# New Journal of Physics 

# Topological qubit design and leakage 

R Ainsworth ${ }^{1}$ and J K Slingerland ${ }^{1,2}$<br>${ }^{1}$ Department of Mathematical Physics, National University of Ireland Maynooth, Co. Kildare, Ireland<br>${ }^{2}$ Dublin Institute for Advanced Studies, School for Theoretical Physics, 10 Burlington Road, Dublin, Ireland<br>E-mail: robert.ainsworth@ nuim.ie and joost@thphys.nuim.ie

New Journal of Physics 13 (2011) 065030 (16pp)
Received 24 February 2011
Published 30 June 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/6/065030


#### Abstract

We examine how best to design qubits for use in topological quantum computation. These qubits are topological Hilbert spaces associated with small groups of anyons. Operations are performed on these by exchanging the anyons. One might argue that in order to have as many simple single-qubit operations as possible, the number of anyons per group should be maximized. However, we show that there is a maximal number of particles per qubit, namely 4 , and more generally a maximal number of particles for qudits of dimension $d$. We also look at the possibility of having topological qubits for which one can perform two-qubit gates without leakage into non-computational states. It turns out that the requirement that all two-qubit gates are leakage free is very restrictive and this property can only be realized for two-qubit systems related to Ising-like anyon models, which do not allow for universal quantum computation by braiding. Our results follow directly from the representation theory of braid groups, which implies that they are valid for all anyon models. We also make some remarks about generalizations to other exchange groups.


## Contents

1. Introduction ..... 2
1.1. Standard topological quantum computation (TQC) scheme and leakage ..... 3
2. Design of a single qudit ..... 4
2.1. Qubits ..... 5
2.2. Qudits with $d>2$ ..... 7
3. Two-qudit gates and leakage ..... 11
3.1. Two qubits ..... 12
3.2. Qutrits and qubit-qutrit combinations ..... 13
3.3. Leakage-free gates in a system with leakage ..... 14
4. Summary and discussion ..... 14
Acknowledgment ..... 15
References ..... 15

## 1. Introduction

Topological quantum computation (TQC) [1, 2] has been with us for well over a decade now and, despite the great difficulty in producing a first experimental realization of the idea, it may represent our best hope for the future of quantum computing because of its inherent fault tolerance and potential for scalability.

Concrete proposals for TQC center around two-dimensional (2D) systems with excitations that have non-trivial behavior under exchanges, non-Abelian anyons. Great theoretical and experimental effort has been made to understand the various systems in which anyons are thought, or hoped, to occur, and a good deal is also known about the types of computations that could be performed if the anyons were given to us and we were allowed to exchange them at will in any way we like. Perhaps most importantly, it is known for a large class of anyon models that they provide for universal quantum computation by exchanges [3, 4]. A sort of standard paradigm for the construction of a topological quantum computer has also emerged and versions of this occur in papers such as [5-7]. The idea is to use the topological quantum numbers of small groups of anyons as qubits and to perform operations on these qubits by exchanging the anyons, both within the groups that form the qubits and, for multi-qubit gates, between groups. We will go into a little more detail about this in section 1.1. The importance of such a paradigm is that it allows one to make direct contact with the circuit model of quantum computation and it enables algorithmic questions to be tackled independently of the details of experimental implementation, at least initially.

The aim of this paper is to study some constraints on the TQC paradigm that exist for any anyon model. These arise when one asks some very basic questions, such as 'What is the optimal number of anyons with which to form a qubit?' and 'To what extent can the problem of leakage be avoided?'. Leakage is the issue that, because the full Hilbert space of a multianyon system does not have a tensor product structure, a subspace of this Hilbert space must be chosen if one wants to deal with qubits, and on exchanging the anyons, some of the topological amplitude may 'leak' into the non-computational states. While these questions must certainly have been considered by the authors of earlier papers, we feel that they have so far not really been brought to the forefront. Nevertheless, some interesting general results can be obtained


Figure 1. (a) A qudit composed of three anyons, where $a$ labels the topological charge of each anyon. The information in the qudit is stored using the topological charge $b$ of the first two. All three together have a fixed topological charge $c$. (b) A qudit composed of four anyons of topological charge $a$. The information is stored using the topological charge $b$ of the first two. The total topological charge is trivial (1) and the last two automatically have the topological charge $\hat{b}$, which can fuse to 1 with $b$.
that are valid for all types of anyon. For example, qubits with groups of five or more anyons are not possible unless one allows for leakage in single-qubit gates. Similar constraints apply to qudits, the $d$-dimensional analogues of qubits. It also turns out that very few topological two-qubit systems allow for totally leakage-free braiding of the anyons, and those that do will not allow for universal braiding. Again, similar results can be obtained for some systems with higher-dimensional qudits.

The structure of this paper is as follows. We start with a brief overview of the standard paradigm for TQC and the leakage problem that is inherent to it. Then we focus on single qubits and qudits, and we show that if exchanges within the groups of anyons forming the qudits are to be leakage free, the number of particles that form the qudits is limited. Our arguments actually show that similar constraints on the number of particles per qudit should hold for any computational scheme based on exchanging localized objects; for example, for closed string excitations in 3D. We then consider two-qubit and two-qudit gates and we show that very few situations exist in which all exchanges of the anyons and hence all conceivable two-qudit gates are leakage free, at least for low-dimensional qudits. Moreover, the exceptions we have identified do not allow for universal quantum computation by braiding. Finally, we make some general remarks about leakage-free gates in systems that do have leaking gates.

### 1.1. Standard topological quantum computation (TQC) scheme and leakage

In the 'standard model' of a topological computer, our system is composed of a collection of anyons, described by an anyon model or topological field theory (see e.g. [8-11] for reasonably 'physicist friendly' introductions to anyon models). The Hilbert space of the entire system is the fusion space of the anyons, which has a basis of states labeled by the different ways in which all the anyons can fuse together. This space typically does not have a natural tensor product structure, so we introduce this by hand; we associate qudits with small groups of anyons. Usually one takes these groups to consist of three or four anyons, as indicated in figure 1.

The overall topological charge of each such group of anyons is usually fixed, and is conserved by exchange processes involving only the anyons in a single qudit. For four-anyon qudits, one may choose this topological charge to be the trivial, or vacuum charge, which is
convenient since it means that the qubit as a whole can be exchanged without any non-trivial effect on the system's state. The quantum number that stores the information in the qudit is the topological charge of the leftmost two anyons in the qudit. The computational Hilbert space is taken to be the tensor product of these qudit spaces and the topological quantum computer is then effectively described by the quantum circuit model, with the important addition that there is a natural set of gates generating all possible quantum operations, namely the elementary exchanges of the anyons in the qudits.

The computational Hilbert space, however, is usually only a subspace of the full topological Hilbert space of the system. While braiding anyons from the same qudit does not change the overall topological charge of the qudit, braiding anyons from different qudits around each other may change the overall topological charge of the qudits and this will result in some of the information 'leaking' out of the computational Hilbert space. Moreover, if such leakage has happened at some stage in a computation, the amplitude in the non-computational subspace may couple back into the computational subspace later on.

In all models of this sort proposed so far (see e.g. [5-7]), leakage is unavoidable and it is of great importance to find gates that leak as little as possible and, in general, to reduce the amount of leakage in a system to a minimum (see [12] for work specifically focused on this). Clearly, in systems where exchange processes allow for an approximation of arbitrary unitaries, it is always possible to avoid leakage to arbitrary accuracy, but avoiding leakage is nevertheless a nuisance that can cause severe overhead. In this paper, we will examine under which circumstances one may have models where all one-qudit and/or all multi-qudit braiding gates are entirely leakage free. Such models would obviously be extremely desirable as they would make computations simpler and more accurate. However, it turns out that excluding leakage is a very severe restriction on the allowable models.

## 2. Design of a single qudit

We would like to find the optimal number of anyons from which to construct a single qudit. Obviously, what is optimal depends on the circumstances; for example, if it is experimentally hard to control multiple anyons, then the optimal number may be the minimal number of anyons that actually can provide a qudit-this would be two anyons, with the qudit of information stored in the fusion channel of the two anyons. However, using two-anyon qudits has a clear disadvantage, which is that in a system with two-anyon qudits, no non-trivial gates can be performed by braiding anyons within a single qudit. As a result, leakage enters even at the level of single-qudit gates-in fact, it may be difficult to perform many exact single-qubit gates, because they would have to be built from special braidings of anyons that are part of different qudits. Qudits with three anyons solve this problem and can even allow for a computationally universal set of single-qudit operations that are implemented by exchanges within the qudits and are hence leakage free. Qudits with four anyons have the additional advantage that they can have trivial total topological charge. When this is the case, the qudits can be moved around the quantum computer without disrupting the computation, since exchanges with the trivial charge have no effect on the state of the system. If we set aside issues of controlling large numbers of anyons, it appears that the optimal number of anyons per qudit may be the largest possible number (we will soon show that there is a maximum, in a useful sense). By increasing the number of anyons in each qubit, we increase the number of elementary exchange operations that are possible within each qubit. This has two advantages: firstly, with more elementary

| 1 |
| :--- |

Figure 2. The exchange of the $i$ th and $(i+1)$ th anyon, i.e. the braid $\tau_{i}$. We may think of this braid diagram as a spacetime diagram of the exchange process. Applying consecutive exchanges then corresponds to stacking such diagrams, or braid group multiplication.
operations, it may be easier to achieve a desired unitary operation, and secondly, it could reduce the need to use two-qudit gates that would introduce leakage errors. We will therefore be interested in finding the maximal number of anyons per qudit.

To study qudits containing $n$ anyons, we will use the braid group, $B_{n}$, which governs the exchanges of the $n$ anyons inside the qudit. $B_{n}$ has $n-1$ generators, $\tau_{1}, \ldots, \tau_{n-1}$, where $\tau_{i}$ exchanges particle $i$ with its neighbor, particle $i+1$ (see figure 2 ). These generators obey the following relations,

$$
\begin{align*}
& \tau_{i} \tau_{j}=\tau_{j} \tau_{i} \quad\{\text { provided }|i-j| \quad 2\}  \tag{1}\\
& \tau_{i} \tau_{i+1} \tau_{i}=\tau_{i+1} \tau_{i} \tau_{i+1} \tag{2}
\end{align*}
$$

$B_{n}$ will act on the $d$-dimensional Hilbert space of the qubit by a unitary representation. In principle, we may choose the $d$-dimensional qudit Hilbert space as a subspace of some higherdimensional representation of $B_{n}$, but we will not be interested in that possibility here, because in such cases, either $B_{n}$ mixes the qudit Hilbert space with the other states in the representation, which means that leakage occurs even for braidings within the qudit, or the qudit's Hilbert space is preserved under the action of $B_{n}$, but then we may as well just consider it by itself as a $d$-dimensional representation of $B_{n}$.

For any $n$, there are 1D unitary representations of $B_{n}$ labeled by an exchange angle $\theta$ and explicitly given by $\tau_{j} \mapsto \mathrm{e}^{\mathrm{i} \theta}$ (for all $j$ ). Clearly this means that $d$-dimensional representations of $B_{n}$ can be constructed for any $n$ by taking direct sums of such 1D representations; in such representations, all $\tau_{i}$ can be diagonalized simultaneously. Such representations are not very useful for TQC. Therefore, given the dimension $d$ of our qudit, we will look for the maximal number of particles $n$ for which we can have a $d$-dimensional representation of $B_{n}$, which is not of this reducible form.

### 2.1. Qubits

2.1.1. No leakage-free qubits with more than four anyons. As stated in the introduction, previous work on qubit design has concentrated on working with models where each qubit contains three or four anyons. We will give a simple argument that shows that there are in fact no qubits with $n>4$ anyons that have a non-trivial representation of $B_{n}$.

To study 2D representations of $B_{n}$, we first choose a basis such that $\tau_{1}$ is a diagonal matrix. Relation (1) then tells us that any generator that is not adjacent to $\tau_{1}$ must commute with it, and relation (2) tells us that if neighboring generators commute then they are equal. Moreover, it is not hard to see that all generators $\tau_{i}$ are conjugate to each other, and this implies that if any pair of neighboring generators $\tau_{i}$, $\tau_{i+1}$ commute, all neighboring pairs commute; and in fact, as a result, if any neighboring generators commute, then all generators are represented by the same matrix, i.e. by the same diagonal matrix as $\tau_{1}$.

If the two eigenvalues of $\tau_{1}$ are equal, then $\tau_{1}$ is a multiple of the identity matrix and hence it commutes with all other generators, giving us a diagonal representation. We therefore look at the case where the eigenvalues of $\tau_{1}$ are not equal. Now we note the fact that if a diagonal $d \times d$-matrix has $d$ distinct eigenvalues, any other matrix that commutes with it must also be diagonal. If $N \quad 5$, we have generators, $\tau_{1}, \ldots, \tau_{3}, \tau_{4}, \ldots$, and then (1) shows that both $\tau_{3}$ and $\tau_{4}$ commute with $\tau_{1}$. As a result, for $d=2$, both $\tau_{3}$ and $\tau_{4}$ must be diagonal. But then $\tau_{3}$ and $\tau_{4}$ commute with each other, which, by (2), gives us a diagonal representation.

It is clear therefore that to avoid our representation of the braid group becoming diagonal (i.e. a sum of two 1 D representations), we must construct our qubits out of no more than four particles. If we do decide to have qubits with more than four anyons, then we have to choose between having qubits without interesting single-qubit operations from in-qubit braiding, or introducing leakage for single-qubit operations. Neither of these alternatives seem desirable, so we should ensure that $N \quad 4$. This shows that the models that have so far been examined do, in fact, use the optimal numbers of anyons per qubit.
2.1.2. Braiding and universality for qubits. Since qubits with three or four anyons are the only ones that allow interesting internal braiding and no leakage, let us give explicit formulae for the elementary exchange matrices as they act in an arbitrary unitary 2D representation of $B_{3}$ or $B_{4}$ (these will also be useful for future reference). In any representation $B_{n} \rightarrow U(d)$, we may divide all representation matrices by their determinant to obtain a representation of $B_{n}$ into $S U(d)$. The determinant is an overall phase and hence irrelevant to TQC, but we may always reobtain all $U(d)$ representations from the $S U(d)$ representations by multiplying these by 1D unitary representations (given by $\tau_{j} \mapsto \mathrm{e}^{\mathrm{i} \phi}$ for some $\phi \in \mathrm{R}$ ). In the case of a qubit, we can thus work with $S U(2)$ matrices. Let us start with the case of $B_{3}$. We will call our arbitrary representation $\eta: B_{3} \rightarrow S U(2)$. It is convenient to choose a basis in which $\eta\left(\tau_{1}\right)$ is diagonal. We will assume that its eigenvalues $a$ and $\bar{a}$ are distinct, since otherwise the whole representation will be diagonal. Using up the remaining freedom in our choice of basis, we can ensure that the off-diagonal elements of $\eta\left(\tau_{2}\right)$ are real and the off-diagonal element in the first row of the matrix is positive. We can then directly use the defining relations of $B_{3}$ to obtain the possible forms for the generators. We find that

$$
\eta\left(\tau_{1}\right)=\begin{array}{cc}
a & 0  \tag{3}\\
0 & \bar{a}
\end{array}, \quad \eta\left(\tau_{2}\right)=\begin{array}{cc}
\frac{1}{a-a^{3}} & b \\
-b & \frac{1}{\bar{a}-\bar{a}^{3}}
\end{array}
$$

 therefore $b^{2}>0$, there are restrictions on the value of $a$. Taking the determinant of $\tau_{2}$ gives $\frac{1}{2-a^{2}-\bar{a}^{2}}+b^{2}=1$ and as a result $\frac{1}{2-a^{2}-\bar{a}^{2}} \quad 1$. Substituting $a=\mathrm{e}^{\mathrm{i} \theta}$, we get the restriction $\frac{-\pi}{6}$ $\theta \quad \frac{\pi}{6}$.

If the qubit is composed of four anyons, we get one extra generator, $\tau_{3}$. Since the generators are all conjugate, they must have the same eigenvalues, and since $\eta\left(\tau_{3}\right)$ commutes with $\eta\left(\tau_{1}\right)$, it must be diagonal. Hence, it has two possible values: $\eta\left(\tau_{3}\right)=\eta\left(\tau_{1}\right)$ or $\eta\left(\tau_{3}\right)=\overline{\tau_{1}}$. If $\eta\left(\tau_{3}\right)=\eta\left(\tau_{1}\right)$, this poses no extra restrictions on $a$ or $b$. However, if $\eta\left(\tau_{3}\right)=\bar{\tau}_{1}$, then one finds from $\tau_{2} \tau_{3} \tau_{2}=\tau_{3} \tau_{2} \tau_{3}$ that $a$ must be a primitive eighth root of unity, that is, $a= \pm \mathrm{e}^{ \pm i \pi / 4}$.

Any representation of the braid group that comes from an anyon model with finitely many distinct topological charges must have eigenvalues for the exchanges $\tau_{i}$, which are roots of unity at some finite order. This is guaranteed by Vafa's theorem (see [13] and also the appendix of [9]). In other words, not all values of $a$ that are allowed by the braid group relations are likely to occur. It is of interest to identify the Jones representations of $B_{3}$, which are related to $S U(2)$ Chern-Simons theory, among the full set of representations given here. Explicit matrices $\rho_{r}\left(\tau_{1}\right)$ and $\rho_{r}\left(\tau_{2}\right)$ for these representations are given in [4], in the following form,

$$
\rho_{r}\left(\tau_{1}\right)=\begin{array}{cc}
q & 0  \tag{4}\\
0 & -1
\end{array}, \quad \rho_{r}\left(\tau_{2}\right)=\begin{array}{cc}
\frac{-1}{q+1} & \overline{[3]_{q}} \\
\overline{[3]_{q}} & \frac{q^{2}}{q+1}
\end{array}
$$

where $[x]_{q}=\frac{q^{x / 2}-q^{-x / 2}}{q^{1 / 2}-q^{-1 / 2}}$ and $q=\mathrm{e}^{ \pm 2 \pi \mathrm{i} / r}$, with $r \in \mathrm{~N}, r \quad 3$.
We can see from this that if we multiply our representation, $\eta$, by a factor of $-a$ and perform a coordinate transformation such that the off-diagonal terms pick up a factor of $i$, then the two representations will be equal, provided $q=-a^{2}$. This means that $q=-\mathrm{e}^{2 i \theta}=\mathrm{e}^{\mathrm{i}(2 \theta-\pi)}$. But $\frac{-\pi}{6} \quad \theta \quad \frac{\pi}{6}$, so taking the two extreme values of $\theta$, we obtain $q=\mathrm{e}^{ \pm 2 i \pi / 3}$.

We can now make some strong statements about the universality of the $B_{3}$ and $B_{4}$ representations we have found. Freedman et al's universality results in [4] reduce, in this simple case, to the statement that the images of the representations $\rho_{r}$ are dense in an $S U(2)$ subgroup of $U(2)$ whenever $r \quad 5, r \neq 6,10$. Hence our corresponding representations are dense in $S U(2)$ for the corresponding values of $a$.

Recent results of Kuperberg [14] actually settle the question of universality for any other roots of unity and even for arbitrary eigenvalues as well. His corollary 1.2 and theorem 1.4 state, for the representations of $B_{3}$ and $B_{4}$ considered here, that their images are all dense in $S U(2)$, unless $q=-a^{2}=\mathrm{e}^{\mathrm{i} \phi}$ with $|\phi|=\pi-\frac{2 \pi}{n}$, where $\phi$ is an angle and $n \in \mathrm{Z}, n \quad 3$, or $q$ is a root of unity of order 10 . Note that the cases $n=3, n=4$ and $n=6$ are the only cases in which $\pi-\frac{2 \pi}{n}$ is of the form $\frac{2 \pi}{r}$ for an integer $r$, with also $r \in\{3,4,6\}$ so that the exceptional cases with $\phi= \pm \frac{2 \pi}{r}$ are the same as those found by Freedman et al.

### 2.2. Qudits with $d>2$

In section 2.1.1, we showed that qubits should involve $n<5$ anyons in order to allow for leakage-free and non-Abelian single-qubit operations. We now argue that there is a similar maximum number of anyons for qudits of any dimension $d$. Our arguments will not depend strongly on the detailed structure on the braid group, beyond features that are common to many similar exchange groups, such as the motion group for ring-shaped excitations in 3D and other motion groups, as defined by Dahm [15] (see also [16]). Specifically, we will use the following properties of the braid group representation that acts on the qudit:

1. Generators that do not involve the same objects (i.e. particles and strands) commute.
2. The group is represented unitarily.
3. The generators in our favored set are conjugate to each other and in fact any adjacent pair of generators is conjugate to any other adjacent pair.

The first of these properties is connected with the basic physical principle that spatially separated operators commute and the second comes from the unitarity of time evolution. The availability of a set of conjugate generators is a bit more special. However, one may expect this whenever, as in the case of the braid group, all generators perform the same type of action and the ordering of the objects being exchanged is just a matter of convention. If there are different types of generator (such as exchanges of distinguishable types of particles), then this will no longer fully hold.
2.2.1. Existence of an upper limit on n for qudits. A representation of $B_{n}$ will become completely Abelian if any generator commutes with a neighboring generator. From property 3 above, it then follows that all generators will commute with those adjacent to them and hence with all other generators (using property 1 ). Let us consider a $d$-dimensional representation $\eta$ of $B_{n}$. Since the generators of $B_{n}$ are conjugate, their representation matrices $\eta\left(\tau_{i}\right)$ all have the same eigenvalues $\left(\lambda_{1}, \ldots, \lambda_{d}\right)$. We now choose a basis in which all the representation matrices of the odd-numbered generators, $\tau_{1}, \tau_{3}, \ldots$, are simultaneously diagonal. For $n \quad 5$, no two of the diagonal matrices $\eta\left(\tau_{i}\right)$ with $i$ odd can be the same, unless $\eta$ is Abelian. The reason for this is that, when $n 5$, for every pair of odd generators $\tau_{i}$, $\tau_{j}$ (with $i, j$ odd) there is an even generator that is adjacent to one of the pair, say $\tau_{i}$, but not adjacent to the other, say $\tau_{j}$. If $\eta\left(\tau_{i}\right)=\eta\left(\tau_{j}\right)$, then the even generator adjacent to $\tau_{i}$ will commute with $\eta\left(\tau_{i}\right)$, since it necessarily commutes with $\eta\left(\tau_{j}\right)$ and $\eta\left(\tau_{i}\right)=\eta\left(\tau_{j}\right)$. But then two neighboring generators commute and as we argued before, the whole representation becomes Abelian. Hence a non-Abelian $d$-dimensional representation of $B_{n}$ must yield a different arrangement of the eigenvalues $\left(\lambda_{1}, \ldots, \lambda_{d}\right)$ in every one of the representation matrices of the odd generators $\tau_{1}, \tau_{3}, \ldots$ when these are diagonalized. Since there are only a finite number of possible distinct arrangements of the eigenvalues (at most $d$ ! if they are all distinct), this places an upper limit on the number of odd generators and hence on the number of anyons one may have at this value of $d$ without making the representation completely Abelian.
2.2.2. Qutrits. The previous paragraph shows that there is an upper limit on the number of anyons per qudit for any $d$, but it obviously overestimates this limit. It is interesting to look in a bit more detail at the case of qutrits, i.e. $d=3$. As previously stated, we can diagonalize all the odd-numbered generators. If all eigenvalues are equal, we will always have a trivial representation, and if all are different, we will get the same result as we obtained for qubits in section 2.1.1, namely we must have $n \quad 4$. There is then only one case left for us to look at: the case with two distinct eigenvalues, one of them with multiplicity 2 and the other with multiplicity 1 . There are only three patterns in which such a selection of eigenvalues can be arranged in a diagonal matrix; therefore we know that we must have no more than three oddnumbered generators. If we now look at the even-numbered generators, we see that there can be at most three, $\tau_{2}, \tau_{4}$ and $\tau_{6}$. The form of the representation matrices of the even-numbered generators is restricted, as they must commute with all spatially separated odd-numbered generators and hence must preserve their eigenspaces.

We see then that for $n=7, \tau_{2}$ and $\tau_{4}$ will preserve the same eigenspaces as $\tau_{5}$ and $\tau_{1}$, respectively, but $\tau_{6}$ will commute with both $\tau_{1}$ and $\tau_{3}$ and so must preserve the same eigenspaces
as both of these generators. But $\tau_{1}$ and $\tau_{3}$ must have different patterns of eigenvalues. Let us denote our basis vectors by $\beta_{1}, \beta_{2}$ and $\beta_{3}$; then by a choice of ordering we can make sure that $\beta_{1}$ and $\beta_{2}$ form the 2D eigenspace of $\tau_{1}$ and $\beta_{2}$ and $\beta_{3}$ form the 2D eigenspace of $\tau_{3}$. Since $\tau_{6}$ must conserve both eigenspaces, it cannot map $\beta_{2}$ into $\beta_{1}$ or $\beta_{3}$, and in fact we see that $\tau_{6}$ must be diagonal. As a result, $\tau_{6}$ commutes with $\tau_{5}$ and so we have two neighboring generators commuting and our representation of $B_{7}$ is Abelian.

Moving to the $n=6$ case, we eliminate the problem of having an even-numbered generator that commutes with two odd-numbered generators. Nevertheless, this case too proves to be Abelian. We now have two even generators, $\tau_{2}$ and $\tau_{4}$, which both commute with only one oddnumbered generator, but we also have to take into consideration the fact that all even generators are non-neighboring and so they must commute among themselves. However, the form of the matrices representing $\tau_{2}$ and $\tau_{4}$ is restricted in different ways, because they preserve different eigenspaces of different odd-numbered generators. By a suitable ordering of the basis, we can make sure that $\tau_{2}$ and $\tau_{4}$ map to matrices of the following form,

$$
\tau_{2} \mapsto \begin{array}{cccccccc} 
& M_{11}^{(1)} & M_{12}^{(1)} & 0 & & \lambda & 0 & 0 \\
M_{21}^{(1)} & M_{22}^{(1)} & 0 & \tau_{4} \mapsto & 0 & M_{11}^{(2)} & M_{12}^{(2)} \\
0 & 0 & \lambda & & 0 & M_{21}^{(2)} & M_{22}^{(2)}
\end{array},
$$

where $M^{(1)}$ and $M^{(2)}$ are unitary $2 \times 2$-matrices and $\lambda$ is the eigenvalue of the $\tau_{i}$ that has multiplicity 2 . The only way two such matrices may commute is if they are both diagonal and in that case the representation becomes Abelian. In conclusion, we see that for $d=3$ we must have $n \quad 5$. Note that we have never explicitly used the braid relation $\tau_{i} \tau_{i+1} \tau_{i}=\tau_{i+1} \tau_{i} \tau_{i+1}$ until now, although of course it has been present in the background, in the sense that it guarantees that the elementary exchanges are all conjugate to each other. Moving to higher dimensions $d$ makes this kind of argument more difficult as the basis vectors can be split into groups such that all of the groups contain more than one vector, which makes it more difficult to determine the precise nature of the restrictions that come from the fact that even generators commute.
2.2.3. Some general definitions and results. Clearly, the actual maximum number $n$ for which we may have a non-Abelian, leakage-free qudit of dimension $d$ involving $n$ anyons, or equivalently, a non-Abelian $d$-dimensional representation of $B_{n}$, depends strongly on the number and multiplicity of the eigenvalues of the generators of the braid group in the representation. The number of distinct eigenvalues of an elementary exchange is usually equal to the number of distinct topological charges that may be produced in the fusion of two of the elementary anyons in the system. Hence we should not expect this to be very large, typically. The actual values of the eigenvalues are connected with the topological spins, or conformal weights of the various fusion products of the elementary anyons, and they are important observables in many physical implementations of anyonic systems. Therefore, it would seem to make sense to refine our search for the qudit with the largest number of anyons. We can define various versions of the 'maximal number of anyons' as follows:

- $N(d)$ is the largest $n$ for which $B_{n}$ has a non-Abelian representation of dimension $d$.
- $N(d, p)$ is the largest $n$ for which $B_{n}$ has a non-Abelian representation of dimension $d$, such that the elementary exchanges have $p$ distinct eigenvalues.
- $N(d, \bar{m})$ is the largest $n$ for which $B_{n}$ has a non-Abelian $d$-dimensional representation such that the exchanges have eigenvalues with multiplicities $m_{1}, \ldots, m_{p}$ given by the partition $\bar{m}$ of $d$. For example, if $\bar{m}=(2,2,1)$, then $d=5$ and the representation is required to have three distinct eigenvalues, two of them with multiplicity 2 and one with multiplicity 1.
- $N(d, \bar{m}, \bar{\lambda})$ is the largest $n$ for which there is a non-Abelian $d$-dimensional representation of $B_{n}$ such that the exchanges have eigenvalues $\bar{\lambda}=\left(\lambda_{1}, \ldots, \lambda_{p}\right)$ with multiplicities $\bar{m}=\left(m_{1}, \ldots, m_{p}\right)$.
Any attempt at a full determination of all these numbers is well beyond the scope of this paper, but the arguments we have given already provide upper bounds for all these numbers (although not very good ones). Our results for qubits and qutrits may be summarized as $N(2)=N(2,2)=4, N(3)=N(3,2)=N(3,(2,1))=5$ and $N(3,3)=4$. It is easy to see that our argument for qubits generalizes to all cases where the number of eigenvalues equals $d$ and we have $N(d, d)=4$. Many interesting representations with two and three distinct exchange eigenvalues (corresponding to two or three fusion channels for the elementary anyons) are obtained from the theory of Hecke algebras and BMW-algebras, and it would be interesting to apply these to find more of the $N(d, \bar{m}, \bar{\lambda})$. It is actually not difficult to see (see also below) that a unitary representation with two eigenvalues and dimension $d$ exists for $n=d+2$, so $N(d, 2) \quad d+2$ (and we will see below that this implies that $N(d, 2)=N(d)=d+2$ ), but the question becomes more interesting if the multiplicities or values of the eigenvalues are given.

An important general result for $N(d)$ has been proved by Formanek in [17]. That paper showed that

$$
N(d)=d+2
$$

which is exactly the result we have found above in the $d=2,3$ cases. We nevertheless gave our own proofs for these special cases because we wanted to make it obvious that these results are based on the simple physical properties of exchange groups highlighted at the start of section 2.2 , namely the fact that the operations are conjugate to each other and non-neighboring generators commute. We therefore expect that the result found for $N(d)$ can be generalized to apply to a range of exchange groups beyond $B_{n}$.

All the irreducible representations of the braid group $B_{n}$ that are of dimension $d \quad n$ have in fact been classified relatively recently in [18]. There are 11 cases, cases (A) through (K), listed in that paper. Cases (A) and (B), shown below, apply to any number of particles, while the remaining cases are special and we shall mention only the ones that are necessary for our calculations.
(A) A representation of Burau type, either:
$\chi(y) \otimes \beta_{n}(z): B_{n} \rightarrow G L_{n-1}(\mathrm{C})$, where $1+z+\cdots+z^{n-1} \neq 0$, or $\chi(y) \otimes \beta_{n}(z): B_{n} \rightarrow G L_{n-2}(\mathrm{C})$, where $1+z+\cdots+z^{n-1}=0$.
(B) A representation of standard type: $\chi(y) \otimes \gamma_{n}(z): B_{n} \rightarrow G L_{n}(\mathrm{C})$, where $z \neq 1$.

In both cases, $\chi$ is a character of $B_{n}$ (i.e. a 1D representation). Also, $\beta_{n}(z)$ denotes the reduced Burau representation of $B_{n}$ with parameter $z$, while $\beta_{n}$ is the non-trivial composition factor of $\beta_{n}(z)$, which exists when $z$ is an $n$th root of unity. Explicit formulae for $\beta_{n}$ and $\beta_{n}$ and also for the standard representation $\gamma_{n}$ can be found in [18].

The special cases all occur for $3<n<9$. We will mention the cases that are relevant to qutrits. These necessarily occur for $2 n \quad 5$. The case $n=2$ is uninteresting because it is necessarily Abelian. For $n=3$, we have case (B) above. For $n=4$, we have $\beta_{4}$ from (A), as well as the special case ( $D$ ). The representation in case (D) is written as $\epsilon_{4}(z): B_{4} \rightarrow G L_{3}(\mathrm{C})$ and is given in [18]. Finally, for $n=5$, we use the non-trivial composition factor $\beta_{5}(z)$ from case (A).

The paper [18] deals with representations into $G L_{d}(\mathrm{C})$ so one may be concerned about unitarity. However, we find that, in each of the above cases, taking $\chi(y)$ unitary and restricting the values of the parameter $z$ to roots of unity yields a unitary (or at least unitarizable) representation.

## 3. Two-qudit gates and leakage

Even if we assume that no leakage occurs in single-qubit gates, it is still likely to plague multiqubit gates. On the other hand, if we are able to construct a universal set of leakage-free two-qubit gates, then we can perform universal quantum computation without any leakage, since any multi-qubit gates can be generated from one-qubit and two-qubit gates. A first simple question one may ask is whether systems of two qubits (or more general qudits) exist in which all anyon exchange processes are leakage free. This means, in effect, that the computational Hilbert space for such a two-qudit system is closed under the action of the braid group for the anyons involved in the qudits. In other words, the computational Hilbert space itself carries a representation of the full two-qubit braid group. Let us assume that the two qubits involve $n$ anyons, with the individual qudits consisting of $n_{1}$ and $n_{2}$ anyons (where $n_{1}+n_{2}=n$ ). Any representation $\rho$ of $B_{n}$ that provides us with leakage-free two-qubit braiding then has some very special properties. First of all, if the individual qudits have Hilbert space dimensions $d_{1}$ and $d_{2}$, then the two-qudit Hilbert space has dimension $d=d_{1} d_{2}$ and we can think of it as the tensor product of the qudits' Hilbert spaces. Now, for the elementary exchanges $\tau_{1}, \ldots, \tau_{n_{1}-1}$ that involve only the anyons in the first qudit, we can write the representation matrices as

$$
\begin{equation*}
\rho\left(\tau_{i}\right)=\rho_{1}\left(\tau_{i}\right) \otimes I_{d_{2}} \quad\left(1 \quad i \quad n_{1}-1\right) \tag{5}
\end{equation*}
$$

where $\rho_{1}$ is the $d_{1}$-dimensional representation of $B_{n_{1}}$ on the Hilbert space of the first qudit and $\mathrm{I}_{d_{2}}$ is the $d_{2}$-dimensional identity matrix. Similarly, the matrices for the elementary exchanges $\tau_{n_{1}+1}, \ldots, \tau_{n-1}$ that involve only the anyons in the second qudit can be written as

$$
\begin{equation*}
\rho\left(\tau_{i}\right)=\mathrm{I}_{d_{1}} \otimes \rho_{2}\left(\tau_{i}\right) \quad\left(n_{1}+1 \quad i \quad n-1\right), \tag{6}
\end{equation*}
$$

where $\rho_{2}$ is the $d_{2}$-dimensional representation of $B_{n_{2}}$ on the Hilbert space of the second qudit. Once the single-qudit representations $\rho_{1}$ and $\rho_{2}$ are fixed, the representation matrix for the only remaining braid generator, $\tau_{n_{1}}$, is subject to the constraint that it must solve all the braid relations (1) and (2). Whenever a solution to these constraints can be found, we have a completely leakage-free two-qudit system. However, we will see that for qudits of low dimension, such as qubits and qutrits, the constraints can usually not be satisfied, so that for almost all types of qubits and qutrits, it is unavoidable that leakage will appear for at least some of the possible exchange processes.

Despite our results for low-dimensional qudits, it is possible to have situations without any leakage for high enough qudit dimensions. For example, if each anyon carries a representation of a quantum group (i.e. a quasitriangular Hopf algebra), the tensor product of these representations
carries a braid group representation defined by exchanging tensor factors and applying the $R$-matrix of the quantum group. This yields leakage-free braiding, since there are no states outside the tensor product to leak into. Since in such situations each anyon must have a vector space of dimension at least 2 attached to it, we get a minimum of $d=8$ dimensions for a qudit made up of three such anyons (or $d=16$ for four anyons). It is conjectured (see e.g. [19], conjecture 6.6) that the braid group representations that occur in this way always have a finite braid group image and therefore are never universal for quantum computation.

### 3.1. Two qubits

We showed in section 2.1 that a leakage-free, non-Abelian qubit can be made of either three or four anyons; therefore there are, in principle, three different types of two-qubit systems: firstly with two qubits each composed of three anyons ( $2 \times 3$-qubit), secondly with two qubits each composed of four anyons ( $2 \times 4$-qubit) and lastly with one 3 -qubit and one 4 -qubit. However, for the $2 \times 4$-qubit system we would need to have a 4 D representation of $B_{8}$, and for the case with a four-qubit and a three-qubit we would need a 4D representation of $B_{7}$ to obtain totally leakage-free braiding. As we discussed in section 2.2 .3 , it was shown in [17] that no $d$-dimensional representation of $B_{n}$ can exist with $d<n-2$ and therefore both of these cases cannot be realized without leakage.

This leaves us with the system of two 3-anyon qubits to consider. We need to construct a 4D representation, $\rho$, of the braid matrices of the group $B_{6}$. For this two-qubit system to be leakage free, we require it to decompose as a tensor product of two 2 D representations. We have five elementary exchanges, $\tau_{1}, \ldots, \tau_{5}$. Of these, $\tau_{1}, \tau_{2}$ and $\tau_{4}, \tau_{5}$ will take the forms given in equations (5) and (6), respectively, and by a convenient choice of basis, we can make sure that the single-qubit representations $\rho_{1}$ and $\rho_{2}$ that occur in those equations are both given by the standard form $\eta$ that we introduced in equation (3). This yields

$$
\begin{aligned}
& \rho\left(\tau_{1}\right)=\begin{array}{cccc}
a & 0 & 0 & 0 \\
0 & a & 0 & 0 \\
0 & 0 & \bar{a} & 0 \\
0 & 0 & 0 & \bar{a}
\end{array}, \quad \rho\left(\tau_{2}\right)=\begin{array}{cccc}
\frac{1}{a-a^{3}} & 0 & c & 0 \\
0 & \frac{1}{a-a^{3}} & 0 & c \\
& 1 & \\
-c & 0 & \frac{1}{\bar{a}-\bar{a}^{3}} & 0 \\
0 & -c & 0 & \frac{1}{\bar{a}-\bar{a}^{3}}
\end{array}
\end{aligned}
$$

All the generators are conjugate and have the same eigenvalues, so $f=a$ or $\bar{a}$, and hence also $e=c=1-\frac{1}{2-a^{2}-\bar{a}^{2}}$. We can now fix $\rho\left(\tau_{3}\right)$ by imposing the braid group relations. Since $\tau_{3}$
is unitary and commutes with $\tau_{1}$ and $\tau_{5}$, we see that it must be diagonal. It will also have eigenvalues $a$ and $\bar{a}$, like the other generators, but it cannot have the same arrangement of eigenvalues as $\tau_{1}$ or $\tau_{5}$ as this will mean one of the adjacent generators will commute with it and we will get an Abelian group (cf section 2.2). Hence,

$$
\rho\left(\tau_{3}\right)=\begin{array}{cccc}
x & 0 & 0 & 0 \\
0 & \bar{x} & 0 & 0 \\
0 & 0 & \bar{x} & 0 \\
0 & 0 & 0 & x
\end{array} \quad\{\text { where } x=a \text { or } x=\bar{a}\}
$$

The relation $\tau_{2} \tau_{3} \tau_{2}=\tau_{3} \tau_{2} \tau_{3}$ now yields the following two equations,

$$
\begin{align*}
& c \frac{x}{a-a^{3}}-\frac{\bar{x}}{\bar{a}-\bar{a}^{3}}=c|x|^{2},  \tag{7}\\
& c \frac{\bar{x}}{a-a^{3}}-\frac{x}{\bar{a}-\bar{a}^{3}}=c|x|^{2} . \tag{8}
\end{align*}
$$

We can equate the left-hand sides of equations (7) and (8) and by some simple manipulations we get a restriction on the eigenvalue $a$,

$$
a^{2}=-\bar{a}^{2} .
$$

But $a=\mathrm{e}^{\mathrm{i} \theta}$, so we obtain $\mathrm{e}^{2 i \theta}=-\mathrm{e}^{-2 i \theta}$, or $\cos (2 \theta)=-\cos (2 \theta)$. It follows that $\cos (2 \theta)=0$, which gives $\theta= \pm \frac{\pi}{4}$ or $\theta= \pm \frac{3 \pi}{4}$. In short, $a$ must be a primitive eighth root of unity. One now checks easily that with these values of $a$, we also satisfy the relation $\tau_{3} \tau_{4} \tau_{3}=\tau_{4} \tau_{3} \tau_{4}$ and so we find that a leakage-free representation $\rho$ exists provided the eigenvalues of the elementary exchange matrices are primitive eighth roots of unity. Unfortunately, this restriction on the eigenvalues makes the system non-universal for quantum computation (even at the single-qubit level). The representations of $B_{6}$ we have found in this way are precisely the ones one obtains from anyon models with the fusion rules of the Ising model and, in fact, for these anyon models the full six-anyon Hilbert space with trivial total topological charge is 4D, which explains the absence of leakage.

### 3.2. Qutrits and qubit-qutrit combinations

We can use the method explained at the start of section 3 also to study whether totally leakagefree braiding is possible in systems consisting of two qutrits or systems that have a qubit and a qutrit. All 3D representations of $B_{n}$ are known and can be divided into just a few classes, as explained at the end of section 2.2.3, with explicit formulae for the representations given in [18], so the analysis proceeds in the same way as for two-qubit systems.

Non-Abelian qutrits can be composed of 3,4 or 5 anyons and so a two-qutrit system can have $3+3$ or $3+4$ or $3+5$ or $4+4$ or $4+5$ or $5+5$ anyons. We have checked all cases in the same way as for the $3+3$ anyon system of two qubits in section 3.1 and found that no leakagefree non-Abelian braid group representations exist, so having at least some braids with leakage is unavoidable in two-qutrit systems.

For a system of one qubit and one qutrit, we are looking for a $B_{n}$ representation of dimension $d=6$, with necessarily $n \quad 8$. Hence we must consider qubit-qutrit systems of $3+3$, $3+4,3+5$ or $4+4$ anyons. Again, we checked all these cases by direct calculation and found no leakage-free non-Abelian braid group representations.

One may, in principle, go at least a little beyond qutrits by the same method, since, for example, all 4D and 5D irreducible representations of $B_{3}$ are given in [20].

### 3.3. Leakage-free gates in a system with leakage

So far we have shown that for systems consisting of qubits and qutrits, it is not possible to have a situation where all braidings are leakage free, except in an exceptional case with nonuniversal qubits of Ising type. However, the requirement that all braids are leakage free is needlessly restrictive. Even if leakage occurs for some braids, we could avoid those and perform computations using only those braids that cause no leakage. In fact, to obtain universal leakagefree quantum computation by braiding, it is enough to have a single leakage-free entangling two-qubit braiding gate in combination with a universal set of leakage-free single-qubit gates. Clearly, the braids that do not cause leakage in a certain representation form a subgroup of the braid group, which we may dub the leakage-free subgroup. It would be of great interest to find the leakage-free subgroup of the braid group for representations that occur in simple anyon models, and of even greater interest to find the closure of the images of these representations in the corresponding unitary groups. Again, if braiding within qubits is universal and a single leakage-free entangling two-qubit gate exists, then the projective image of the leakage-free subgroup should be dense. Unfortunately, no one has so far been able to construct a leakagefree entangling two-qudit braiding gate in any anyon model that has universality for single-qudit operations by braiding, and we will not attempt to change that situation here. Pessimists may be tempted to conjecture at this point that the image of the leakage-free subgroup is always either finite or composed of combinations of single-qudit gates.

## 4. Summary and discussion

We have considered some basic questions concerning the optimal design of qudits in topological quantum computers, notably the question of how many anyons we should use per qudit and the question of to what extent leakage can be avoided in single- and multi-qudit systems. In section 2, we determined that topological qubits cannot be composed of more than four anyons, and for general qudits of dimension $d$, there is an upper limit of $d+2$ anyons. We also saw that this upper limit may be lowered if restrictions are placed on the eigenvalues of the elementary exchanges of adjacent anyons. We summarized the properties of qubits with three and four anyons and indicated the full set of braid group representations that could be used for qutrits. In section 3 , we examined the possibility of creating leakage-free two-qubit gates and found that we can usually not require all braid operations to be leakage free, and in the exceptional cases where this is possible, we cannot have universality. Similar results were obtained for systems that are built from qutrits or from a mixture of qubits and qutrits.

While our results are only a very small step in what will surely become a great journey toward the optimal framework for TQC, we hope that they highlight some interesting directions that have so far not received much attention. In particular, it would be very interesting to obtain more information about the various numbers $N(d, p), N(d, p, \bar{m})$, etc defined in section 2.2.3. Apart from obtaining the actual numbers, one might, for example, ask in which cases these maxima are obtained by a braid group representation that describes the exchanges of anyons and is hence embedded in a topological quantum field theory. Any progress in the determination of
the leakage-free group, even for a single-anyon model with universal braiding in single qubits, would also be of great importance.

One may wonder if leakage might be avoided better with a more flexible construction of qubits; for example, by not completely fixing the combined topological charge of the anyons forming a single qubit. There does naively seem to be more potential for avoidance of leakage in anyon models that possess anyons whose quantum dimensions are integers or square roots of integers, such as the anyon model that comes from the $S U(2)_{4}$ Chern-Simons theory. For such models, the dimension of the full topological Hilbert space scales as $p^{N / 2}$ where $N$ is the number of anyons and $p$ is an integer. This suggests that the full topological Hilbert space might split as a tensor product of $p$-dimensional 'qupits'. In reality, this usually does not happen because the scaling formula is only asymptotic (for exact formulae for the dimensions of the braid group representations associated with $S U(2)_{4}$, see, for instance, [21]). Nevertheless, in a recent preprint [22], Rowell and Wang indicate how in some cases the topological Hilbert space may be enlarged to allow for an actual tensor product splitting. An interesting question is whether this enlargement could somehow be achieved physically. One may ask similar questions about anyons with quantum dimensions that are higher-order roots of integers, but we are not aware of any anyon models that allow for such quantum dimensions. Finally, we note that it is conjectured [19], and known for the cases treated in [22], that braid group representations coming from anyons with quantum dimensions that square to an integer are non-universal for TQC, so this leads again to an alternative between allowing for leakage or losing universality.

## Acknowledgment

This work was supported by Science Foundation Ireland Principal Investigator award number 08/IN.1/I1961.

## References

[1] Kitaev A Yu 2003 Fault-tolerant quantum computation by anyons Ann. Phys. 3032
[2] Freedman M H 1998 P/NP and the quantum field computer Proc. Natl Acad. Sci. USA 95 98-101
[3] Freedman M H, Larsen M J and Wang Z 2002 A modular functor which is universal for quantum computation Commun. Math. Phys. 227 605-22
[4] Freedman M H, Larsen M J and Wang Z 2002 The two-eigenvalue problem and density of Jones representation of braid groups Commun. Math. Phys. 228 177-99
[5] Bonesteel N E, Hormozi L, Zikos G and Simon S H 2005 Braid topologies for quantum computation 2005 Phys. Rev. Lett. 95140503
[6] Hormozi L, Zikos G, Bonesteel N E and Simon S H 2007 Topological quantum compiling Phys. Rev. B 75165310
[7] Freedman M H, Kitaev A, Larsen M J and Wang Z 2003 Topological quantum computation Bull. Am. Math. Soc. 4031
[8] Preskill J 2004 Topological quantum computation Lecture Notes http://www.theory.caltech.edu/~preskill/ ph219/topological.ps
[9] Kitaev A 2006 Anyons in an exactly solved model and beyond Ann. Phys. 321 2-111
[10] Bonderson P, Shtengel K and Slingerland J K 2008 Interferometry of non-abelian anyons Ann. Phys. 323 2709-55
[11] Bonderson P H 2007 Non-Abelian anyons and interferometry PhD Thesis Caltech, Pasadena, CA
[12] Haitan Xu and Wan X 2008 Constructing functional braids for low-leakage topological quantum computation Phys. Rev. A 78042325
[13] Vafa C 1988 Toward classification of conformal theories Phys. Lett. B 206 421-426
[14] Kuperberg G 2009 Denseness and Zariski denseness of Jones braid representations arXiv:0909.1881
[15] Dahm D M 1962 A generalisation of braid theory PhD Thesis Princeton University, Princeton
[16] Goldsmith D L 1981 The theory of motion groups Michigan Math. J. 28 3-17
[17] Formanek E 1996 Braid group representations of low degree Proc. London Math. Soc. s3-73(2) 279-322
[18] Formanek E, Lee W, Sysoeva I and Vazirani M 2003 The irreducible representations of the braid group on $n$ strings of degree $n$ J. Algebr. Appl. 2 317-33
[19] Rowell E, Stong R and Wang Z 2009 On classification of modular tensor categories Commun. Math. Phys. 292 343-89
[20] Tuba I and Wenzl H 2001 Representations of the braid group $B_{3}$ and of SL(2,Z) Pac. J. Math. 197 491-510
[21] Slingerland J K and Bais F A 2001 Quantum groups and non-abelian braiding in quantum hall systems Nucl. Phys. B 612 229-90
[22] Rowell E C and Wang Z 2010 Localization of unitary braid group representations arXiv:1009.0241

