained from $m = j \frac{2^n}{r}$, where j is the smallest integer such that the equation is satisfied. However, in this work we are merely interested in a proof of concept demonstration of factorizing the number 15 and if we pick $a = 11$, the circuit can be reduced so that only two qubits are required in each register, instead of four. This is due to the fact that the MEF will always return only two states $|1\rangle$ and $|11\rangle$ for this particular instance of a . In Fig. 3 (a) the circuit is represented in its higher level modular form and in Fig. 3 (b) the different oracles are broken down into the elementary gates.

Appendix B: Structure of the $\mathcal{D}(\mathbb{Q}_8)$ anyon model

Here we outline the structure of the $\mathcal{D}(\mathbb{Q}_8)$ anyon model which is based on the quaternion group \mathbb{Q}_8 .

1. Cayley table of the quaternion group \mathbb{Q}_8

Table II shows the Cayley table for the quaternion group \mathbb{Q}_8 . The colors correspond to the five conjugacy classes of this group with eight group elements.

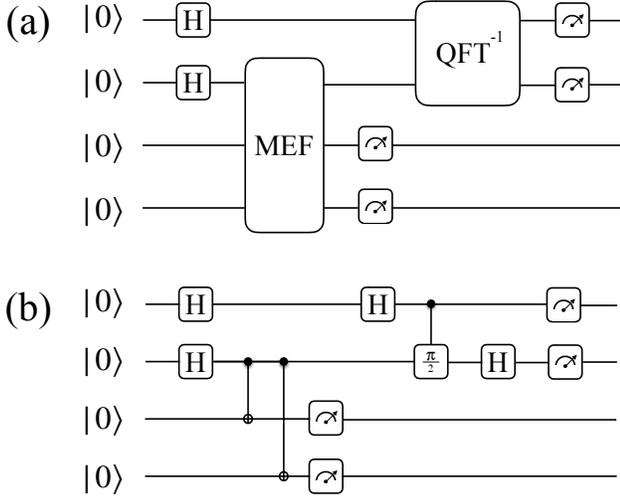


FIG. 3. (a) Modular circuit for Shor's algorithm for $N = 15$ and $a = 11$. (b) Same circuit as in (a) but with the subroutines decomposed into elementary gate operations.

TABLE II. Cayley table of the quaternion group \mathbb{Q}_8 .

\times	e	\bar{e}	i	\bar{i}	j	\bar{j}	k	\bar{k}
e	e	\bar{e}	i	\bar{i}	j	\bar{j}	k	\bar{k}
\bar{e}	\bar{e}	e	\bar{i}	i	\bar{j}	j	\bar{k}	k
i	i	\bar{i}	\bar{e}	e	k	\bar{k}	\bar{j}	j
\bar{i}	\bar{i}	i	e	\bar{e}	k	k	j	\bar{j}
j	j	\bar{j}	\bar{k}	k	\bar{e}	e	i	\bar{i}
\bar{j}	\bar{j}	j	k	\bar{k}	e	\bar{e}	\bar{i}	i
k	k	\bar{k}	j	\bar{j}	\bar{i}	i	\bar{e}	e
\bar{k}	\bar{k}	k	\bar{j}	j	i	\bar{i}	e	\bar{e}

2. Fusion rules

The complete set of fusion rules [31] are presented below for the sake of completeness.

Chargeons only:

$$\begin{aligned} \rho_x \otimes \rho_x &= \mathbb{1}, & \rho_x \otimes \rho_y &= \rho_z \\ \rho_x \otimes \Delta &= \Delta, & \Delta \otimes \Delta &= \mathbb{1} \oplus \rho_x \oplus \rho_y \oplus \rho_z \end{aligned} \quad (\text{B1})$$

Fluxons only:

$$\begin{aligned} \bar{\mathbb{1}} \otimes \bar{\mathbb{1}} &= \mathbb{1}, & \Phi_x \otimes \Phi_x &= \mathbb{1} \oplus \bar{\mathbb{1}} \oplus \rho_x \oplus \bar{\rho}_x \\ \Phi_x \otimes \Phi_y &= \Phi_z \oplus \tilde{\Phi}_z, & \bar{\mathbb{1}} \otimes \Phi_x &= \Phi_x \end{aligned} \quad (\text{B2})$$

Dyons only:

$$\begin{aligned} \tilde{\Phi}_x \otimes \tilde{\Phi}_x &= \mathbb{1} \oplus \bar{\mathbb{1}} \oplus \rho_x \oplus \bar{\rho}_x, & \tilde{\Phi}_x \otimes \bar{\rho}_x &= \tilde{\Phi}_x \\ \tilde{\Phi}_x \otimes \bar{\rho}_y &= \Phi_x, & \bar{\rho}_x \otimes \bar{\Delta} &= \bar{\Delta} \\ \bar{\Delta} \otimes \tilde{\Phi}_x &= \Sigma_x \oplus \tilde{\Sigma}_x, & \bar{\Delta} \otimes \Sigma_x &= \Phi_x \oplus \tilde{\Phi}_x \\ \Sigma_x \otimes \Sigma_x &= \mathbb{1} \oplus \rho_x \oplus \bar{\rho}_y \oplus \bar{\rho}_z, & \tilde{\Sigma}_x \otimes \tilde{\Sigma}_x &= \bar{\mathbb{1}} \oplus \bar{\rho}_x \oplus \rho_y \oplus \rho_z \\ \Sigma_x \otimes \Sigma_y &= \Phi_z \oplus \tilde{\Phi}_z \end{aligned} \quad (\text{B3})$$

Chargeons, fluxons and dyons:

$$\begin{aligned} \rho_x \otimes \Phi_x &= \Phi_x, & \rho_x \otimes \Phi_y &= \tilde{\Phi}_y \\ \Delta \otimes \Phi_x &= \Sigma_x \oplus \tilde{\Sigma}_x, & \tilde{\Phi}_x \otimes \bar{\mathbb{1}} &= \tilde{\Phi}_x, \\ \bar{\mathbb{1}} \otimes \Sigma_x &= \tilde{\Sigma}_x, & \bar{\mathbb{1}} \otimes \tilde{\Sigma}_x &= \Sigma_x \\ \rho_x \otimes \Sigma_x &= \Sigma_x, & \rho_y \otimes \Sigma_x &= \tilde{\Sigma}_x \\ \bar{\rho}_x \otimes \Sigma_x &= \tilde{\Sigma}_x, & \Delta \otimes \Sigma_x &= \Phi_x \oplus \tilde{\Phi}_x \\ \Delta \otimes \tilde{\Sigma}_x &= \Phi_x \oplus \tilde{\Phi}_x, & \Delta \otimes \bar{\mathbb{1}} &= \bar{\Delta} \\ \Phi_x \otimes \Sigma_x &= \Delta \oplus \bar{\Delta}, & \Phi_x \otimes \Sigma_y &= \Phi_z \oplus \tilde{\Phi}_z, \\ \Phi_x \otimes \Phi_x &= \mathbb{1} \oplus \bar{\mathbb{1}} \oplus \rho_x \oplus \bar{\rho}_x, & \Phi_x \otimes \Phi_y &= \Phi_z \oplus \tilde{\Phi}_z, \\ \Sigma_x \otimes \Sigma_x &= \mathbb{1} \oplus \rho_x \oplus \bar{\rho}_y \oplus \bar{\rho}_z, & \Sigma_x \otimes \Sigma_y &= \Sigma_z \oplus \tilde{\Sigma}_z \end{aligned} \quad (\text{B4})$$

3. Two qubit braid matrices

The two qubit braid matrices presented here can be computed with the aid of graphical calculus, given that the single qubit braid matrices are known. For a thorough discussion we refer the reader to [10].

$$\sigma_1^2(X, Y) = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b \end{pmatrix} \quad (\text{B5})$$

$$\sigma_2^2(X, Y) = \frac{1}{\sqrt{2}} \begin{pmatrix} c & 0 & d & 0 & 0 & 0 & 0 & 0 \\ 0 & c & 0 & d & 0 & 0 & 0 & 0 \\ d & 0 & c & 0 & 0 & 0 & 0 & 0 \\ 0 & d & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & c & 0 & d \\ 0 & 0 & 0 & 0 & d & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & d & 0 & c \end{pmatrix} \quad (\text{B6})$$

TABLE III. Values of the variables a, b, c, d and e when braiding X and Y .

(X, Y)	Φ_x	Σ_x
Φ_y	$a = -1, \quad b = e^{i\frac{\pi}{2}}, \quad c = e^{i\frac{3\pi}{4}}, \quad d = e^{i\frac{5\pi}{4}}, \quad e = e^{i\frac{3\pi}{4}}$	$a = -e^{-i\frac{\pi}{4}}, \quad b = e^{i\frac{\pi}{4}}, \quad c = 1, \quad d = -1, \quad e = e^{i\frac{\pi}{2}}$
Σ_y	$a = -e^{-i\frac{\pi}{4}}, \quad b = e^{i\frac{\pi}{4}}, \quad c = 1, \quad d = -1, \quad e = e^{i\frac{\pi}{2}}$	$a = e^{-i\frac{\pi}{4}}, \quad b = e^{-i\frac{3\pi}{4}}, \quad c = -1, \quad d = 1, \quad e = 1$

$$\sigma_3^2(X, Y) = \frac{1}{\sqrt{2}} \begin{pmatrix} a & 0 & 0 & 0 & b & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & b \\ b & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & a & 0 & 0 & b & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & a \end{pmatrix} \quad (\text{B7})$$

$$\sigma_4^2(X, Y) = \frac{1}{\sqrt{2}} \begin{pmatrix} c & d & 0 & 0 & 0 & 0 & 0 & 0 \\ d & c & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 & 0 & 0 \\ 0 & 0 & d & e & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c & d & 0 & 0 \\ 0 & 0 & 0 & 0 & d & e & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & c & d \\ 0 & 0 & 0 & 0 & 0 & 0 & d & e \end{pmatrix} \quad (\text{B8})$$

$$\sigma_5^2(X, Y) = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b \end{pmatrix} \quad (\text{B9})$$

4. Exactly realizable quantum gates

We list below explicit forms, in terms of the elementary braid matrices, for a set of gates that can be realised exactly by braiding alone within the $\mathcal{D}(\mathbb{Q}_8)$.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \sigma_1^{-1} \quad (\text{B10})$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \sigma_1 \sigma_2 \sigma_1 \quad (\text{B11})$$

$$\text{Pauli} - X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_2 \sigma_2 \quad (\text{B12})$$

$$\text{Pauli} - Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_1 \sigma_1 \sigma_2^{-1} \sigma_2^{-1} \quad (\text{B13})$$

$$\text{Pauli} - Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_1 \sigma_1 \quad (\text{B14})$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \mathcal{P} \sigma_3^{-1} \sigma_4^{-1} \sigma_5^{-1} \mathcal{P} \sigma_3 \sigma_4 \mathcal{P} \sigma_3 \sigma_1 \quad (\text{B15})$$

$$\text{controlled} - Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \sigma_1 \mathcal{P} \sigma_3^{-1} \sigma_5. \quad (\text{B16})$$

The two qubit controlled gates need to be accompanied by a projective measurement \mathcal{P} that projects the quantum state onto the computable subspace to avoid leakage to non-computable subspace.

5. S and T matrices

The modular S and T-matrices span the group $\text{SL}(2, \mathbb{C})$ [21]. The S-matrix can be regarded as the equivalent of a character table in the context of quantum double structure and can be computed as

$$S_{\Gamma\Lambda}^{AB} = \frac{1}{H} \sum_{h_A \in C^A, h_B \in C^B} \text{Tr}(\Gamma(g_A^{-1} h_B g_A))^* \text{Tr}(\Lambda(g_B^{-1} h_A g_B))^*, \quad (\text{B17})$$

where the sum is carried out over all elements belonging to the conjugacy classes C^A and C^B such that $[h_A, h_B] = e$ is satisfied, and Γ and Λ are the centralizer irreducible representations. The S-matrix is provided explicitly in [31] and is provided for the sake of completeness in Table IV. The T-matrix contains information about the topological spins of the particles and can be computed as

$$T_{\Gamma\Lambda}^{AB} = \delta_{\Gamma,\Lambda} \delta^{A,B} e^{i2\pi s_{\Gamma}^A} = \frac{1}{d_{\Gamma}} \text{Tr}(\Gamma(h^A)), \quad (\text{B18})$$

where s is the topological spin and d is the quantum dimension.

TABLE IV. The modular S matrix of $\mathcal{D}(\mathbb{Q}_8)$. Here $\epsilon_{ij} = 2\delta_{ij} - 1$ and δ_{ij} is the Kronecker delta.

S	$\mathbb{1}$	$\bar{\mathbb{1}}$	ρ_j	$\bar{\rho}_j$	Δ	$\bar{\Delta}$	Φ_j	$\bar{\Phi}_j$	Σ_j	$\bar{\Sigma}_j$
$\mathbb{1}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
$\bar{\mathbb{1}}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$
ρ_i	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$
$\bar{\rho}_i$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}\epsilon_{ij}$	$-\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$
Δ	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{2}$	0	0	0	0
$\bar{\Delta}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
Φ_i	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}\epsilon_{ij}$	$-\frac{1}{4}\epsilon_{ij}$	0	0	$\frac{1}{2}\delta_{ij}$	$-\frac{1}{2}\delta_{ij}$	0	0
$\bar{\Phi}_i$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}\epsilon_{ij}$	$-\frac{1}{4}\epsilon_{ij}$	0	0	$-\frac{1}{4}\delta_{ij}$	$\frac{1}{4}\delta_{ij}$	0	0
Σ_i	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$	0	0	0	0	$\frac{1}{4}\delta_{ij}$	$-\frac{1}{4}\delta_{ij}$
$\bar{\Sigma}_i$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}\epsilon_{ij}$	$\frac{1}{4}\epsilon_{ij}$	0	0	0	0	$-\frac{1}{4}\delta_{ij}$	$\frac{1}{4}\delta_{ij}$

6. F and R symbols

In this section we provide the background material required to work out the braid matrices. The single qubit braid matrices are given by $\sigma_1 = R$ and $\sigma_2 = F^{-1}RF$, where R and F correspond to the anyon interchange and change of fusion basis, respectively, and are given by [21]

$$R_{j_i j_j}^{j_k} = \sum_{m_i, m_j} \sum_{m_q, m_p} \sigma_{m_i, m_q}^{m_j, m_p} \circ \mathcal{R}_{j_i, j_j}^{(m_i, m_q), (m_j, m_p)} \quad (\text{B19})$$

and

$$[F_{j_i, j_j, j_k}^{j_q}]_{j_l}^{j_p} = \sum_{m_i, m_j, m_k, m_q, m_p} \begin{bmatrix} j_i & j_j & j_l \\ m_i & m_j & m_l \end{bmatrix} \begin{bmatrix} j_l & j_k & j_q \\ m_l & m_k & m_q \end{bmatrix} \begin{bmatrix} j_q & j_p & j_i \\ m_q & m_p & m_i \end{bmatrix} \begin{bmatrix} j_p & j_j & j_k \\ m_p & m_j & m_k \end{bmatrix}, \quad (\text{B20})$$

where j_i and m_i are the topological spins and magnetic moments, respectively, and the brackets denote the quantum double Clebsch–Gordan coefficients which are given by Eqs. (B23)–(B25). The $\sigma_{m_i, m_q}^{m_j, m_p}$ are elements of the permutation operator σ which is equivalent to a decoupling followed by a recoupling where the anyons are swapped, i.e.

$$\sigma_{m_i, m_q}^{m_j, m_p} = \begin{bmatrix} j_i & j_j & j_k \\ m_i & m_j & m_k \end{bmatrix} \begin{bmatrix} j_k & j_j & j_i \\ m_k & m_p & m_q \end{bmatrix} \quad (\text{B21})$$

and the $\mathcal{R}_{j_i, j_j}^{(m_i, m_q), (m_j, m_p)}$ elements are given by

$$\mathcal{R}_{j_i, j_j}^{(m_i, m_q), (m_j, m_p)} = \sum_h \sum_g \Lambda_{m_i, m_q}^{j_i}(P_g e) \otimes \Lambda_{m_j, m_p}^{j_j}(P_h g), \quad (\text{B22})$$

where $\Lambda_{m_i, m_q}^{j_i}$ are the representations corresponding to the topological charge j_i mapping the quantum double element $P_h g$ (a gauge transformation g followed by a flux

measurement P_h) to a matrix implementing the quantum double action. The Clebsch–Gordan coefficients can be derived analytically by unpacking the representations via the projection operators in the representation theory of the quantum double. In doing so, one finds that the coefficients must satisfy

$$\sum_n \begin{bmatrix} j_i & j_j & j_l \\ m_i & m_j & m_l \end{bmatrix}_n^* \begin{bmatrix} j_q & j_p & j_k \\ m_q & m_p & m_k \end{bmatrix}_n = \frac{d_{j_k}}{|H|} \sum_{h, g} \Lambda_{m_k, m_l}^{j_k}(P_h g)^* \sum_{h' h''=h} \Lambda_{m_i, m_q}^{j_i}(P_{h'} g) \Lambda_{m_j, m_p}^{j_j}(P_{h''} g), \quad (\text{B23})$$

where n is the multiplicity of the corresponding irreducible representation. In the $\mathcal{D}(\mathbb{Q}_8)$ anyon model all fusion outcomes have unit multiplicity meaning that we can solve Eq. (B23) analytically since there is only one term on the left hand side of the equation. Setting $i = q$, $j = p$ and $k = l$ we find the solution corresponding to the diagonal elements of the representations

$$\begin{bmatrix} j_i & j_j & j_k \\ m_i & m_j & m_k \end{bmatrix} = \sqrt{\frac{d_{j_k}}{|H|} \sum_{h, g} \Lambda_{m_k, m_k}^{j_k}(P_h g)^* \sum_{h' h''=h} \Lambda_{m_i, m_i}^{j_i}(P_{h'} g) \Lambda_{m_j, m_j}^{j_j}(P_{h''} g)}. \quad (\text{B24})$$

Finally, we can divide Eq. (B23) by the solution given by Eq. (B24) to obtain the full solution

$$\begin{bmatrix} j_q & j_p & j_k \\ m_q & m_p & m_k \end{bmatrix}_{(m_i, m_j, m_k)} = \frac{\sum_{h, g} \Lambda_{m_k, m_l}^{j_k}(P_h g)^* \sum_{h' h''=h} \Lambda_{m_i, m_q}^{j_i}(P_{h'} g) \Lambda_{m_j, m_p}^{j_j}(P_{h''} g)}{\sqrt{\frac{d_{j_k}}{|H|} \sum_{h, g} \Lambda_{m_k, m_k}^{j_k}(P_h g)^* \sum_{h' h''=h} \Lambda_{m_i, m_i}^{j_i}(P_{h'} g) \Lambda_{m_j, m_j}^{j_j}(P_{h''} g)}}. \quad (\text{B25})$$

This result is similar to that obtained with a different method in [51] for regular finite groups. One can recover

Eq. (B25) from their derivation by considering the quantum double of the discrete group.