FS2011 Advanced Topics in Quantum Information Theory

Matthias Christandl

May 23, 2011

1 Decoherence Free Subspaces

1.1 General Theory

We have seen two ways of deriving a master equation for the evolution of the density matrix ρ of a system which interacts with an environment (I drop the subscript S for system) in Atac Imamoglu's lectures. The derivation was based on three assumptions about the time evolution

- initial decoupling of system and environment
- complete positivity
- Markovian dynamics.

This master equation reads:

$$\frac{d}{dt}\rho(t) = L(\rho),$$

where

$$L(\rho) = -i[H, \rho] + L_D(\rho)$$

where

$$L_D(\rho) := \sum_i \gamma_i \left(c_i \rho c_i^\dagger - \frac{1}{2} c_i^\dagger c_i \rho - \frac{1}{2} \rho c_i^\dagger c_i \right)$$

for some operators c_i, positive numbers γ_i and the system Hamiltonian H (the γ_i's may be absorbed into the c_i's). The time evolution of the system is then given by a semigroup of completely-positive trace preserving maps $T_t = \exp(tL)$, transforming the initial state of the system $\rho(0)$ into the state $\rho(t) = T_t(\rho(0))$ at time $t \geq 0$. More information on how one derives such equations can be found in [1]. In this lecture we will follow the discussion in [4] which identifies and discusses subspaces of the system Hilbert space which are untouched or nearly untouched by decoherence. For this, we restrict our attention to the case where the system Hilbert space $\mathcal{H}$ is of finite dimension N, i.e. $\mathcal{H} \cong \mathbb{C}^N$ and assume that the number of operators c_i in the sum equals $M \leq N^2 - 1$ (without loss of generality $\gamma_i > 0$).

A *decoherence-free subspace* $\tilde{\mathcal{H}}$ of $\mathcal{H}$ is a subspace that satisfies $L_D(\rho) = 0$ for all $\rho \in \mathcal{S}(\tilde{\mathcal{H}})$, the density operators on $\tilde{\mathcal{H}}$. Note that such a subspace may still be affected by decoherence since the unitary dynamics induced by H does not necessarily preserve this subspace. But for the moment we can think of $H = 0$ and will discuss effects coming from non-vanishing H later. We now want to find a classification of decoherence free subspaces, but before we do so we need to introduce a technical condition to rid us of some cumbersome cases. We say that a decoherence-free subspace is *generic* if it does not depend on the parameters γ_i.

We have the following characterisation of such subspaces

Theorem 1. *$\tilde{\mathcal{H}}$ is a generic decoherence-free subspace of $\mathcal{H}$ if and only if there are numbers β^i such that for all i and $|v\rangle \in \tilde{\mathcal{H}}$:*

$$c_i \left|v\right\rangle = \beta^i \left|v\right\rangle .$$

Proof. Let $\{|k\rangle\}_{k=1}^{\dim \tilde{\mathcal{H}}}$ be an orthonormal basis for $\tilde{\mathcal{H}}$ and $\{|k\rangle\}_{k=\dim \tilde{\mathcal{H}}+1}^{\dim \mathcal{H}}$ be an orthonormal basis for the orthogonal complement of $\tilde{\mathcal{H}}$ in $\mathcal{H}$. Since the subspace is generic it must hold that for every i and every $\rho \in \mathcal{S}(\tilde{\mathcal{H}})$ (and hence also every $\rho \in M(\tilde{\mathcal{H}})$, the matrices on $\tilde{\mathcal{H}}$):

$$c_i \rho c_i^\dagger - \frac{1}{2} c_i^\dagger c_i \rho - \frac{1}{2} \rho c_i^\dagger c_i = 0 \tag{1}$$

Let us write

$$c_i \left|k\right\rangle = \sum_{k'=1}^{\dim \mathcal{H}} \beta^i_{k,k'} \left|k'\right\rangle$$

and consider $\rho = |k\rangle \langle l|$ for $1 \leq k, l \leq \dim \tilde{\mathcal{H}}$. Then (1) equals

$$\sum_{k',k'',l',l''=1}^{\dim \mathcal{H}} \left(\beta^i_{k,k'} \bar{\beta}^i_{l,l'} \left|k'\right\rangle \left\langle l'\right| - \frac{1}{2} \bar{\beta}^i_{k',k''} \beta^i_{k,k'} \left|k''\right\rangle \left\langle l\right| - \frac{1}{2} \bar{\beta}^i_{l,l'} \beta^i_{l',l''} \left|k\right\rangle \left\langle l''\right| \right) = 0.$$

Consider the case, where $k = l$, choose $\tilde{k} \neq k$ and apply the function $\left\langle \tilde{k} \right| \cdot \left| \tilde{k} \right\rangle$ to the equation. This gives $|\beta_{k,\tilde{k}}|^2 = 0$. Hence $\beta^i_{k,k'} = \beta^i_k \delta_{k,k'}$ which, when inserted into (1) implies

$$\beta^i_k \bar{\beta}^i_l \left|k\right\rangle \left\langle l\right| - \frac{1}{2} \bar{\beta}^i_k \beta^i_k \left|k\right\rangle \left\langle l\right| - \frac{1}{2} \bar{\beta}^i_l \beta^i_l \left|k\right\rangle \left\langle l\right| = 0.$$

Equivalently,

$$\frac{\bar{\beta}^i_k}{\bar{\beta}^i_l} + \frac{\beta^i_l}{\beta^i_k} = 2.$$

Setting $z := \frac{\bar{\beta}_k^i}{\bar{\beta}_l^i}$ this equation becomes $z + \frac{1}{\bar{z}} = 2$ which has the unique solution $z = 1$. This shows that β_k^i is independent of k and hence

$$c_i \left|k\right\rangle = \beta^i \left|k\right\rangle$$

for all $1 \leq k \leq \dim \tilde{\mathcal{H}}$. □

Note that this implies that $[c_i, c_j] \left|v\right\rangle = 0$, a property which allows us to build a Lie algebra out of the c_i's and formulate this in Lie theoretic terms. Let $\mathcal{L}$ be *Lie closure* of the c_i's. The Lie closure is the span of the set of elements that is obtained by repeated application of the commutator to the c_i's, i.e.

$$\mathcal{L} := \operatorname{span}_{\mathbb{R}}\{c_1, c_2, \cdots, c_M, [c_1, c_2], \cdots, [c_1, [c_1, c_2], \cdots\}.$$

Equipped with the commutator as Lie bracket this is easily seen to be a Lie algebra[1], since the c_i's are matrices for which the Jacobi-identity holds.

Corollary 2. *$\tilde{\mathcal{H}}$ is a generic decoherence-free subspace of $\mathcal{H}$ if and only if $\tilde{\mathcal{H}}$ decomposes under the action of $\mathcal{L}$ into* $\dim \tilde{\mathcal{H}}$ *copies of the same one-dimensional irreducible representation*[2] *π of $\mathcal{L}$, i.e. $\mathcal{H} \cong \bigoplus_{j=1}^{\dim \tilde{\mathcal{H}}} \pi_j$, where $\pi_j \cong \pi$ for all j.*

Proof. It is clear that every $\left|v\right\rangle \in \tilde{\mathcal{H}}$ forms a (one-dimensional) invariant subspace under the action $\mathcal{L}$. Furthermore, the action is identical for every $\left|v\right\rangle$. □

Let us now look at two characteristic models of decoherence:

- (total decoherence) In total decoherence, $\mathcal{L} = su(N)$, the Lie algebra of $SU(n)$. There is no decoherence-free subspace. For $N = 2^K$, a basis for $su(N)$ is given by strings of K Pauli operators (in total $4^K - 1$ operators).
- (collective decoherence) Here we have $su(2)$ embedded into $su(2^K)$ by: $X \mapsto X \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1} + \mathbf{1} \otimes X \otimes \mathbf{1} \cdots \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{1} \cdots \otimes X$. For even K, the subspace $\tilde{\mathcal{H}} = \operatorname{span}\{\pi \left|01 - 10\right\rangle^{\otimes K/2}, \pi \in S_K\}$ is decoherence free.

The latter example illustrates why Lidar et al. call elements in the decoherence-free subspace *singlets*.

[1] A Lie algebra is a vector space $\mathcal{L}$ over a field F (here $\mathbb{R}$ or $\mathbb{C}$) equipped with a binary operation $[\cdot, \cdot] : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ that satisfies for all $x, y, z \in \mathcal{L}$ and $\alpha, \beta \in F$

- bilinearity: $[\alpha x + \beta y, z] = \alpha[x, z] + \beta[y, z]$ and $[z, \alpha x + \beta y] = \alpha[z, x] + \beta[z, y]$
- alternating: $[x, x] = 0$
- Jacobi identity: $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$

[2] A representation t of $\mathcal{L}$ is a homomorphism $t : \mathcal{L} \to \operatorname{End}(V)$ that preserves the Lie bracket $[t(A), t(B)] = t([A, B])$ for all $A, B \in \mathcal{L}$. The dimension of t is the dimension of V. t is *irreducible* if V contains no invariant subspace $0 \neq W \subsetneq V$.

1.2 Effect of system Hamiltonian

We now want to consider in how far a system Hamiltonian $H \neq 0$ effects a decoherence-free subspace. Note that even though the evolution under H is unitary, it may not preserve the decoherence-free subspace: states encoded into the decoherence free subspace may be transferred by the time evolution under the system Hamitonian outside this subspace where they are subject to decoherence. We will now show that this effect is rather small. Without loss of generality, it will suffice to study this effect for pure states. We use the fidelity in order to quantify how close the initial state $\rho(0) = |v\rangle\langle v|$ and final state of this evolution $\rho(t)$ are:[3]

$$F(\rho(0), \rho(t)) := (\mathrm{tr}\sqrt{\sqrt{\rho(0)}\rho(t)\sqrt{\rho(0)}})^2 = \mathrm{tr}|v\rangle\langle v|\rho(t).$$

The initial state $\rho(0)$ is perfectly preserved if and only if $F(\rho(0), \rho(t)) = 1$. Inserting $\rho(t) = \exp(tL)(|v\rangle\langle v|)$ and using the Tayler expansion of the exponential we find

$$F(t) = \sum_{n=0}^{\infty} \frac{t^n}{n!}\mathrm{tr}|v\rangle\langle v|L^n(|v\rangle\langle v|) = \sum_{n=0}^{\infty} \frac{1}{n!}\left(\frac{t}{\tau_n}\right)^n$$

where we defined

$$\tau_n = (\mathrm{tr}|v\rangle\langle v|L^n(|v\rangle\langle v|))^{-1/n}.$$

The first order decoherence rate is

$$\frac{1}{\tau_1} = \mathrm{tr}\rho(0)L(\rho(0)) = (-i)\mathrm{tr}\rho(0)[H, \rho(0)] = -i(\mathrm{tr}\rho(0)H\rho(0) - \mathrm{tr}\rho(0)\rho(0)H) = 0,$$

by the cyclic property of the trace. The decoherence free subspace is thus only effected to second order by the system Hamiltonian.

Likewise one can show that weak symmetry breaking decoherence operators only have a second order effect [4]. This small decoherence could then be suppressed by the active error correction schemes discussed in Renato Renner's lecture.

1.3 Collective Decoherence

In order to study the collective decoherence model introduced above, we start by recalling some representation theory of $su(2)$.

1.3.1 Representations of $su(2)$

Note that representations of $su(2)$ extend linearly to the complexification

$$su(2)_{\mathbb{C}} := su(2) \oplus isu(2) \cong sl(2) = \{\text{2x2 complex traceless matrices}\}.$$

[3] Unfortunately, some people define the fidelity with and some without the square

It is often convenient to consider $su(2)_{\mathbb{C}}$ instead of $su(2)$ since it can be given a somewhat nicer basis in terms of the raising and lowering operators and the Pauli-σ_z matrix:

$$\sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We now quickly recall the irreducible representations of $su(2)$. For each $j \in \{0, \frac{1}{2}, 1, \frac{3}{2}, \cdots\}$, there is a $2j+1$ dimensional irreducible representation, in the physics literature known as spin-$\mathbf{j}$ representation. We define this representation by its action on the $2j+1$ orthonormal basis states $\{|j,m\rangle\}_{m=-j}^{j}$.

$$\begin{aligned} \sigma_- |j,m\rangle &= \sqrt{j(j+1)-m(m+1)}\,|j,m+1\rangle \\ \sigma_+ |j,m\rangle &= \sqrt{j(j+1)-m(m-1)}\,|j,m-1\rangle \\ \sigma_z |j,m\rangle &= 2m\,|j,m\rangle\,. \end{aligned}$$

The decomposition of two irreducible representations of $su(2)$ is known as the Clebsch-Gordan decomposition. In terms of the vector spaces, the decomposition reads

$$\mathbf{j_1} \otimes \mathbf{j_2} \cong \bigoplus_{j=|j_1-j_2|}^{j_1+j_2} \mathbf{j} \tag{2}$$

and in terms of the basis elements we find

$$|j,m\rangle = \sum_{m_1,m_2} c_{j_1,j_2,j}^{m_1,m_2,m}\,|j_1,m_1\rangle\,|j_2,m_2\rangle\,. \tag{3}$$

with the *Clebsch-Gordan coefficients* $c_{j_1,j_2,j}^{m_1,m_2,m}$ (see your favourite QM textbook for more details).

Applying the Clebsch-Gordan decomposition iteratively onto $\frac{\mathbf{1}}{\mathbf{2}}^{\otimes n}$ we find:

$$\begin{aligned} \frac{\mathbf{1}}{\mathbf{2}}^{\otimes n} &\overset{(2)}{\cong} (\mathbf{0} \oplus \mathbf{1}) \otimes \frac{\mathbf{1}}{\mathbf{2}}^{\otimes(n-2)} \\ &\cong \left(\mathbf{0} \otimes \frac{\mathbf{1}}{\mathbf{2}} \oplus \mathbf{1} \otimes \frac{\mathbf{1}}{\mathbf{2}}\right) \otimes \frac{\mathbf{1}}{\mathbf{2}}^{\otimes(n-3)} \\ &\overset{(2)}{\cong} \left(\frac{\mathbf{1}}{\mathbf{2}} \oplus \left(\frac{\mathbf{1}}{\mathbf{2}} \oplus \frac{\mathbf{3}}{\mathbf{2}}\right)\right) \otimes \frac{\mathbf{1}}{\mathbf{2}}^{\otimes(n-3)} \\ &\cong \left(\frac{\mathbf{1}}{\mathbf{2}} \otimes \mathbb{C}^2 \oplus \frac{\mathbf{3}}{\mathbf{2}}\right) \otimes \frac{\mathbf{1}}{\mathbf{2}}^{\otimes(n-3)} \\ &\vdots \\ &\cong \bigoplus_j \mathbf{j} \otimes \mathbb{C}^{m_j^n}\,. \end{aligned}$$

1.3.2 Size of decoherence free subspace

Since $\mathbf{0}$ is the trivial representation of $su(2)$, the dimension of the decoherence-free subspace is – according to Corollary 2 – m_0^n. In order to estimate this number, let us first compute a recursion formula for m_j^n and start by noting that n even implies $m_j^n = 0$ for j half-integer and n odd implies $m_j^n = 0$ for j integer. It is also clear that $m_j^n = 0$ for $2j > n$. Assume

$$\frac{\mathbf{1}}{\mathbf{2}}^{\otimes n} \cong \bigoplus_{j=0}^{n} \mathbf{j} \otimes \mathbb{C}^{m_j^n}$$

then

$$\begin{aligned}\frac{\mathbf{1}}{\mathbf{2}}^{\otimes (n+1)} &\cong \bigoplus_{j} \mathbf{j} \otimes \frac{\mathbf{1}}{\mathbf{2}} \otimes \mathbb{C}^{m_j^n} \\ &\cong \bigoplus_{j} \left((\mathbf{j} + \frac{\mathbf{1}}{\mathbf{2}}) \oplus (\mathbf{j} - \frac{\mathbf{1}}{\mathbf{2}}) \right) \otimes \mathbb{C}^{m_j^n} \\ &\cong \bigoplus_{j} \mathbf{j} \otimes \mathbb{C}^{m^n_{j-\frac{1}{2}} + m^n_{j+\frac{1}{2}}}\end{aligned}$$

where we defined $m^n_{-\frac{1}{2}} = 0$ for all n. We find that for even n and integral j (and for odd n with half-integral j):

$$m_j^{n+1} = m^n_{j-\frac{1}{2}} + m^n_{j+\frac{1}{2}}.$$

The multiplicities then follow from this formula and the base case $m_j^1 = \delta_{j,\frac{1}{2}}$ and are[4]

$$m_j^n = \binom{n}{\frac{n}{2} - j} \frac{2j+1}{\frac{n}{2} + 2j + 1}. \tag{4}$$

[4] Consider $0 \leq 2j < n$ with $n \mod 2 = 2j \mod 2$ and define

$$m_j^n := \binom{n}{\frac{n}{2} - j} - \binom{n}{\frac{n}{2} - j - 1},$$

and $m^n_{\frac{n}{2}} = 1$ (and zero otherwise). With this definition, the m_j^n satisfy the recursion relation since

$$\begin{aligned} m^n_{j-\frac{1}{2}} + m^n_{j+\frac{1}{2}} &= \binom{n}{\frac{n}{2} - (j - \frac{1}{2})} - \binom{n}{\frac{n}{2} - (j - \frac{1}{2}) - 1} + \binom{n}{\frac{n}{2} - (j + \frac{1}{2})} - \binom{n}{\frac{n}{2} - (j + \frac{1}{2}) - 1} \\ &= \left[\binom{n}{\frac{n+1}{2} - j} + \binom{n}{\frac{n+1}{2} - j - 1} \right] - \left[\binom{n}{\frac{n+1}{2} - j - 1} + \binom{n}{\frac{n+1}{2} - j - 1 - 1} \right] \\ &\overset{Pascal}{=} \binom{n+1}{\frac{n+1}{2} - j} - \binom{n+1}{\frac{n+1}{2} - j - 1} \\ &= m_j^{n+1} \end{aligned}$$

where we used Pascal's rule.

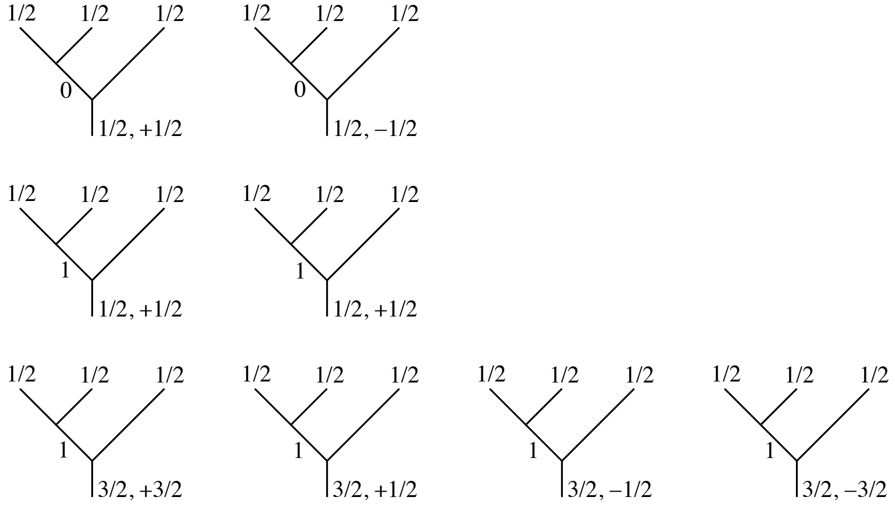
Consider even n and note that $m_0^n \geq m_j^n$ for all j. In total there are exactly $n{+}1$ different values of j, hence $2^n \leq m_0^n(n{+}1)$. This implies that the size of the decoherence-free subspace (counted in number of qubits is) is lower bounded by $\log m_0^n \geq n - \log(n+1)$. For large n, the number of logical qubits per physical qubits is therefore

$$\frac{\#\text{ logical qubits}}{\#\text{ physical qubits}} = \lim_{n\to\infty} \frac{1}{n} \log m_0^n \geq \lim_{n\to\infty} \left(1 - \frac{\log(n+1)}{n}\right) = 1.$$

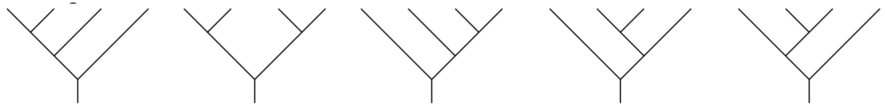
Alternatively, one can use Stirling's approximation in order to derive this result.

1.3.3 Basis for decoherence-free subspace

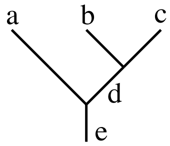
We have seen in the exercise that a (rather ad hoc) basis for the decoherence-free subspace is given by $\{\pi\,|01-10\rangle^{\otimes n/2}, \pi \in S_n\}$. This basis is a little inconvenient, since the vectors are not orthonormal. We obtain an orthonormal basis by following again the Clebsch-Gordan decomposition and recalling whether we increased or decreased the spin in each step. We can then label the basis vectors by the following trees (here for n=3):



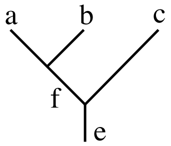
As an example, note that the basis vector with the sequence of intermediate labels $0, \frac{1}{2}, 0, \frac{1}{2}, \cdots, 0$ is given by $|01-10\rangle^{\otimes n/2}$. Of course we could have performed the decomposition in other orders:



The transition between the different bases (which is independent of the label m, which we therefore omit) has at its main building block the following equation, known as *recoupling move.*



$$= \sum_f \left[\begin{array}{ccc} a & b & f \\ c & e & d \end{array} \right]$$



The matrix elements (known as Wigner 6j coefficients) can be expressed in terms of the Clebsch-Gordan coefficients (also known as Wigner 3j coefficients), as we can accomplish the basis transform as two inverse Clebsch-Gordan transforms following by two Clebsch-Gordan transforms.

1.3.4 Computation in the decoherence-free subspace

Up to now we have considered the decoherence-free subspace as a quantum memory and have disregarded the problem of performing computation on the logical qubits. When we perform computation, we would naturally like to perform it by *local* operations on the physical qubits. But in general, this will mean that our operations will take us out of the decoherence-free subspace, unless our operations commutes with the the action of the Lie algebra. As an example, let us consider the case of collective decoherence with $n = 2$: the unitary operators U that commute with the action of $su(2)$

$$A \to A \otimes \mathbf{1} + \mathbf{1} \otimes A$$

are easily seen to be either the identity operator or the *flip operator* (or transposition) defined via its action $F |i\rangle |j\rangle = |j\rangle |i\rangle$. This example generalises to arbitrary n, where the unitaries that commute with the action of $su(2)$ can be written as linear combinations of the permutations of n elements acting naturally on $(\mathbb{C}^2)^{\otimes n}$.[5] It is easy to see how the action of S_n acts on the nonorthogonal basis states $\{\pi |01 - 10\rangle^{\otimes n/2}, \pi \in S_n\}$. In order to express this action in the

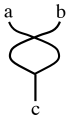
[5] More precisely, the action of the symmetric group S_n is given by

$$\pi |i_1 \dots i_n\rangle = \left| i_{\pi^{-1}(1)} \cdots i_{\pi^{-1}(n)} \right\rangle .$$

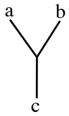
This is a representation of S_k since

$$\begin{aligned} \pi' \pi |i_1 \dots i_n\rangle &= \pi' \left| i_{\pi^{-1}(1)} \cdots i_{\pi^{-1}(n)} \right\rangle \\ &=: \pi' |j_1 \dots j_n\rangle \\ &= \left| j_{\pi'^{-1}(1)} \cdots j_{\pi'^{-1}(n)} \right\rangle \\ &=: |j_{\ell_1} \cdots j_{\ell_n}\rangle \\ &= \left| i_{\pi^{-1}(\ell_1)} \cdots i_{\pi^{-1}(\ell_n)} \right\rangle \\ &= \left| i_{\pi^{-1}(\pi'^{-1}(1))} \cdots i_{\pi^{-1}(\pi'^{-1}(n))} \right\rangle \\ &= \left| i_{(\pi'\pi)^{-1}(1)} \cdots i_{(\pi'\pi)^{-1}(n)} \right\rangle . \end{aligned}$$

orthogonal *tree basis* that we have introduced one observes that



$$= (-1)^{a+b-c}$$



We may check the phase factor with the example $a = b = \frac{1}{2}$. For $c = 0$ we have the singlet state with a phase of -1 and for $c = 1$ the triplet state with the trivial phase 1.

If we consider the left standard basis and want to permute particle one and two we can simply apply the above rule and obtain the transformed state. If we want to permute particle two and three we first need to perform a recoupling move to the basis where particles two and three fuse directly, then perform the permutation and subsequently undo the recoupling move in order to return to the left standard basis.

Since there are only $n!$ different permutations but an infinite number of unitary transformations a quantum computer could perform on the encoded qubits, universal quantum computation is not possible by permutation alone. For more information on this *permutational quantum computer* see [2].[6]

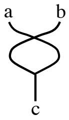
The deeper reason for the permutation group arising lies in the fact that the particles that we considered arose as representations of $SU(2)$ which is the double cover of the three dimensional rotation group $SO(3)$. Since this is a fundamental reason reason and not one that arose from our specific particle model, the only way out is to consider two-dimensional or quasi-two-dimensional models. An alas, here permutations turn out to be more interesting and in some cases allow for universal quantum computation. This is the topic of topological quantum computation.

2 Topological Quantum Computer

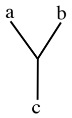
2.1 Particles in two and three dimensions

When we exchange two particles twice in clockwise direction this corresponds to winding one particle around the other. As a physical operation this operation should have a unitary matrix as its mathematical equivalent. In three space dimensions, however, the path winding one particle around the other is easily seen to be contractible to the trivial path that leaves both particles where they are. This implies that the unitary matrix corresponding to a double particle exchange must equal the identity matrix and this again shows that the unitary matrix representing particle exchange can only have eigenvalues one and minus one. And indeed this is what we had found above

[6] I also thank Stephen Jordan for letting me use his figures.



$$= (-1)^{a+b-c}$$



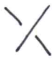
This argument can be related to a rotation around itself and the double cover $SU(2)$ of the rotation group $SO(3)$, but we will not discuss this connection in more detail in this course. The interested reader is referred to John Preskill's lecture notes and his remarks about the relation between spin and statistics.

Interestingly, particle exchange is different in two dimensions. Here, a path of one particle around the other cannot be deformed into the trivial path and hence does not have to be represented by the identity matrix. In consequence, particle exchange in a two-dimensional world may be represented by a unitary matrix that does not only have eigenvalues one or minus one (or equivalently exchange phases of 0 or π) but may have *any* phase. In analogy to bosons and fermions, such particles are called anyons.

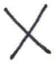
In our three-dimensional world we cannot hope to have elementary particles that behave like anyons, even if we confine them two a two-dimensional surface since we could always remove the confinement. In certain materials, however, we may hope to see quasi-particles (or excitations) that behave like anyons.

2.2 The braid group

So what could we do if we had anyons at our hand? We have argued above that exchanging anyons twice in the same direction, for instance clockwise, is not the same as doing nothing. In other words, exchanging particles clockwise or counterclockwise may make a difference in two spatial dimensions. We may therefore represent a clockwise exchange of particles by the following diagram



which replaces our particle exchange in the three-dimensional world where clockwise and counterclockwise exchange were identical.



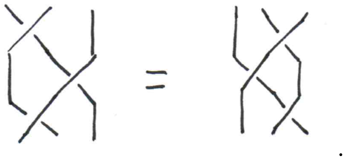
In three dimensions, the exchange of n particles was governed by the symmetric group S_n acting on n strands - in two dimensions the relevant group is the braid group B_n. Let τ_i, $i = \{1, \ldots, n-1\}$ be the generators of the braid group on n strands exchanging strand i and $i+1$ in clockwise manner. The braid group is then characterised by the following set of algebraic relations: When two exchanges act on entirely different strands then

$$\tau_i \tau_j = \tau_j \tau_i \qquad |i-j| \geq 2 \tag{5}$$

whereas when they have a strand in common the following relation holds

$$\tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1} \tag{6}$$

Represented graphically for three-strand braids it reads

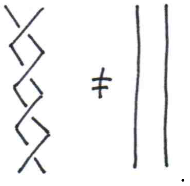


Note that the symmetric group has one relation in addition, namely

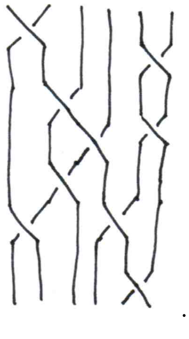
$$(\tau_i)^2 = e \tag{7}$$

where e is the identity element.

Since the symmetric group S_n has only $n!$ different elements we had seen above that exchanging particles in three dimensions cannot lead to a universal model for quantum computation. This argument does not hold anymore for particles in two dimensions since we can easily see that the braid group B_n has an infinite number of elements. Even for two strands every additional exchange of the strands (in the same direction) results in a new braid.



So there is the hope that we may perform universal quantum computation (or at least a very good approximation of it, since with a discrete number of braids we can certainly not get an arbitrary unitary exactly) by braiding particles with a circuit looking like this:



But in order to have a quantum mechanical particle model, it is not sufficient to play around with strands. We need a representation of the braid group. Let us recall how we obtained the representations of the symmetric group in the attempt to generalise this approach. Here, each strand was represented by a vector space $V \cong \mathbb{C}^2$ (we disregard that this space was endowed with an action of $SU(2)$) and the symmetric group was acting as

$$S_n \ni \pi_i \mapsto \underbrace{\mathbf{1} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1}}_{i-1} \otimes \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes \underbrace{\mathbf{1} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1}}_{n-(i+1)}$$

when expressed in terms of the computational basis. This action may easily be generalised to arbitrary local dimensions. Since it is a representation of S_n, the matrices fulfill equations (5) (6) and (7). It is then natural to ask if we can find a modification of

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

that violates (7), but still satisfies (5) and (6)? In other words, can we find a non-trivial representation of the braid group by deforming particle exchange? Formally, we are looking for an element $b : V \otimes V \to V \otimes V$ that satisfies the following equation, known as the Yang-Baxter equation

$$b_{12}b_{23}b_{12} = b_{23}b_{12}b_{23}. \tag{8}$$

Each side of the equation acts on $V \otimes V \otimes V$ and the subscript of b indicates on which two tensor factors b acts.[7] It is indeed possible to find representations

[7] Sometimes, the following different equation is called the Yang-Baxter equation

$$R_{23}R_{13}R_{12} = R_{12}R_{13}R_{23}, \tag{9}$$

where $R : V \otimes V$. The element b and R are then related by a permutation:

$$b = \pi R$$

where π is the exchange operator on $V \otimes V$, i.e.

$$\pi = \sum_{k,l} |l\rangle \langle k| \otimes |k\rangle \langle l|$$

It remains to verify that (8) is equivalent to (9)

$$b_{12}b_{23}b_{12} = b_{23}b_{12}b_{23}$$

The LHS equals

$$\begin{aligned} b_{12}b_{23}b_{12} &= \pi_{12}R_{12}\pi_{23}R_{23}\pi_{12}R_{12} \\ &= \pi_{12}R_{12}\pi_{23}\pi_{12}R_{13}R_{12} \\ &= \pi_{12}\pi_{23}R_{13}\pi_{12}R_{13}R_{12} \\ &= \pi_{12}\pi_{23}\pi_{12}R_{23}R_{13}R_{12} \\ &= \pi_{13}R_{23}R_{13}R_{12}. \end{aligned}$$

of the braid group this way, but unfortunately this is not so easy. We therefore choose a different route: we will build anyon models directly.

2.3 The Toric Code

2.3.1 The model

The toric code is arguably the simplest nontrivial anyon model and can be given an explicit representation in a lattice model with the anyons corresponding to excitations in the model.

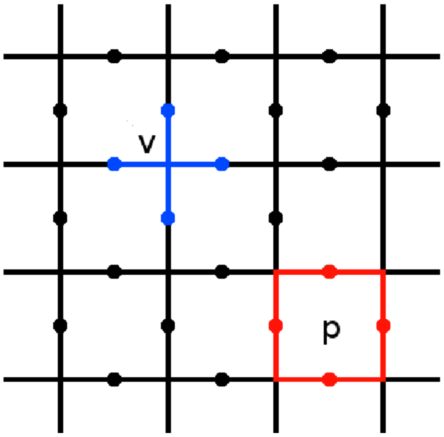


Figure 1: The Toric Code. Graphic by James Wootton via Wikipedia `http://en.wikipedia.org/wiki/Toric_code`

Consider a square lattice as depicted in Figure 2.3.1 where we put a qubit on each edge, i.e. consider local basis states $\{|0\rangle, |1\rangle\}$. For the moment we do not worry about the boundary conditions and consider for each vertex v in the lattice the local operator

$$A_v = \prod_{i \in v} \sigma_x^{(i)}$$

where the product extends over all edges adjacent to the vertex v and the operator $\sigma_x^{(i)}$ acts as σ_x on site i and as identity on all other sites. Similarly, we

The RHS equals

$$\begin{aligned} b_{23} b_{12} b_{23} &= \pi_{23} R_{23} \pi_{12} R_{12} \pi_{23} R_{23} \\ &= \pi_{23} R_{23} \pi_{12} \pi_{23} R_{13} R_{23} \\ &= \pi_{23} \pi_{12} R_{13} \pi_{23} R_{13} R_{23} \\ &= \pi_{23} \pi_{12} \pi_{23} R_{23} R_{13} R_{23} \\ &= \pi_{13} R_{23} R_{13} R_{23} \end{aligned}$$

and hence the statement is equivalent to (9).

consider for each plaquette p the operator

$$B_p = \prod_{j \in p} \sigma_z^{(j)}$$

where the sum extends over all edges j adjacent to the plaquette p. It is easy to see that all these operators commute: clearly all vertex operators commute with each other since they only contain σ_x operators. The same is true for the plaquette operators which only contain σ_z operators. A_v and B_p also commute if v and p do not have a common edge. But note that if they have a common edge, they actually have two! In this case

$$\begin{aligned} A_v B_p &= \sigma_x^{(1)} \sigma_x^{(2)} \sigma_x^{(3)} \sigma_x^{(4)} \sigma_z^{(3)} \sigma_z^{(4)} \sigma_z^{(5)} \sigma_z^{(6)} && (10) \\ &= \sigma_z^{(3)} \sigma_z^{(4)} \sigma_z^{(5)} \sigma_z^{(6)} \sigma_x^{(1)} \sigma_x^{(2)} \sigma_x^{(3)} \sigma_x^{(4)} && (11) \\ &= B_p A_v && (12) \end{aligned}$$

since we have to commute the operators on edges 3 and 4, and thus have two minus signs which cancel each other. The operators A_v and B_p can be considered as stabilizer operators for a code. The subspace of the code is given by the vectors $|\psi\rangle$ which satisfy

$$\begin{aligned} A_v |\psi\rangle &= |\psi\rangle \\ B_p |\psi\rangle &= |\psi\rangle \end{aligned}$$

for all v and p. We can also interpret these states as ground states of the following Hamiltonian

$$H = -\sum_v A_v - \sum_p B_p.$$

If we identify parallel borders of the square lattice, we have a model that lives on a torus and this is what gives our code its name. The ground state subspace turns out to be four-dimensional as we will see in a moment.

2.3.2 Quasi-particle excitations

Excited states of this model correspond to violations of the vertex or plaquette conditions. Since these are local conditions, excitations can be considered as (quasi-)particles in the model. That is, if for a vertex v, the stabilizer condition is violated,

$$A_v |\phi\rangle = - |\phi\rangle \, ,$$

we say that we have an "electronic particle" and if for a plaquette p,

$$B_p |\phi\rangle = - |\phi\rangle \, ,$$

we have a "magnetic particle". If several conditions are violated we have several particles in the model.

Particles can be moved around with ribbon operators. In order to move an electric particle from edge e_0 to edge e_1 consider a path r in the lattice connecting e_0 and e_1 and apply the associated operator

$$R_r = \prod_{i \in r} \sigma_z^{(i)}.$$

Likewise, in order to move a magnetic particle which lives on the dual lattice from e_0^* to e_1^* apply

$$R_{r^*} = \prod_{i \in r^*} \sigma_x^{(i)}.$$

where r^* is a path from e_0^* to e_1^* in the dual lattice. If r is a loop, then R_r does not excite the system, since every A_v has an even number vertices in common with R_r (and similarly for p^*).

Trivial loops in the lattice do not affect the ground states (since they can be written as a product of B_p's, whereas loops that wrap around the torus do. In particular, R_r and R_{r^*} anticommute if they wrap around the torus in different directions, since they have an odd number of edges in common. This shows that the ground state is at least two dimensional. This is in fact the correct dimension and more generally a surface of genus g supports $2g$ qubits in its ground state. Hence, the ground state degeneracy is a topological property of the code.

Before we continue to discuss the properties of the particles, let us pause for the moment and analyse the resilience of the code against errors. Note that we can still detect the excitations by measuring the stabilizer operators and thus undo the corresponding errors. Only if a pattern of σ_x errors happened that wraps around the torus are we unable to detect it and a logical error happened in the code. Considering a model of independent errors, the probability of this is exponentially small in the thickness of the torus and thus provides a rather stable code.

We are now in the position to analyse particle exchange (braiding) in this model. We do this by

- creating two pairs of particles from the ground state (vacuum)
- move one particle from one pair around one particle from the other pair
- annihilating the pairs again

If both pairs consist of electric particles,

$$R_l R_r R_{r'} |\psi\rangle = R_r R_{r'} R_l |\psi\rangle = R_r R_{r'} |\psi\rangle$$

where l is a loop of the particle at e_0 around the particle at e_0'. The operators commute since they all consist of σ_z operators. A similar argument holds if both pairs are of magnetic type.

If, however, the second pair is of magnetic type, then l will intersect r^* in an odd number of positions and therefore

$$R_l R_{r^*} = -R_{r^*} R_l$$

which implies

$$R_l R_r R_{r^*} \left|\psi\right\rangle = -R_r R_{r^*} R_l \left|\psi\right\rangle = -R_r R_{r^*} \left|\psi\right\rangle .$$

We can summarize the model in the following way:

The model has four types of particles, a trivial particle denoted by 1 which sits on an edge if there is no other particle, an electric one, e, a magnetic one, m, and a particle consisting of an electric and a magnetic particle, ψ. When the particles are combined or "fused" they obey the rules

$$\begin{aligned} 1\times 1 = 1, \qquad e\times 1 = e, \qquad m\times 1 = m, \qquad \psi\times 1 = \psi \\ e\times e = 1, \qquad m\times m = 1, \qquad \psi\times\psi = 1 \\ e\times m = \psi, \qquad \psi\times e = m, \qquad \psi\times m = e. \end{aligned} \tag{13}$$

In this sense, the particles are their own antiparticles and the trivial particle acts as the identity. We have seen that the electric particles are bosons with respect to each other and the magnetic ones as well. We have also seen that a double exchange of an electric charge around a magnetic one gives a phase of -1, hence a single exchange has a phase of i![8] Electric and magnetic particles have therefore nontrivial braiding with each other (they are neither bosons nor fermions with respect to each other). It will be an exercise to show that the ψ particles are fermions.

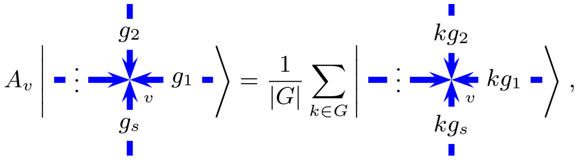
2.4 Kitaev's Quantum Double Models

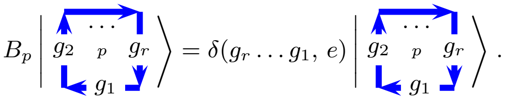
The particles in the Toric Code have Abelian statistics which means that their particle exchange can be described by phases only and does not need more general unitary matrices.[9] There is a nice generalisation of the toric code to so-called Quantum Double models which support non-Abelian anyons useful for universal quantum computation.[10]. Again we have a Hamiltonian on a square lattice with state space on each edge given by a basis that is labelled by the elements of a finite group G. The vertex operators are defined by their action on the adjacent vertices

[8] We may also chose $-i$.

[9] In this case, this is already clear even without analysing the braiding, since there is only one possible particle two particle can fuse to

[10] For a physical introduction to these models see Preskill's lecture notes on the non-abelian superconductor





Note that the edges are oriented. The orientation of an edge may be changed if at the same time g is changed into g^{-1}. As an exercise you may show that the Toric Code is a special case of this construction for $G = \mathbb{Z}_2$.[11] In general, the excitations of this model do not separate into electric and magnetic charges anymore, but only combined charges corresponding to a violation of a vertex constraint and the adjacent (to the top right) plaquette constraint.[12] They are labelled by the irreducible representations of the so-called quantum double $D(G)$ of the group. $D(G)$ is a Hopf algebra with certain nice properties and can be regarded as the symmetry of the model that is not accessible. Recalling our discussion of decoherence-free subspaces, the decoherence of our model is therefore described by $D(G)$ and the decoherence-free subspace by the trivial representation of $D(G)$ (the ground state with no particle). An anyon model that allows universal quantum computation (i.e. where through braiding we can approximate any unitary transformation) is given for $G = S_6$. For more information see [3].

2.5 General Anyon models

In general, an anyon model is given by the following set of data:

- *Particle types* are labeled by elements from a discrete (mostly finite) set.

- *Fusion rules* tell us the possibilities of the outcomes when two particles, k_1 and k_2, are fused.

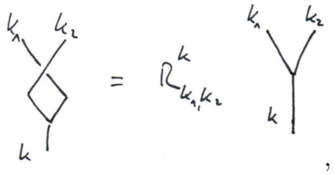
  $$k_1 \times k_2 = \sum_k N^k_{k_1,k_2} k$$

  where $N^k_{k_1,k_2}$ is the number of different ways in which two particles fuse to a particular third particle. Not to clutter our notation, we will only consider fusion rules where there is at most one way, i.e. $N^k_{k_1,k_2} \in \{0,1\}$.

- *Braiding rules* tell us what happens when particles are being exchanged. Braiding of two particles does not affect the particle to which they fuse, hence

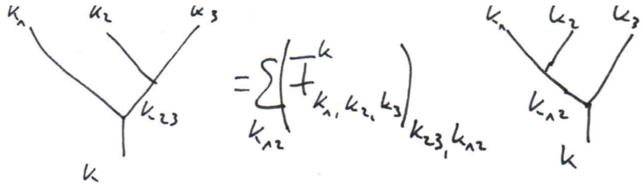
[11] In order to obtain the plaquette and vertex operators from the from the previous section, one needs to subtract an one half times the identity of each operator – a trivial change what concerns the properties of the model.

[12] In the toric code, such a combined excitation is the ψ-particle



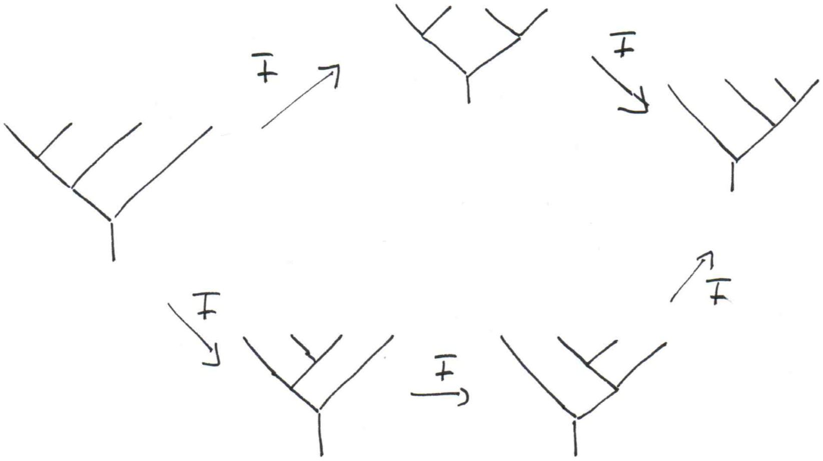
where $R^k_{k_1,k_2} = e^{i\Theta^k_{k_1,k_2}}$ is a phase factor.

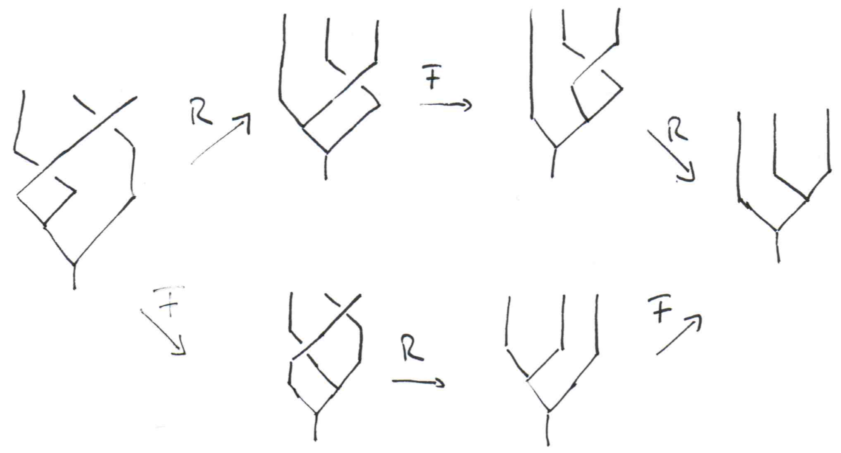
- The *F-matrix* relates the different orders in which particles can be fused.

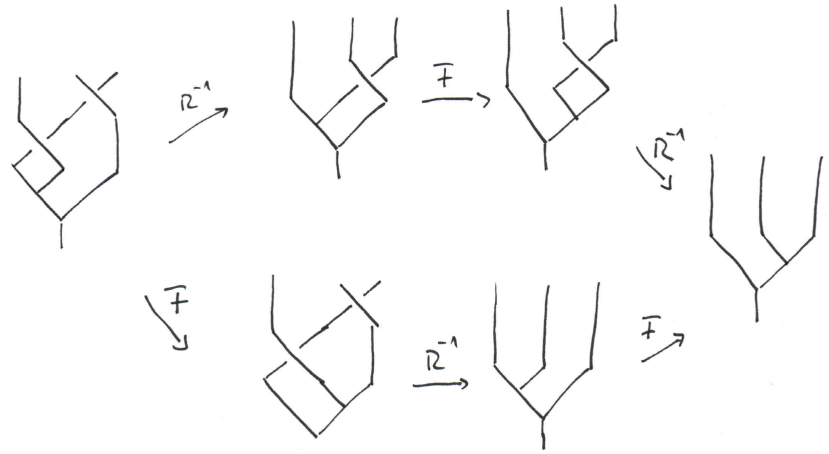


In the Toric Code these were trivial.

The following three equations – written in diagrammatic form and known as pentagon and hexagon equations – provide consistency conditions on the F and R-matrices.







MacLane's coherence theorem tells us that for an anyon model to be consistent it is sufficient that these three equations are satisfied.

Example 1. *Toric Code*

- *Particle types* $\{1, e, m, \psi\}$.
- *Fusion rules, see* (13).
- *The only interesting phase (i.e.* $\neq \pm 1$*) is* $R^{\psi}_{e,m} = i$.
- *F-Matrix not needed.*

Example 2. *SU*(2)

- *Particle types* $\{0, \frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\}$

- *Fusion rules*
$$j_1 \times j_2 = \sum_{j=|j_1-j_2|}^{j_1+j_2} j$$
- *Braiding rules* $R^{j}_{j_1,j_2} = (-1)^{j_1+j_2-j}$.
- *F-Matrix*
$$(F^{j}_{j_1,j_2,j_3})_{j_{23},j_{12}} = \begin{bmatrix} j_1 & j_2 & j_{12} \\ j_3 & j & j_{23} \end{bmatrix}.$$

The first example has nontrivial braiding but is abelian. The second example is non-abelian but has trivial braiding. The simplest non-abelian anyon model with nontrivial braiding that is furthermore universal for quantum computation is the Fibonacci model.

References

[1] H.-P. Breuer and F. Petruccione, *The theory of open quantum systems*, Oxford University Press, 2002.

[2] S. P. Jordan, *Permutational Quantum Computing*, Quantum Information and Computation, 10 (2010), pp. 0470–0497.

[3] A. Kitaev, *Fault-tolerant quantum computation by anyons*, Ann. Phys., 30 (2003), p. 3.

[4] D. A. Lidar, I. L. Chuang, and K. B. Whaley, *Decoherence-free subspaces for quantum computation*, Phys. Rev. Lett., 81 (1998), pp. 2594–2597.