MP 472 Quantum Information and Computation

http://www.thphys.may.ie/staff/jvala/MP472.htm

Outline

Open quantum systems

The density operator

Quantum noise (decoherence)

Quantum error correction
- CSS codes: example
- Introduction to stabilizer formalism

Fault-tolerant quantum computation
- principles of fault tolerance
- natural fault tolerance
- topological quantum computation

Hamming codes (review)

A good illustrative class of linear ECC (error correcting codes).

Suppose an integer $r \geqq 2$, let H be the matrix whose columns are all 2^r-1 bit strings of length r which are not identically 0. This parity check matrix defines $[2^r\text{-}1, 2^r\text{-}r\text{-}1]$ linear code known as a Hamming code.

Example

[7,4] code

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

He_j gives a binary representation of j.

Gilbert-Varshamov bound

Let an [n,k] code, with large n, be an ECC protecting against errors on t bits for some k

$$k/n \geq 1 - H(t/n)$$

where $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary Shannon entropy.

Calderbank-Shor-Steane (CSS) codes (review)

Dual construction of ECC

Let C be an [n,k] code with G and H, we can define another code, the dual of C, $C^{\perp}$, to be the code with the generator matrix H^T and the parity check matrix G^T.

Equivalently the dual of C consists of all codewords y s.t. y is orthogonal to all the codewords in C.

A code is said to be weakly self-dual if $C \subseteq C^{\perp}$, and
it is strictly self dual if $C = C^{\perp}$.

CSS Codes

Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes resp., such that $C_1 \subset C_2$ and both C_1 and $C_2^{\perp}$ can correct errors up to t bits. Then $CSS(C_1,C_2)$ is an $[n,k_1\text{-}k_2]$ code which can correct arbitrary error up to t qubits.

Furthermore, the error detection and recovery require only the application of Hadamard and CNOT gates, in each case a number of the gates is linear in the size of the code.

Steane code

A [7,4,3] Hamming code which is a simple example of a CSS code:

$$H(C) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$C_1 = C$ is the distance three code which can correct errors on 1 bit.

$C_2 = C^{\perp}$ is defined by the parity check matrix

$$H(C_2) = G(C_1)^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$C_2 \subset C_1$ (see Nielsen & Chuang for proof)

As $C_2^{\perp} = (C^{\perp})^{\perp} = C$, both codes are d=3 codes which can correct errors on 1 bit.

Since C_2 is a [7,4] code and C_1 is a [7,3] code, it follows that CSS(C_1,C_2) is a [7,1] quantum code which can correct arbitrary errors on a single qubit.

$$|0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}(|0000000\rangle+|1010101\rangle+|0110011\rangle+|1100110\rangle+ \\ + |0001111\rangle+|1011010\rangle+|0111100\rangle+|1101001\rangle)$$

$$|1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}(|1111111\rangle+|01010101\rangle+|1001100\rangle+|0011001\rangle+ \\ + |1110000\rangle+|0100101\rangle+|1000011\rangle+|0010110\rangle)$$

Introduction to stabilizer codes (additive codes)

Idea

$$|\psi\rangle = (1/2)^{1/2}(|00\rangle+|11\rangle)$$

$$\left.\begin{aligned} X_1X_2|\psi\rangle &= |\psi\rangle \\ Z_1Z_2|\psi\rangle &= |\psi\rangle \end{aligned}\right\} \quad |\psi\rangle \text{ is stabilized by } X_1X_2 \text{ and } Z_1Z_2$$

Quantum states can more easily be specified by the operators that stabilize them than working explicitly with quantum states.

Theory

The Pauli group G_n on n qubits.

Example G_1:

$$\{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

- this set forms a group under matrix multiplication

Definition:
Suppose S is a subgroup of G_n and let V_S be the set of n qubit states which are fixed by every element of S. V_S is a vector space stabilized by S, and S is said to be the stabilizer of the space V_S.

Introduction to stabilizer codes

Definition:

Suppose S is a subgroup of G_n and let V_S be the set of n qubit states which are fixed by every element of S. V_S is a vector space stabilized by S, and S is said to be the stabilizer of the space V_S.

Example:

n=3 qubits and S = {I, Z_1Z_2, Z_2Z_3, Z_1Z_3}

The subspace stabilized by: Z_1Z_2 is spanned by {|000>,|001>,|110>,|111>}.

Z_2Z_3 is spanned by {|000>,|100>,|011>,|111>}.

Z_1Z_3 is spanned by {|000>,|010>,|101>,|111>}.

The elements |000> and |111> are fixed by all the operators, so V_s is spanned by these states.

Clearly we can work with only two of the operators because e.g.

$Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$, and $(Z_1Z_2)^2 = I$.

The description in terms of these generators is convenient because we only need to show that the states are stabilized by the generators:

in this example, S = $\langle Z_1Z_2, Z_2Z_3 \rangle$.

What subgroup S of the Pauli group can be used as the stabilizer for a nontrivial V_S?

- two conditions need to be satisfied:
  (a) the elements of S commute;
  (b) –I is not an element of S.

Error correction using stabilizer codes

Suppose C(S) is a stabilizer code corrupted by an error $E \in G_n$:

If E anticommutes with an element of the stabilizer, then E takes C(S) to an orthogonal subspace, and th eerror can in principle be detected by projective measurement.

If $E \in S$, then E does not corrupt the state at all.

But the problem emerges from possibility that E commutes with all elements of S, but $E \notin S$, i.e. $Eg = gE$ for all $g \in S$.

Centralizer Z(S): the set $E \in G_n$ s.t. $Eg = gE$ all $g \in S$.

Normalizer N(S): the set $E \in G_n$ s.t. $EgE^+ \in S$;
- for any subgroup S of G not containing –I, N(S) = Z(S).

Theorem:
Let S be the stabilizer for a stabilizer code C(S). Suppose $\{E_j\}$ is a set of operators in G_n s.t. $E_j^+E_k \notin N(S) - S$ for all j and k. Then $\{E_j\}$ is a correctable set of errors for the code C(S).

Examples of stabilizer codes

Theorem:
Let S be the stabilizer for a stabilizer code C(S). Suppose $\{E_j\}$ is a set of operators in G_n s.t. $E_j^+E_k \notin N(S) - S$ for all j and k. Then $\{E_j\}$ is a correctable set of errors for the code C(S).

1) Three qubit bit flip code

is spanned by |000> and |111> with the stabilizer generated by Z_1Z_2 and Z_2Z_3 .

The error set is $\{I, X_1, X_2, X_3\}$

It is easy to show explicitly that every possible product of two elements of this set anticommutes with the stabilizer (except for I which is the element of S), so thus by the theorem above the error set forms a correctable set for the three qubit Bit flip code with the stabilizer $S = \langle Z_1Z_2, Z_2Z_3 \rangle$.

Error detection is carried by measuring the stabilizer generators.

If for example, the error X_1 occurred, then the stabilizer is transformed into $\langle -Z_1Z_2, Z_2Z_3 \rangle$, so the syndrom measurement gives the result -1 and +1. Similarly the error X_2 gives syndromes -1 and -1, and X_3 gives +1 and -1.

The original state is recovered by applying the inverse operation to the error Indicated by the error syndrome.

Examples of stabilizer codes

2) Shor's nine-qubit code

$$|0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}[(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)]$$

$$|1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}[(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)]$$

Stabilizer generators

g_1	Z	Z	I	I	I	I	I	I	I
g_2	I	Z	Z	I	I	I	I	I	I
g_3	I	I	I	Z	Z	I	I	I	I
g_4	I	I	I	I	Z	Z	I	I	I
g_5	I	I	I	I	I	I	Z	Z	I
g_6	I	I	I	I	I	I	I	Z	Z
g_7	X	X	X	X	X	X	I	I	I
g_8	I	I	I	X	X	X	X	X	X

It is easy to check that all single qubit errors form a correctable set of errors for this code.

For example, consider the errors X_1 and Y_4. Their product X_1Y_4 anticommutes with Z_1Z_2 and thus is not in N(S). Similarly, all other products of two errors from the error set of all single qubit errors for this code anticommute with at least one element of the stabilizer S, and thus are not in N(S).

This implies that the Shor code can be used to correct an arbitrary single qubit error.

Homework: Show that the encoded Z and X operations over the Shor code are realized by the operators $X_1X_2X_3X_4X_5X_6X_7X_8X_9$ and $Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9$ respectively.

Examples of stabilizer codes

3) Steane [7,1] code

$|0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}(|0000000\rangle+|1010101\rangle+|0110011\rangle+|1100110\rangle+$
$+ |0001111\rangle+|1011010\rangle+|0111100\rangle+|1101001\rangle)$

$|1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}(|1111111\rangle+|01010101\rangle+|1001100\rangle+|0011001\rangle+$
$+ |1110000\rangle+|0100101\rangle+|1000011\rangle+|0010110\rangle)$

To construct the stabilizer generators for a CSS(C_1,C_2) code, we first introduce a check matrix, which for CSS codes is formed as

$$\left(\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right)$$

The rows of this matrix correspond to the stabilizer generators g_1, …, g_l;
the left side of the matrix contains "1"s to indicate which generators contain Xs, and
the right side contains "1"s to indicate which generators contain Zs.
(In general case, the presence of "1"s on both sides indicates Ys in the generator.)

Example
the check matrix of
the Steane code

$C_1 = C$
$C_2 = C^{\perp}$

$$\left(\begin{array}{ccccccc|ccccccc} 0&0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 0&1&1&0&0&1&1&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right)$$

Examples of stabilizer codes

Steane [7,1] code

$|0\rangle \rightarrow |0_L\rangle = (1/2)^{3/2}(|0000000\rangle+|1010101\rangle+|0110011\rangle+|1100110\rangle+$
$+ |0001111\rangle+|1011010\rangle+|0111100\rangle+|1101001\rangle)$

$|1\rangle \rightarrow |1_L\rangle = (1/2)^{3/2}(|1111111\rangle+|01010101\rangle+|1001100\rangle+|0011001\rangle+$
$+ |1110000\rangle+|0100101\rangle+|1000011\rangle+|0010110\rangle)$

Stabilizer generators

g_1	I	I	I	X	X	X	X
g_2	I	X	X	I	I	X	X
g_3	X	I	X	I	X	I	X
g_4	I	I	I	Z	Z	Z	Z
g_5	I	Z	Z	I	I	Z	Z
g_6	Z	I	Z	I	Z	I	Z

It is easy to check that all single qubit errors form a correctable set of errors for the Steane code, implying that this code can be used to correct an arbitrary single qubit error.

Encode operations

$X_e = X_1X_2X_3X_4X_5X_6X_7$

$Z_e = Z_1Z_2Z_3Z_4Z_5Z_6Z_7$

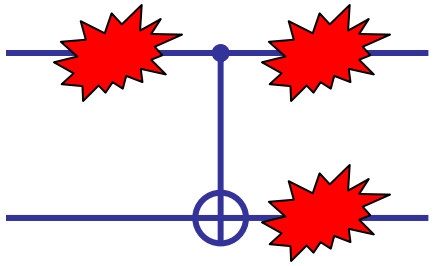
Fault-tolerant quantum computation

Reliable quantum computation can be achieved even with faulty gates provided the error probability per gate is below certain threshold.

To perform quantum computation directly on encoded quantum states, we replace an original quantum circuit by encoded circuit, i.e. each qubit by encoded qubit using e.g. the Steane code, and each operation by the appropriate encoded operation. This is not enough for fault-tolerance.

Problems:

1) Encoded gates can cause errors to propagate;
2) The encoded CNOT can cause an error on encoded control qubit to spread to an encoded target qubit.



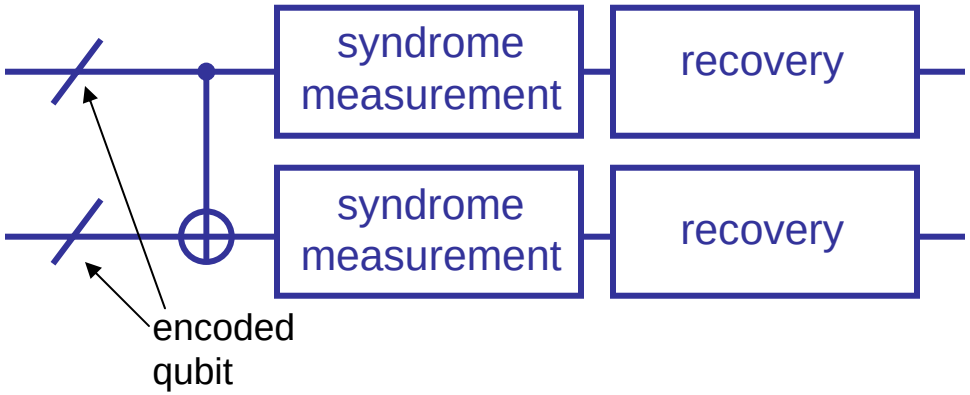
Fault-tolerant encoded operations are those which ensure that a failure anywhere during the computation can only propagate to a small number of qubits in each block Of the encoded data, so that error correction can effectively remove it.

We define the fault-tolerance of a procedure to be the property that if only one component in the procedure fails then the failure causes at most one error in each encoded block of qubits output from the procedure.

Concatenated codes and threshold

A fault tolerant CNOT gate

The procedure introduces two errors into the 1st encoded block with probability $O(p^2)$.

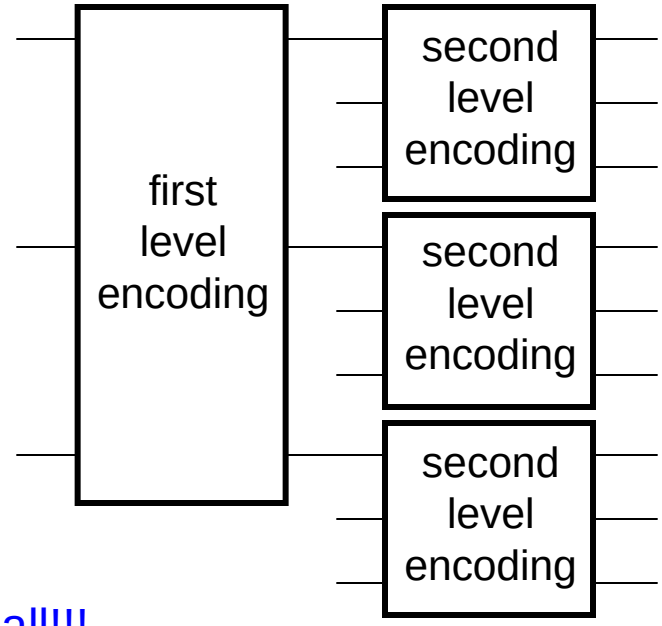


Concatenated codes and the threshold theorem

A quantum circuit containing p(n) gates may be simulated with probability of error at most ε using

$$O(\text{poly}(\log p(n)/\varepsilon)p(n))$$

gates on hardware whose components fail with probability at most p, provided p is below some constant threshold, $p<p_{th}$, and given reasonable assumptions about the noise in the underlying hardware.



The typical thresholds are $p_{th} \sim 10^{-4} – 10^{-5}$

i.e. allowable noise (error) is about 0.01% - too small!!!

Are there any other routes to fault-tolerant quantum computing?

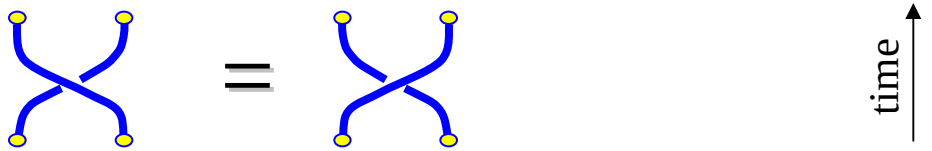
Natural fault-tolerance
Quantum statistics

Configuration space of **n** indistinguishable particles in **d** dimensional space excluding diagonal points D:

$$M_n = (R^{nd} - D)/S_n$$

In (3+1) dimensions, the configuration space is simply connected; quantum mechanics permits only two kinds of statistics:

Exchanging particles in 3D space belongs to the permutation group S_n



Statistics follows from one-dimensional representations of S_n :

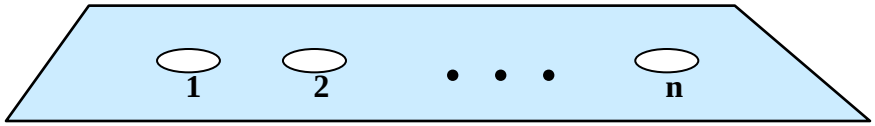
Bose-Einstein statistics: $\chi_+ (\sigma) = +1$

Fermi-Dirac statistics: $\chi_- (\sigma) = +1$ (even) or -1 (odd permutations)

Anyons

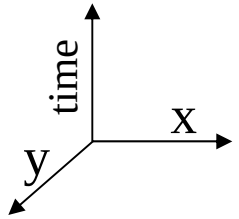
are particles with fractional statistics

The configuration space of **n** indistinguishable particles in **2** dimensional space excluding diagonal points is multiply connected



Leinaas and Myrheim'77
Wilczek'82

Exchanging particles on a plane is not anymore an element of permutation group



it is braiding, an element of a braid group!

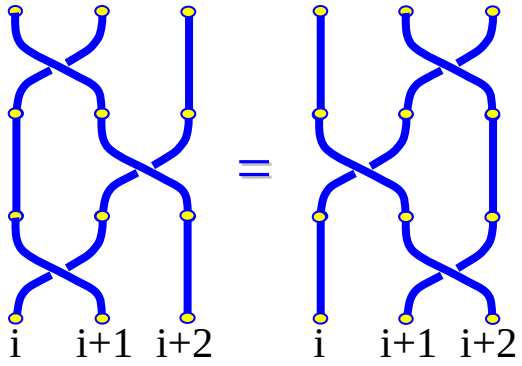
Braid group B_n

Artin, Ann. Math. 48, 101 (1947)

A braid group for n strands (particles) has n generators $\{1, \sigma_1, \ldots, \sigma_{n-1}\}$ which satisfy:

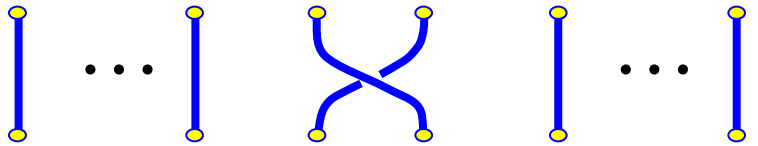
$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{for } |j - i| > 1$$

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$



Yang-Baxter equation

Example: σ_i



One-dimensional irreps of B_n correspond to abelian fractional statistics:

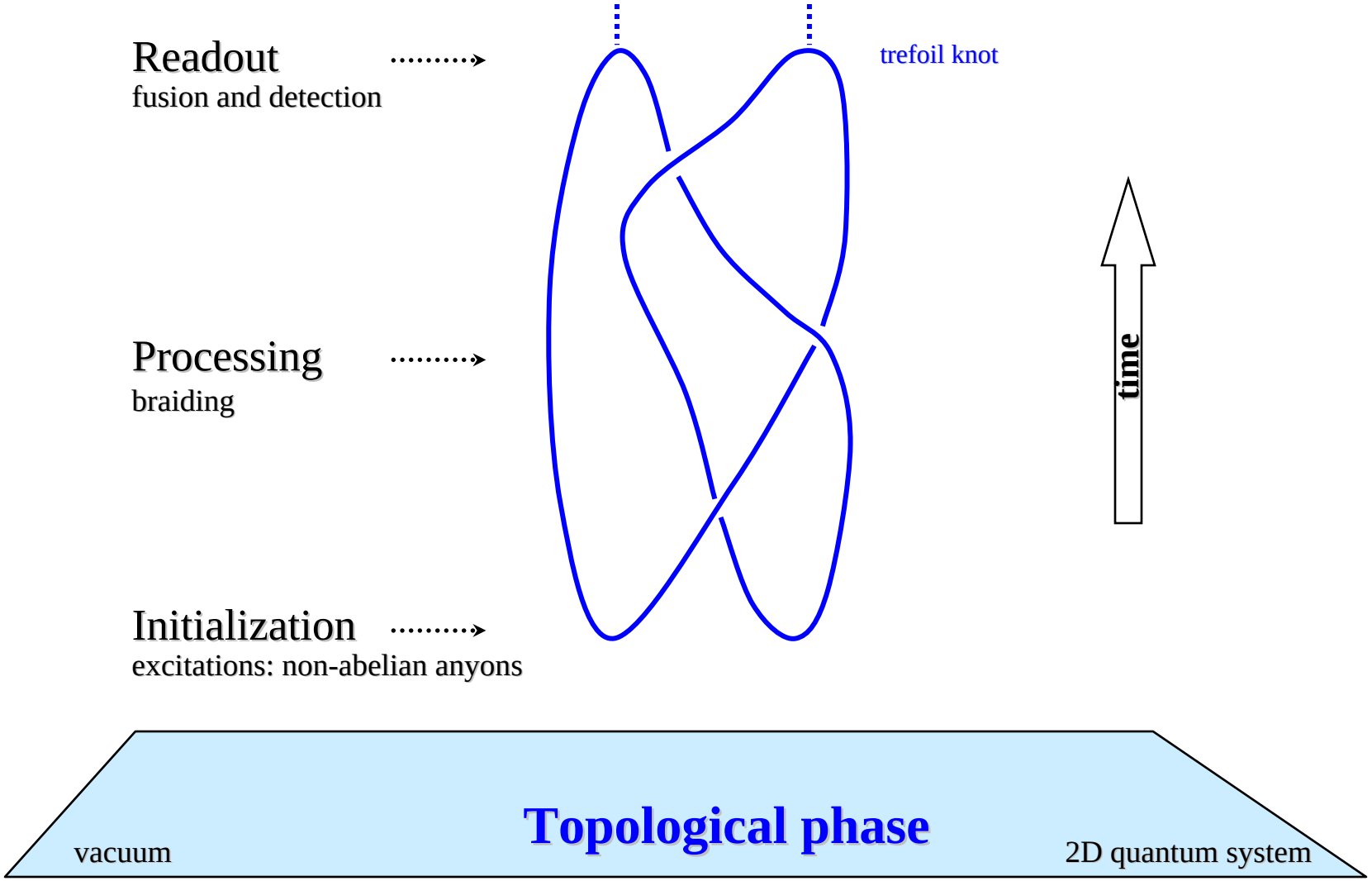
$$\chi_\theta(\sigma) = e^{i\theta} \qquad \in U(1)$$

Higher dimensional irreps correspond to nonabelian fractional statistics:

$$\chi_\theta(\sigma) = e^{i\theta\Lambda} \qquad \text{e.g. } \in SU(2)$$

Topological quantum computation

- **is naturally fault-tolerant**
- is realized by braiding (and exciting and fusing) non-abelian anyons



Topological phases of matter

- topological phases are phases of two-dimensional many-body quantum systems whose properties depend only on topology of the manifold on whose surface a given phase is realized

- their effective description is given by topological quantum field theory (3 dimensional) defined e.g. by the Chern-Simons action:

Witten, Commun. Math. Phys. 121, 351 (1989)

$$S = k/4\pi \int_{\Gamma} dt\, dx\, dy\, (a_y \partial_t a_x - a_x \partial_t a_y)$$

level of theory (integer); Γ ← (2+1)D manifold; gauge field

no metric!!!

Example: doubled $SU(2)_k$ Chern-Simons theory (PT invariant theory):

Freedman,et al., CMP 227, 605 (2002)

$k = 1$	- abelian topological phase	- quantum memory
$k \geq 2$	- non-abelian	
$k = 3, 5 \ldots$	- non-abelian and universal	- universal QC

- topological phases are invariant with local geometry and hence quantum information stored in them is invariant with local error processes

no metric, no error!!!

Topological phases of matter

- are ground states of certain strongly correlated many-body quantum systems

  e.g. in Coulomb gauge, $a_t = 0$: $\mathcal{L} = a_y \partial_t a_x - a_x \partial_t a_y$

$$\mathcal{H} = \frac{\partial \mathcal{L}}{\partial(\partial_t a_x)} \partial_t a_x + \frac{\partial \mathcal{L}}{\partial(\partial_t a_y)} \partial_t a_y - \mathcal{L} = \mathbf{0}$$

no metric, no energy!!!

- energy spectrum of matter in a topological phase is characterized by

finite topology-dependent ground state degeneracy,

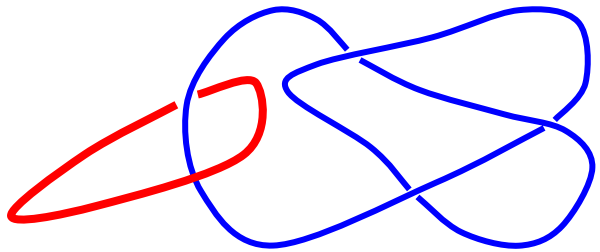
e.g. for the doubled $SU(2)_k$ Chern-Simons theory: $(k+1)^{2g}$ (genus)

Freedman et al. Ann. Phys. 310, 428 (2004)

⇓

spectral gap

excitations of stray anyons, which may cause errors via non-local processes, are at sufficiently low temperatures exponentially suppressed due to the spectral gap !!!



Topological phases of matter in physical systems

- fractional quantum Hall systems (FQH)
  particularly promising !!!

  Das Sarma, et al., Phys. Rev. Lett. 94, 166802 (2005)

- quantum lattice systems
  - atoms in optical lattices — **Duan, et al., Phys. Rev. Lett. 91, 040902 (2003)**
  - polar molecules — **Micheli et al., Nature Phys. 2, 341 (2006)**
  - Josephson-junction arrays — **Ioffe et al., Nature 415, 503 (2002)**

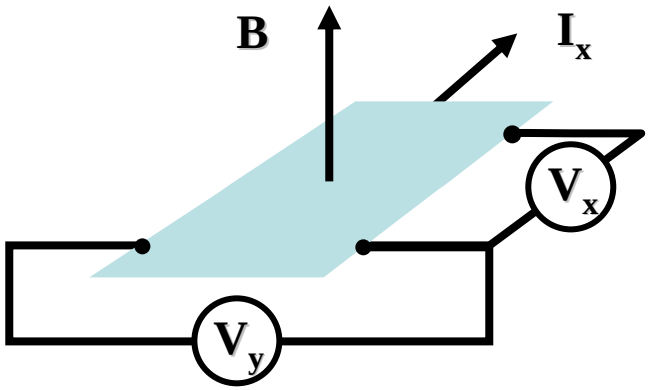
- p_x+ip_y superconductors
  - Sr_2RuO_4 — **Das Sarma, et al., Phys. Rev. B 73, 220502 (2006)**
  - Helium-3 — **Salomaa, Volovik, Rev. Mod. Phys. 59, 533 (1989)**

- rotating Bose-Einstein condensates

- nuclear matter

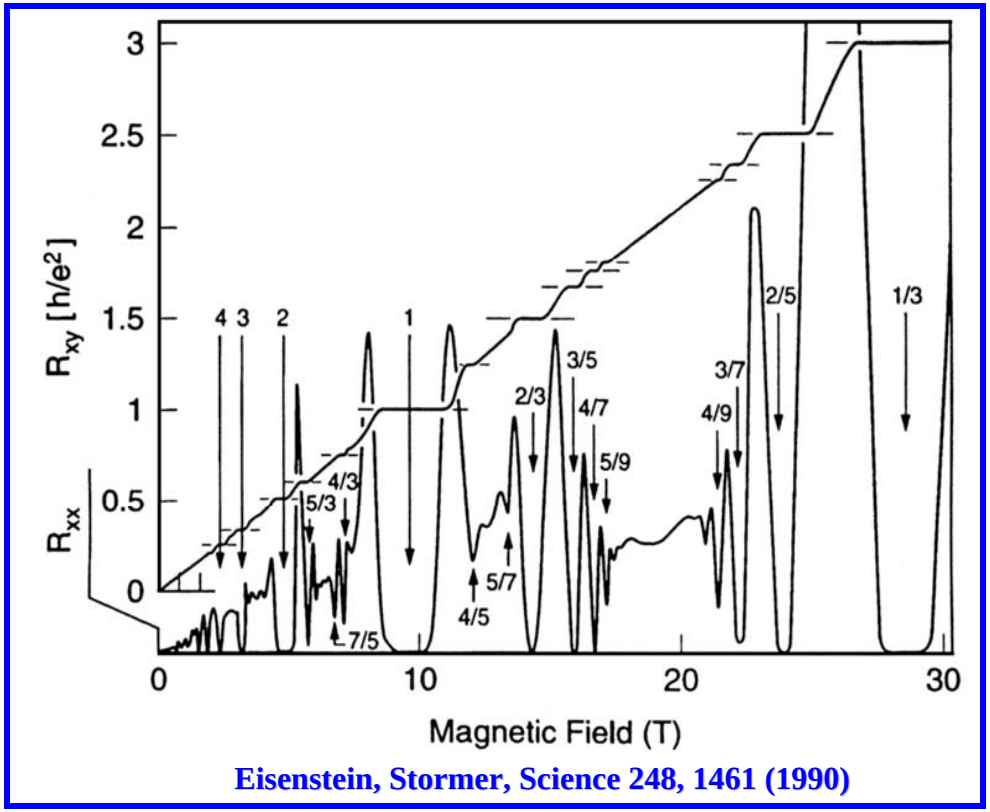
Topological phases of matter in FQH systems

Stormer, Tsui, Gossard, Phys. Rev. Lett. 48, 1559 (1982)
Rev. Mod. Phys. 71, S298 (1999)



Longitudinal resistance
$R_{xx} = V_x / I_x$

Transverse (Hall) resistance
$R_{xy} = V_y / I_x = h / \nu e^2$
- is quantized!!!



Eisenstein, Stormer, Science 248, 1461 (1990)

Theory

nonabelian quantum Hall phases at ν=5/2 and 12/5

Read, Rezayi, Phys. Rev.B 59, 8084 (1999)

Experiment

detecting these phases in high mobility samples

Xia et al., Phys. Rev. Lett. 93, 176809 (2004)

Topological quantum computation in FQH systems

- non-abelian topological phases predicted in fractional quantum Hall systems at the filling ν=5/2 and 12/5; these have recently been detected experimentally in extremely clean samples

Read, Rezayi, Phys. Rev.B 59, 8084 (1999)

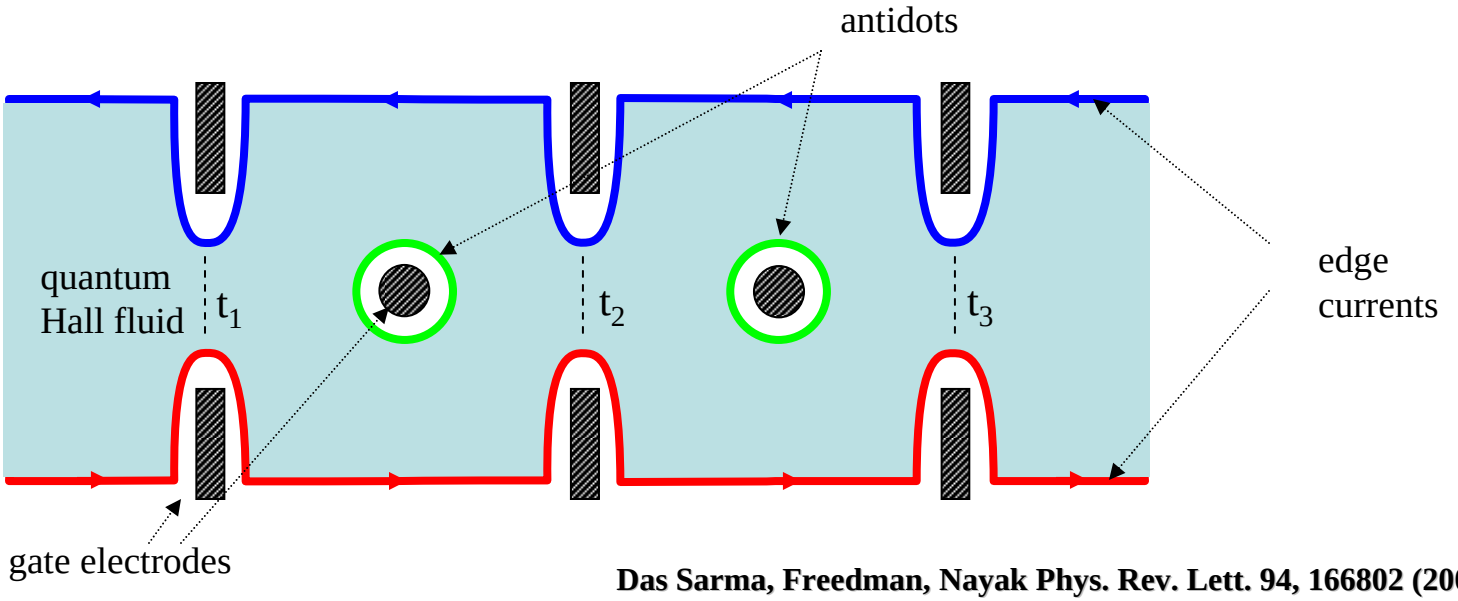
Xia et al., Phys. Rev. Lett. 93, 176809 (2004)

- experimental tests of fractional statistics using Laughlin interferometer

Camino, Zhou, Goldman, Phys. Rev. B 72, 075342 (2005)

- relation between boundary (CFT) and bulk (TQFT) – "holographic principle"

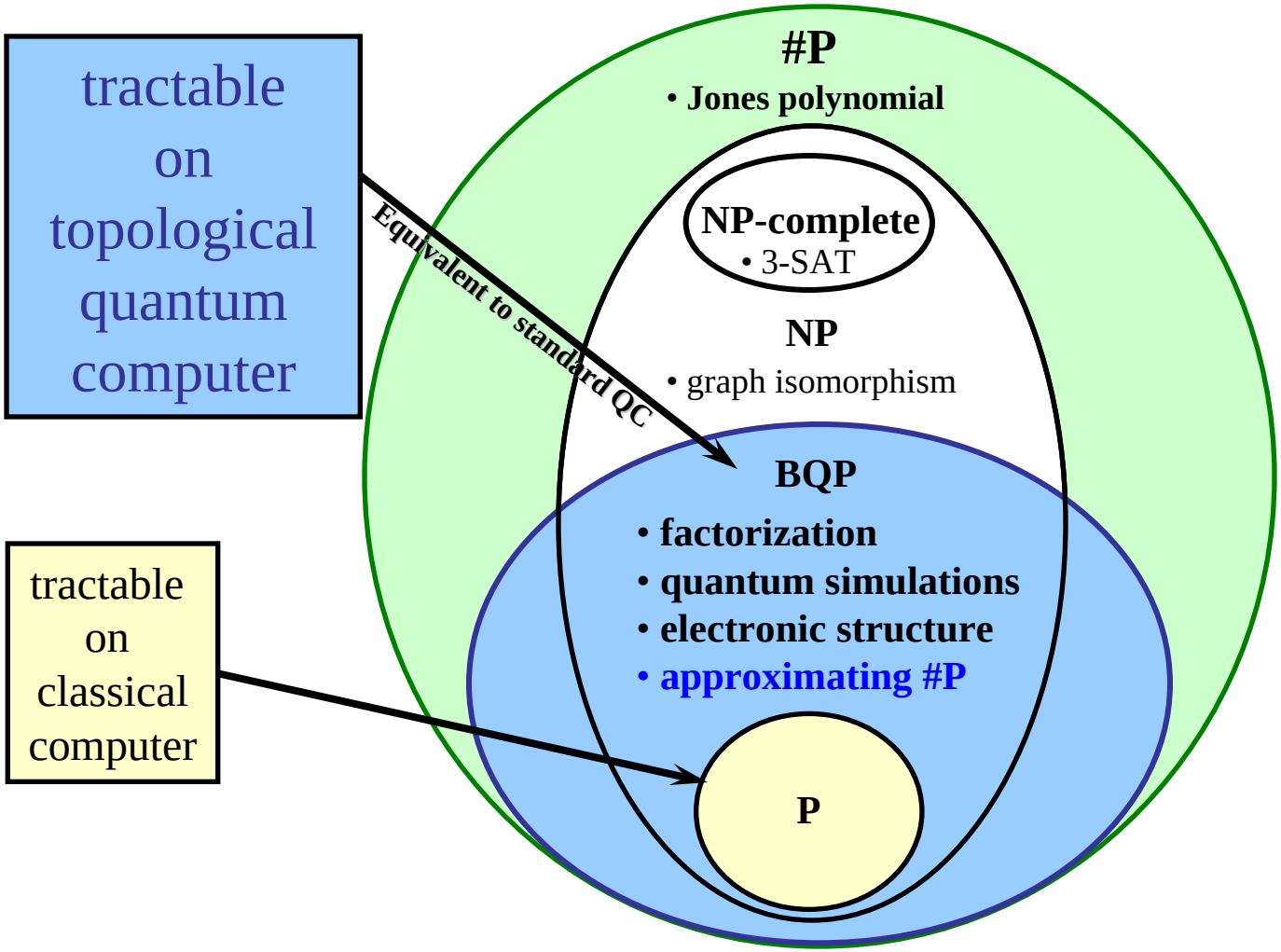
- topologically protected qubit



Das Sarma, Freedman, Nayak Phys. Rev. Lett. 94, 166802 (2005)

Topological quantum computation

• provides new insights into quantum algorithms and complexity theory



Freedman et al.,
Commun. Math. Phys. (2002)
Bordewich et al.
Comb. Prob. Comp (2005)
Aharonov, Jones, Landau,
STOC 2006

For more information about topological quantum computation, see e.g.

• G. P. Collins: Computing with Knots, **Scientific American**, April 2006

• S. Das Sarma, M. Freedman, and C. Nayak: Topological Quantum Computation, **Physics Today**, July 2006.