Braids, knots & quantum algorithms

Annalisa Marzuoli

Dipartimento di Fisica Nucleare e Teorica
Università degli Studi di Pavia
&
Sezione INFN

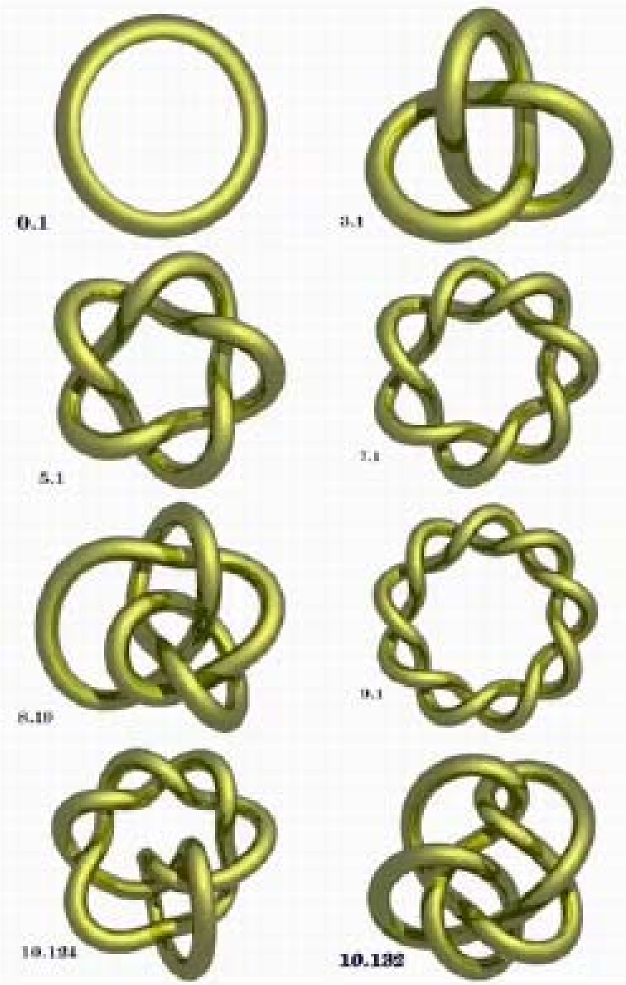
Introduction

- **The objective**:
  Construction of new efficient **quantum algorithms**
  for combinatorial (algebraic, topological) problems
- **The general context**:
  Quantum Information Theory in a generalized Q-circuit setting (Spin Network Q-automata, discretized version of **Topological Q-computation)**
- **The results**:
  Efficient quantum algorithms for approximating any observable of Chern-Simons Topological Quantum Field Theory, i.e. **(colored) Jones polynomials for knots** and combinatorial **invariants of 3-manifolds**

Outline

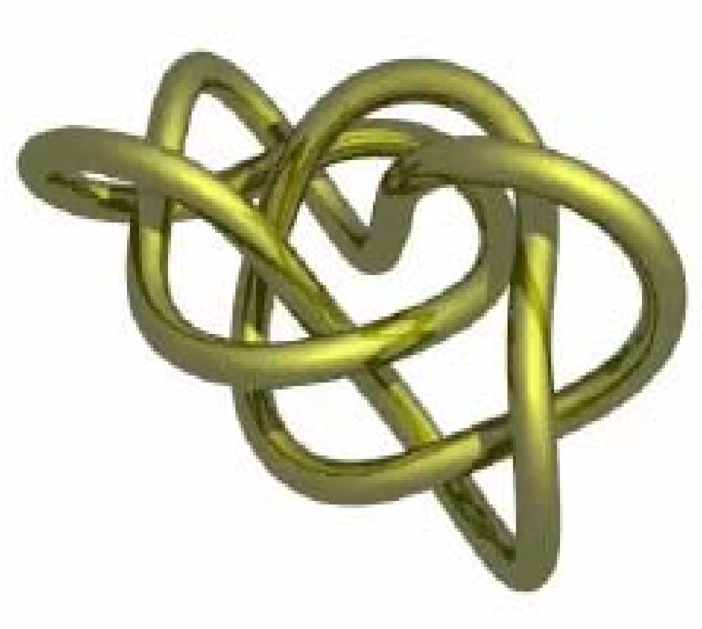
- Part I
  - Knot theory and the Jones polynomial
  - Computational complexity
  - Quantum automata
- Part II
  - Knot invariants in Chern-Simons TQFT
  - Unitary representation of the braid group
  - (Quantum circuits)
  - Combinatorial invariants of 3-manifolds

Knots



Knot theory is the branch of topology concerning with the properties of knots.
The most important problem in knot theory is the **classification of knots**: given two knots determine whether they are topologically equivalent or not.

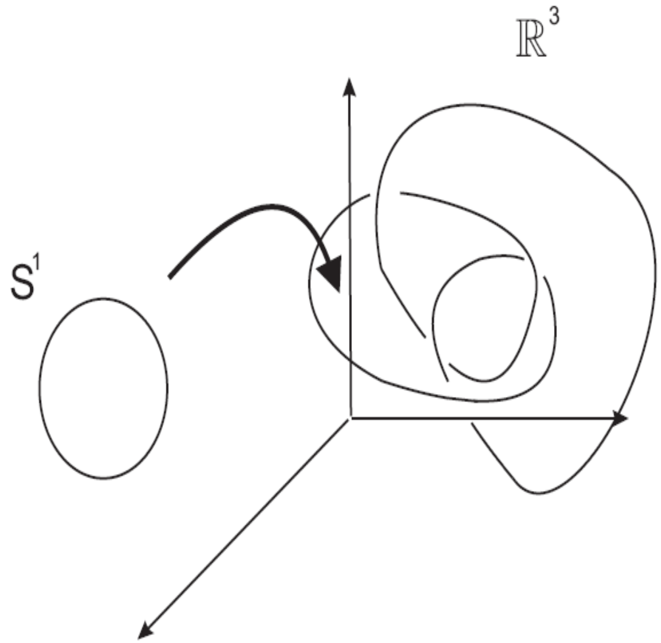
More knots



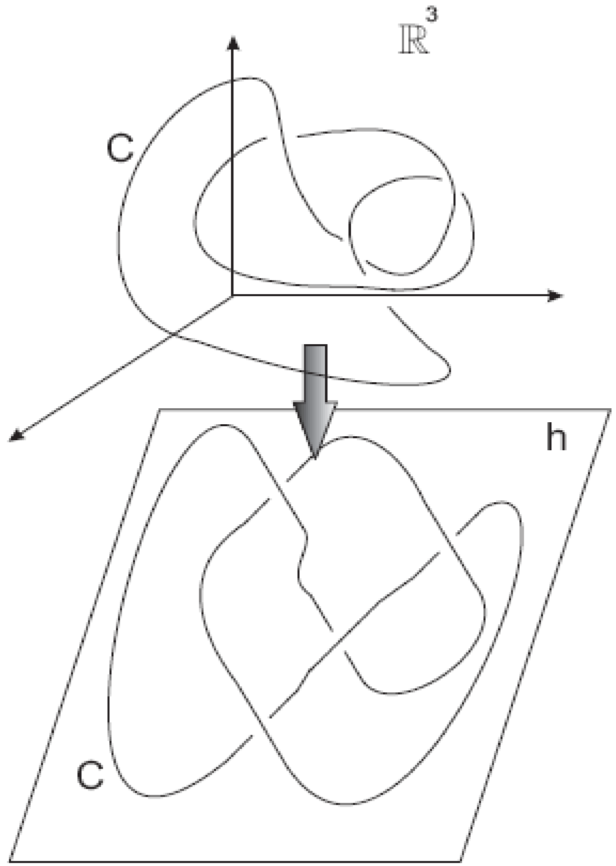
the “non-alternating
12-725 knot“

the "figure 8 knot"

Knot diagram



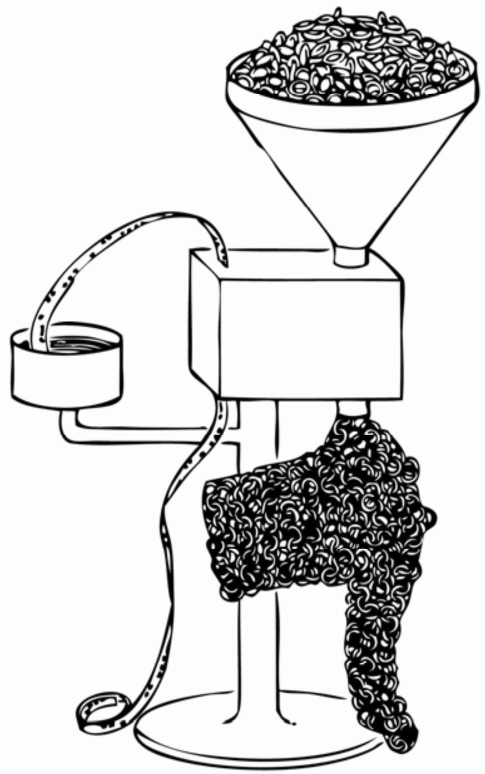
The embedding of S^1 into $\mathbb{R}^3$.



The projection of a knot on a plane.

Algorithmic problems in knot theory, *e.g.* **detecting the unknot**

"Wheeler Machine"



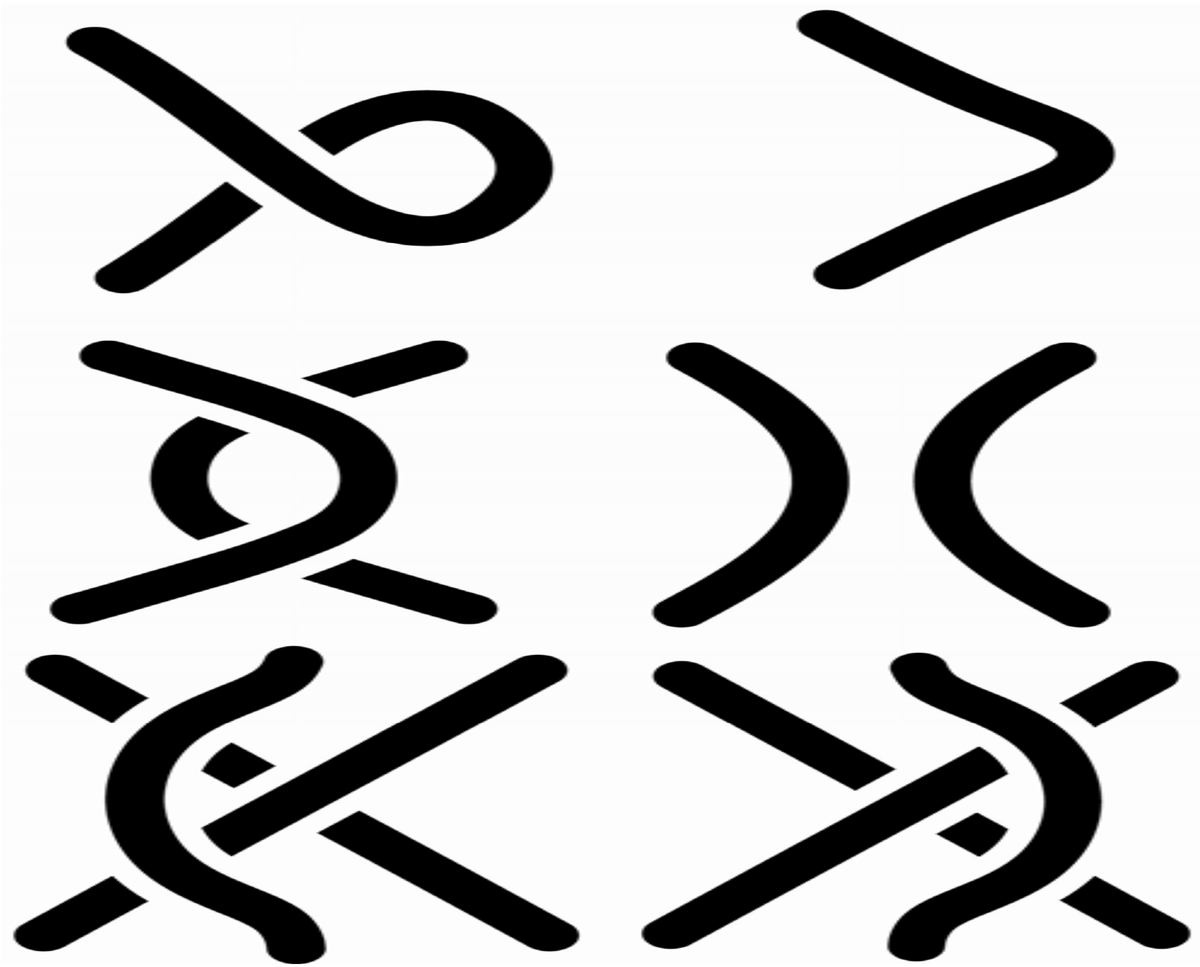
Unknotting Problem

- Instance : A knot diagram *D*
- Question : Does *D* a represents the ‘trivial’ knot?
- This problem is in **NP** (the class of decision problems that can be checked in polynomial time on a deterministic Turing machine)
- Haken’s algorithm (1961) runs in exp- time.
- Finding a Poly-time algorithm for an NP (complete) problem would imply P=NP (!)

Combinatorics of knot diagrams

- **Reidemeister moves** : Combinatorial transformations on the knot diagram that don’t change the equivalence class of the knot.
- A knot diagram is unknotted if and only if there exists a finite sequence of Reidemeister moves that converts it to the trivial knot diagram.
- Recursive procedure applied to subsets of the diagram: **exp-growth** in terms of the **n° of crossings** (the measure of the ‘size’ of the input)

Reidemeister Moves



The Jones polynomial

A **knot polynomial** is a knot 'invariant' in the form of a polynomial whose coefficients encode for some of the topological properties of classes of knot diagrams.

The Jones polynomial can distinguish mirror images of knots not detected by other knot invariants

JP for
the trefoil knot

$$J(q) = q^{-1} + q^{-2} - q^{-4}$$

Laurent polynomial in one formal variable q

The original definition of the Jones polynomial (*)
is given in terms of
the **trace** of a **matrix representation** of the
braid group into a Temperley-Lieb algebra TL(q)

Such an operation takes care of invariance of the
knot diagram(s) under Reidemeister moves, *i.e.*
J(q) depends only on intrinsic topological features

(in a quantum computation framework:
search for **unitary** representations)

(*) V.F.R. Jones, Bull. Amer. Math. Soc. 129 (1985), 103-112.

Braid group

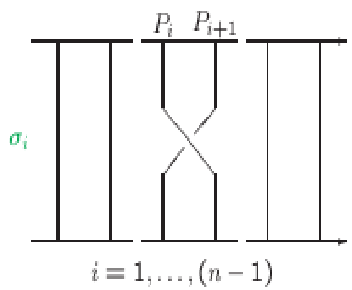
The braid group on n strands, B_n, is a finitely presented group on (n-1) generators with a simple geometrical realization (weaving patterns)

Presentation of Bn :

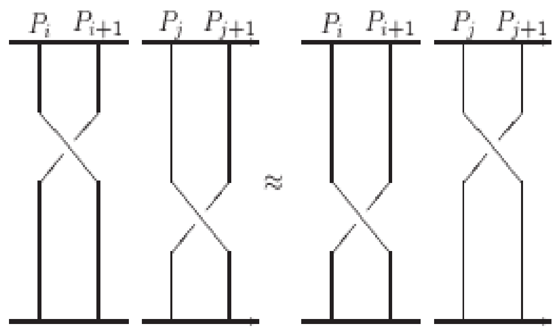
$$\sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \; (|i-j| \geq 2), \; \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \; (i = 1, 2, \ldots, n-2)$$

(Second relation:
algebraic Yang-Baxter equation)

Generators & relations

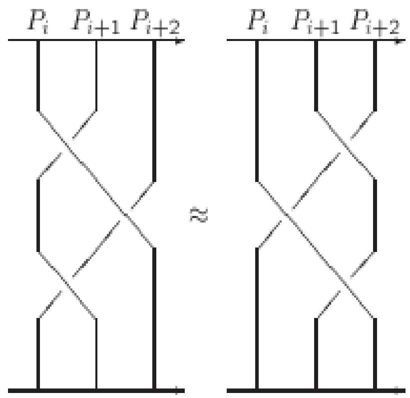


The braid group: generators



The braid group: relations

$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{if} \quad |i-j| \geq 2$

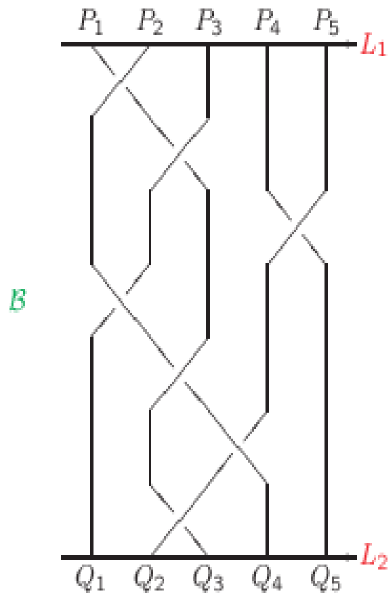


The braid group: relations

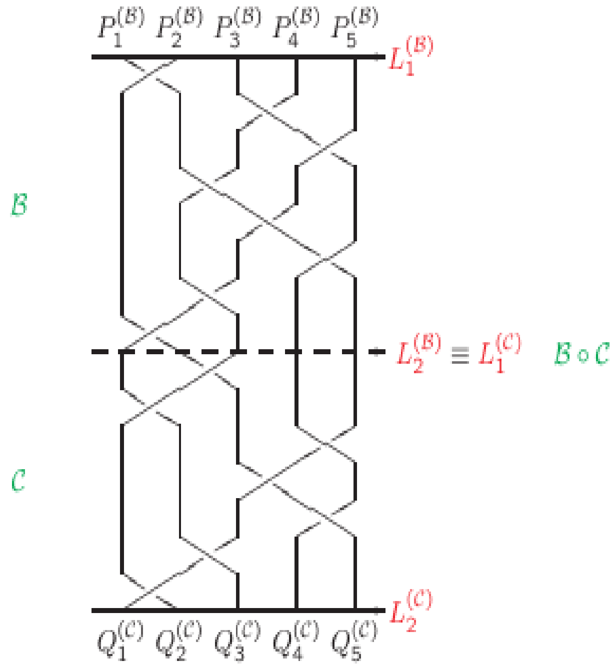
$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \quad \forall i = 1, \ldots, n-1$

Composition law

The braid group $\mathcal{B}_n$

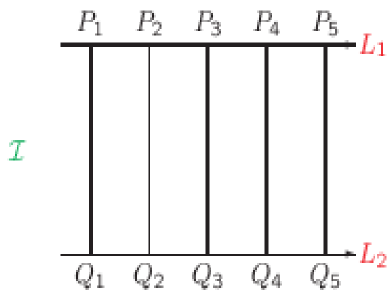


Elements *of the braid group:* **weaving patterns**

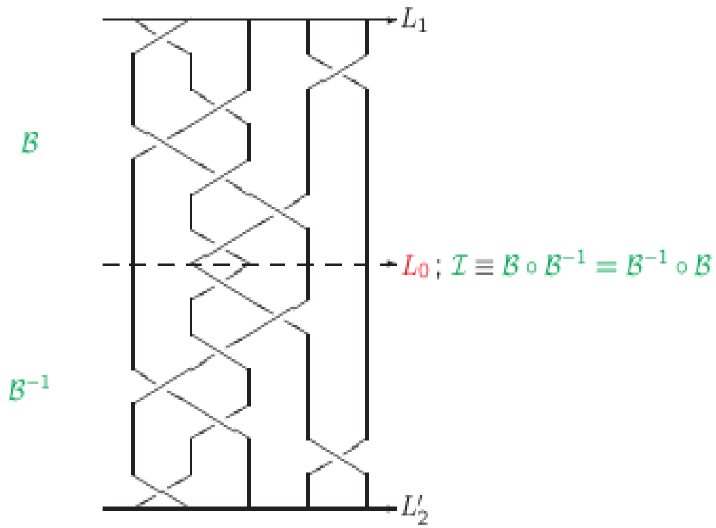


The braid group multiplication: **composition of two weaving patterns**

Identity & inverse braid



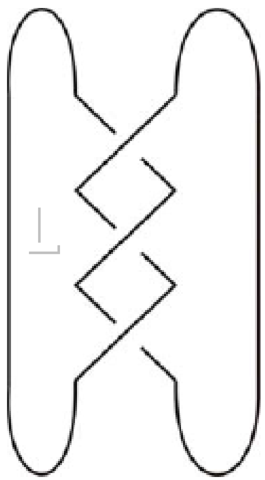
Elements of the braid group: **the identity pattern**

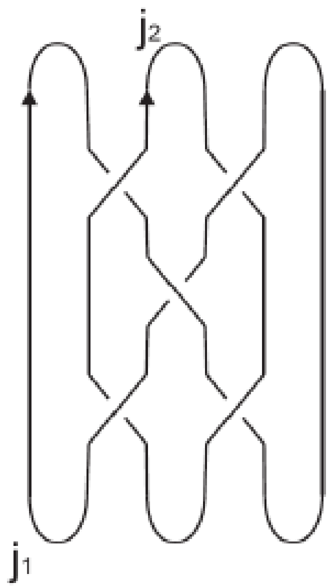


Elements of the braid group: **the inverse weaving pattern**

From knots to braids

Any given link **L (collection of knots)**

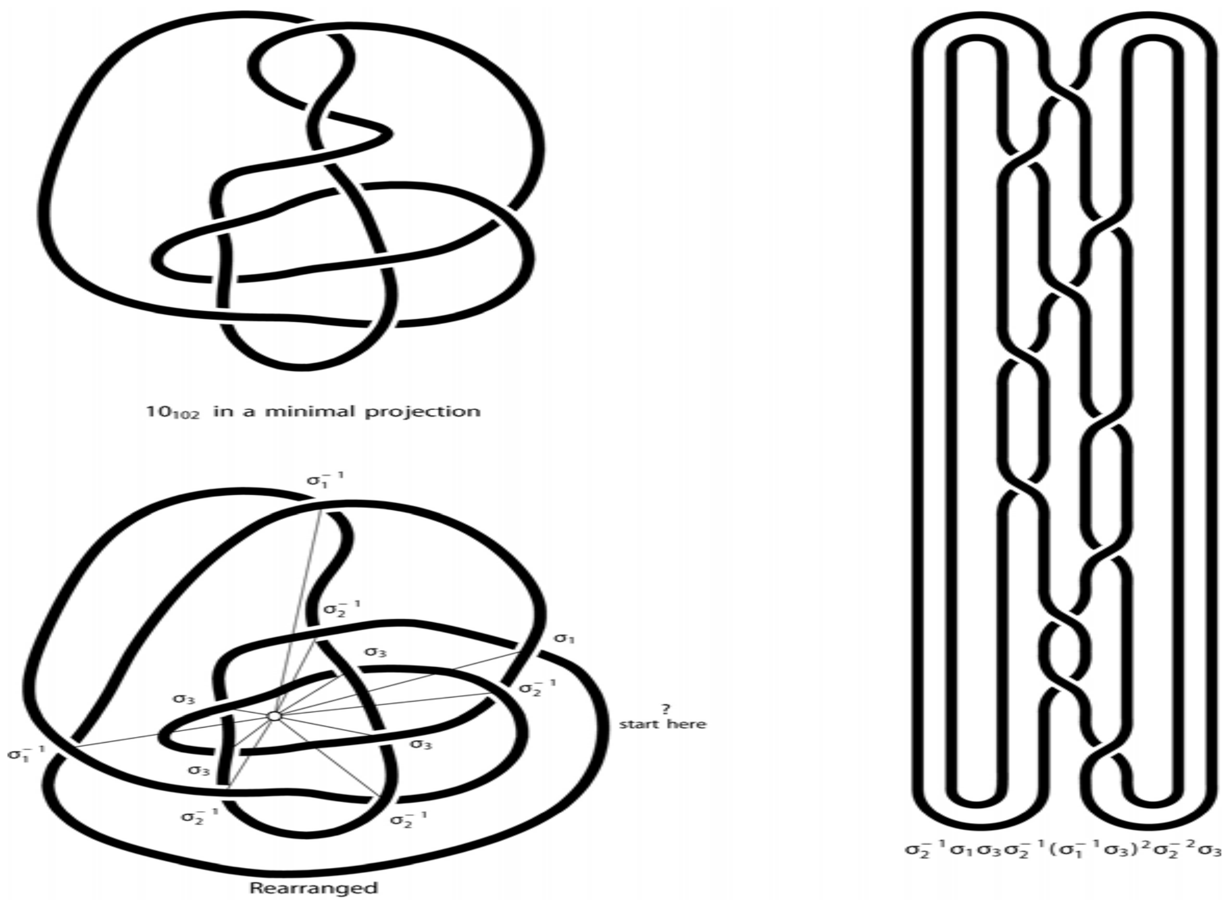




('colored' link)

can always be seen as the closure of a braid (Alexander theorem)

Any such transformation can be done efficiently



Construction of a closed braid from a knot diagram.

Figure from Interactive Topological Drawing (1998) by R. G. Scharein
www.pims.math.ca/knotplot/

Computational complexity of Jones polynomial J(q)

- We know that there exist no efficient classical algorithms for its evaluation, more precisely it is a

#P-hard problem

- Can we construct an efficient (employing **P**olynomially-bounded resources) **quantum algorithm**?

- What about 'approximate' calculation?

Jaeger, Vertigan and Welsh, *On the computational complexity of the Jones and Tutte Polynomials*, Math. Proc. Cambridge Phil. Soc. 108(1990), 35-53

- **#P-hard** problem: 'hard' means that all problems in #**P** can be polynomially reduced to it.
- **#P** is the complexity class of counting problems associated with 'decision' problems belonging to **NP**. Tipically:

(NP) Is there a solution to a given algorithmic problem? (yes/no)
(#P) How many solutions are there?

EX. Existence of Hamiltonian circuit(s) in graphs (NP-c & #P)

- A **#P** problem is at least as hard as the associated **NP** problem

- Then efficiently solving a **#P**-hard problem would imply efficient solution to the corresponding **NP**-complete problem, and so we could prove **P=NP**

- It is known that a few **#P**-hard problems admit efficient classical algorithms for their **approximate solutions** (this is not the case for Jones polynomial)

- Evaluating (generalizations of the) Jones polynomial of any knot can be done efficiently with a quantum computer if we search for an **additive approximation** of its value when the formal variable is **$q=2\Pi i/k$** (K=positive nteger)

- In fact such approximate evaluation of (extended) Jones polynomials is the first known **BQP**-complete problem ever solved

D Aharonov, V Jones, Z Landau quant-ph/0511096
S Garnerone, A Marzuoli, M Rasetti quant-ph 0601169 [QIC 7 (2007) 479]

- **BQP** = **B**ounded error **Q**uantum **P**olynomial time: the class of decision problems solvable by a quantum computer in polynomial time with an error probability < ¼

- These are the problems that a quantum computer can 'reasonably' solve

- A **BQP**-complete problem is important to compare quantum and classical models of computation as well as complexity classes of algorithmic problems

Bordewich, Freedman, Lovasz, Welsh, *Approximate counting and quantum Computation*, Comb. Probab. Comput. 14(2005), 737-754

- An **additive approximation** of J (L, q) (L:link) is a random variable X such that, for each small $\delta \geq 0$, the value X is accepted as the result of the (quantum) computation with

$$\mathbf{Prob}\ \{\ |J(L,q) - X| \leq \delta\ \} \geq 3/4$$

- In case q= k-th root of unity the approximate value X of J (L, q) can be evaluated `efficiently', namely the running time of the quantum algorithms (AJL & GMR) is bounded from above by

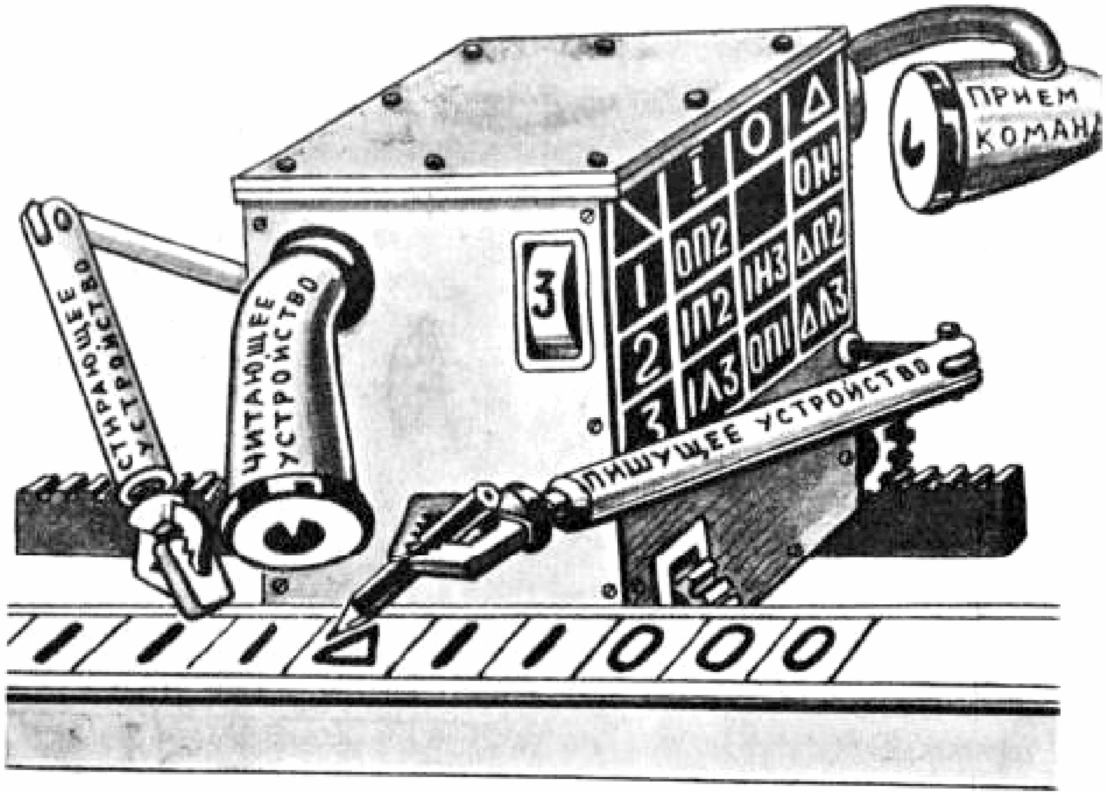
$$\mathcal{O}[\ \mathrm{poly}\ (N, \kappa)\ ]$$

N= # of strands of the associated braid

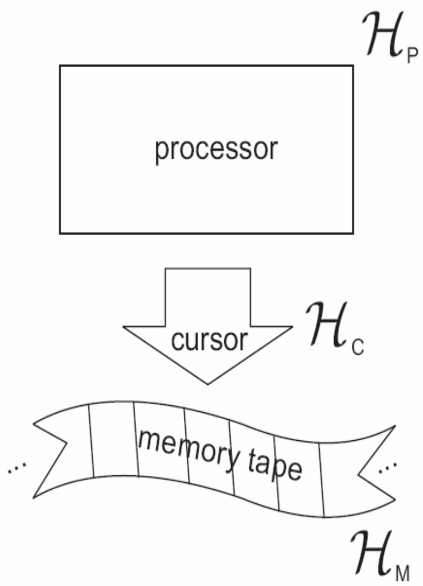
κ= # of crossings of the link diagram

- (GMR): 'colored' Jones polynomial J (L, q; $j_1, j_2,\ldots,j_N$) and the result holds for each choice of ($j_1, j_2,\ldots,j_N$) (see below)

Computing machines



Turing machine



(quantum)

- Classical physics and quantum mechanics support several different implementations of the Turing machine model of computation (abstract **universal model**)

- These reference models are equivalent to Boolean circuits

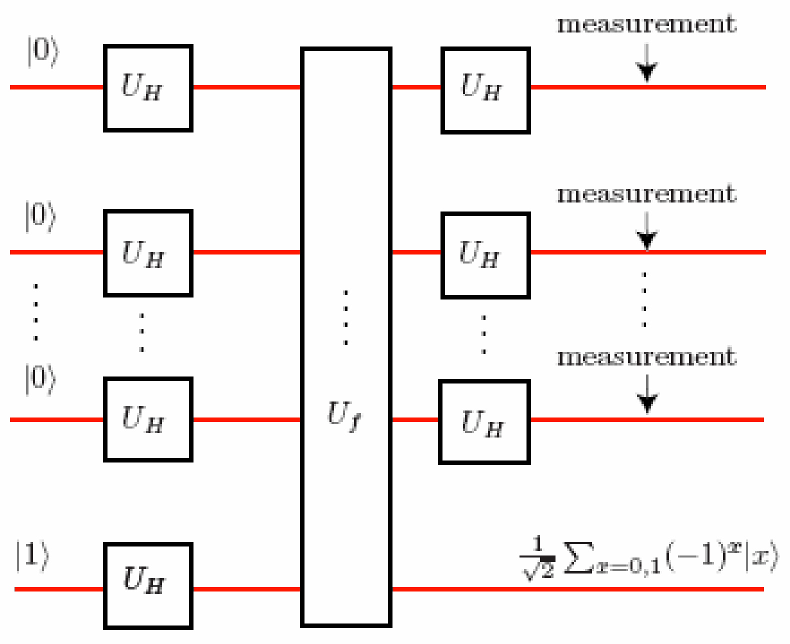
  - **Complexity classes** of algorithmic problems are defined with respect to such universal models:

  - **P** w.r.t. classical Turing machine
  - **BPQ** w.r.t. quantum circuits based on qubits and a set of elementary unitary gates

Quantum computing

What is a **quantum algorithm**?

A computational procedure which can be performed on a quantum system



Ingredients:

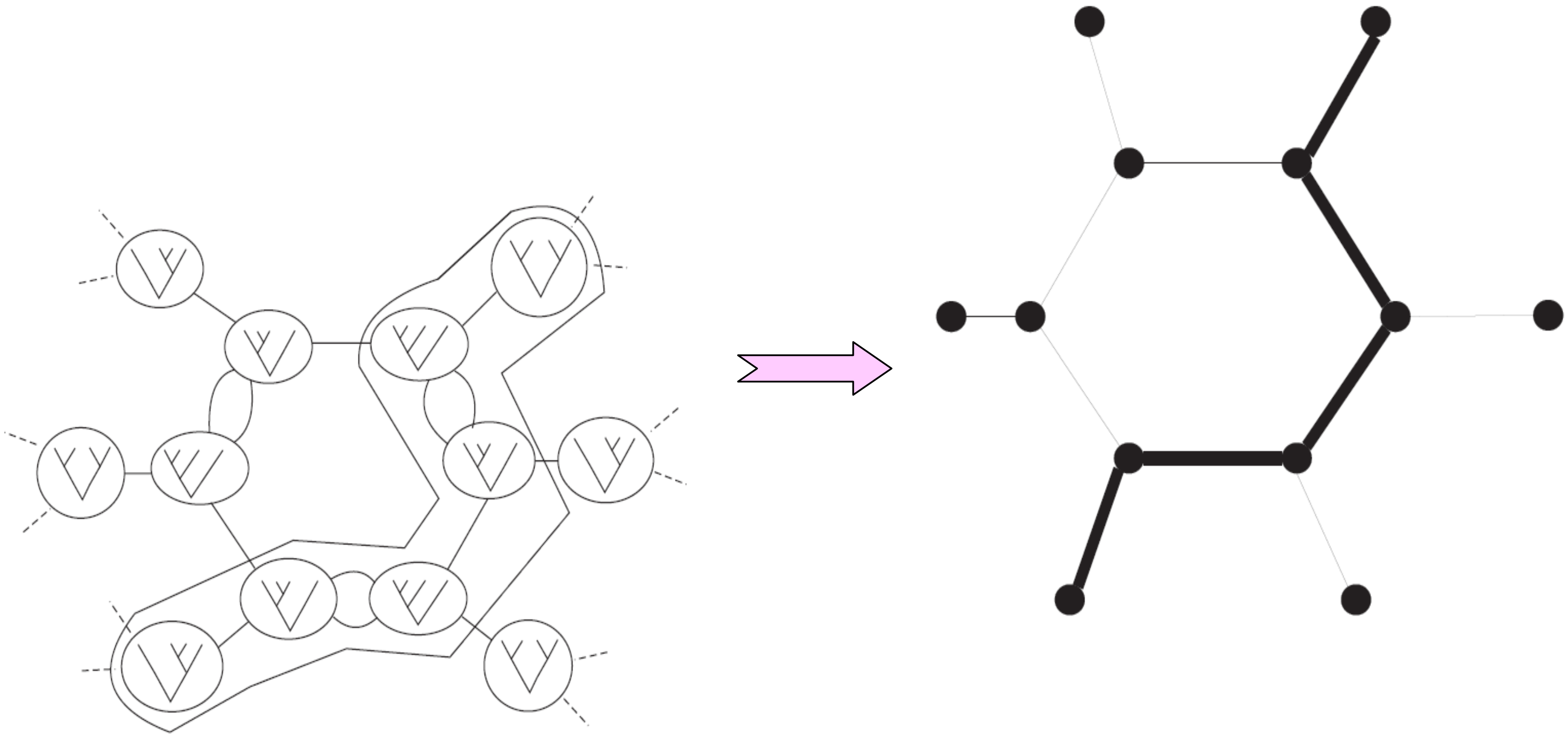
- **Superposition**
- **Entanglement**
- **Unitary evolution**

- When dealing with combinatorial problems it may be useful to switch to **automaton architectures**
- A finite-states & discrete-time **quantum** automaton is a graph-like structure where

- Nodes encode for computational finite-dimensional Hilbert spaces
- Links between contiguous nodes represent admissible unitary evolutions (each corresponding to 1 computational step)

'Spin Network' quantum simulator

Nodes: Hilbert spaces of N binary coupled SU(2) angular momenta
Edges: unitary operations (Racah-Wigner 6j-symbols)



A. Marzuoli and M. Rasetti
Ann. Phys. **318** (2005) 345

Spin Network quantum automata

The spin network simulator scheme relies on the
Racah-Wigner tensor algebra of the group SU(2).

It can be thought of as non-Boolean version of the quantum circuit model, with unitary gates expressed by recoupling transformations (3nj symbols) among inequivalent binary coupling scheme of N SU(2)-angular momenta
(not just ½ spins).

• connects circuit schemes for quantum computation with Topological Quantum Field Theory;
• its combinatorial properties are related to SU(2) ‘state sums’ used in low-dimensional quantum gravity models.

Spin Network Quantum Automata (**SNQA)** are families of finite-states quantum machines generated by considering the tensor algebra of the deformation of the universal enveloping algebra of SU(2), SU(2)q, where

q=2Πi/k

k≥3 (integer)

SNQA process linearly unitary representations of the braid broup

1-step unitary transformations:

- **U (**σ_i**)** (elementary braiding operator associated with each generator of the braid group)
- **U (q-6j)** (q-Racah transform implemented by the deformed version of the SU(2) 6j-symbol)

From QSN automata to standard quantum computation

- Recall that **complexity classes** of algorithms are defined within the proper (classical, quantum) **universal model** of computation
- Given a quantum automaton scheme it is necessary to prove that each computational step can be efficiently performed by a (suitable designed) **standard Q-circuit**
- The SNQA states can be encoded efficiently into many-qubits states and the unitaries **U** (σ_i) & **U** (**q-6j**) can be polynomially compiled by quantum circuits (*cfr.* final slides)

Knot invariants in Quantum Field Theory

- **Unitary representations** of the braid group &
- realizations of Jones polynomials as **'traces'** of associated matrix representations

arise naturally in the context of

Chern-Simons Topological Quantum Field Theory (CS-TQFT)

E. Witten, *Quantum field theory and the Jones polynomial,* Comm. In Math. Phys. 121(1989), 351-399

Chern-Simons TQFT

3-dimensional 'topological' quantum field theory:
the quantum partition functional and correlation functions do not depend on the space-time metric and then must be related to topological invariants

Classical action

$$S = \frac{k}{4\pi} \int_M Tr\left(A \wedge dA + \frac{2}{3} A \wedge A \wedge A \right)$$

k is the (integer) coupling constant

A is a connection one-form, valued in the Lie algebra of the group ***G*** (=SU(2)), the gauge group

M is a 3-dimensional closed manifold (*e.g.* the 3-sphere)

Observables in **CS-TQFT**

Wilson loop operators associates with closed, 'knotted' curves (P: operator ordering)

$$W(C;\rho) = \mathrm{Tr}\,\mathrm{P}\,\exp\left(i\oint_C A^a_\mu(x)T^a_{(\rho)}\,dx^\mu\right)$$

ρ is a representation of the gauge group **G;**
C is a knot (or link);
T are the generators of **G** in representation **ρ**;
A is a connection on the principal fibre bundle **P(M,G)**

If **G**=SU(2) the expectation values of Wilson operators are (colored) Jones polynomial (suitable normalized)

Kaul unitary representation

CS-TQFT is **exactly solvable** for each fixed value of the coupling constant K.

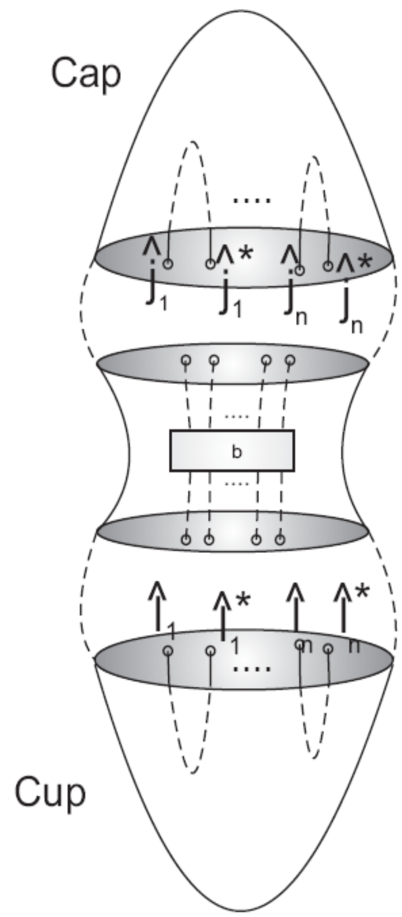
Procedure (outline)

- give a knot present it as the 'plat' closure of a braid embedded in the 3-sphere
- cut the braid with horizontal lines in such a way that between two lines there is at most one crossing
- use Kaul **unitary** representation of the braid group to get the **colored Jones invariant** as v.e.v. (vacuum expectation value) of its Wilson operator

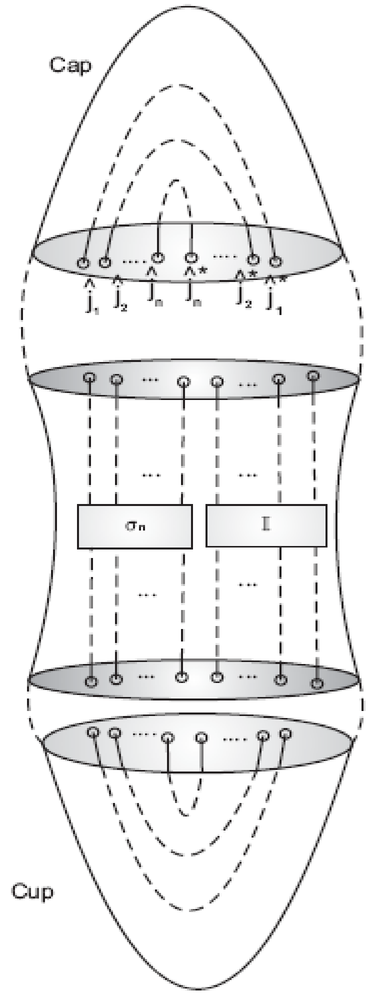
R. Kaul, *Chern-Simons theory, colored-oriented braids and links invariants*, Comm. In Math.Phys. 162(1994), 289

Kaul unitary representation of the group of oriented colored braids

$j_1, j_2, \ldots, j_n$ label irreps of **SU(2)q** **(colors)**



The plat-closure of a braid inside a 3-manifold



The standard closure of a braid pattern inside a 3-manifold

Generators of the braid group are mapped into "elementary" braiding operators

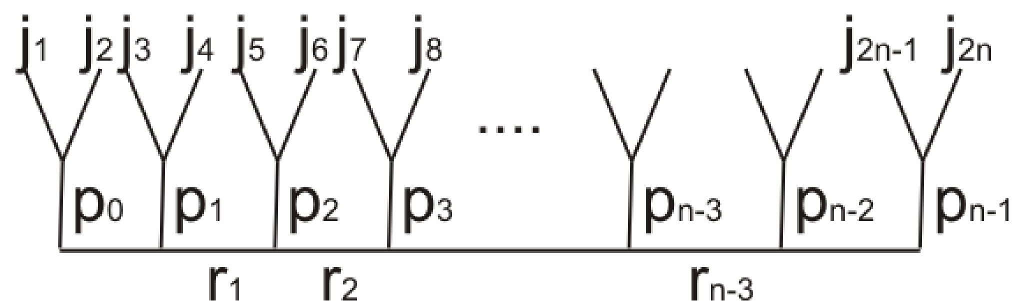
$$\sigma_i \rightarrow U\left(\sigma_i\right)$$

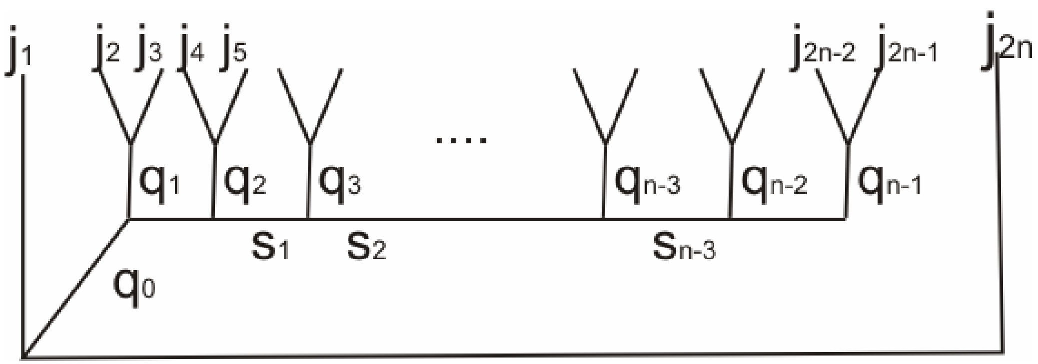
The finite-dimensional Hilbert spaces supporting Kaul representation are the conformal blocks of Wess-Zumino-Witten Conformal Field Theory (living on 2 copies of the 2-sphere embedded in the ambient 3-sphere)

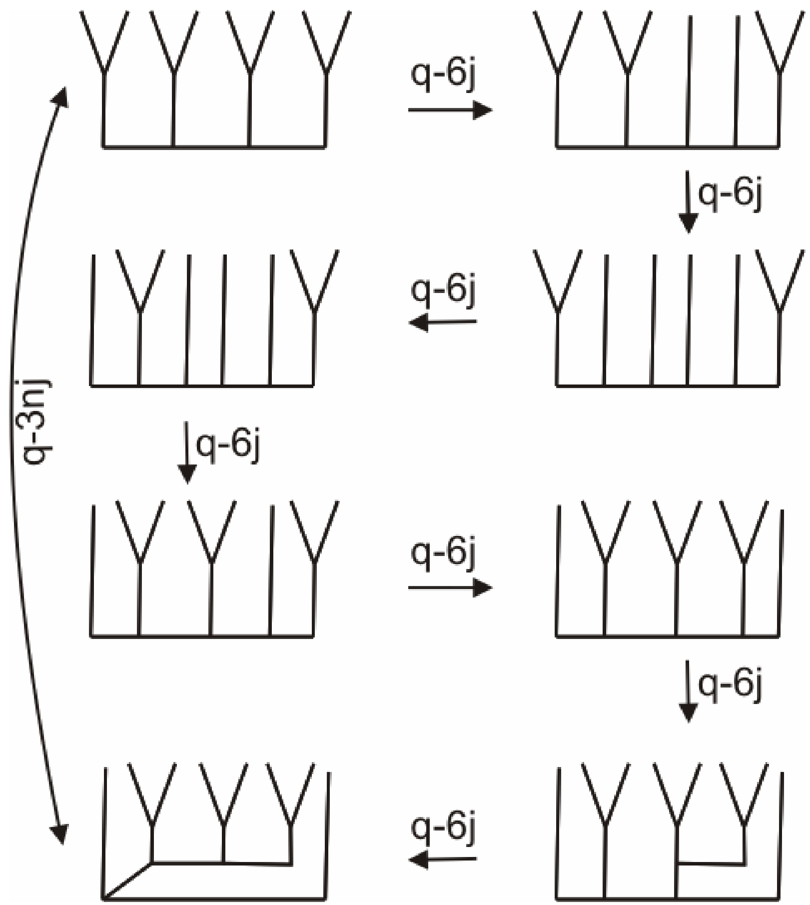
$$U[\sigma_{2i+1}]_{(\mathbf{p};\mathbf{r})(\mathbf{p}';\mathbf{r}')} = \lambda_{p_i}(\hat{j}_{2i+1}, \hat{j}_{2i+2})\delta_{\mathbf{p},\mathbf{p}'}\delta_{\mathbf{r},\mathbf{r}'}$$

$$U[\sigma_{2i}]_{(\mathbf{p};\mathbf{r})(\mathbf{p}';\mathbf{r}')} = \sum_{(\mathbf{q};\mathbf{s})} \lambda_{q_i}(\hat{j}_{2i}, \hat{j}_{2i+1}) A_{(\mathbf{p}';\mathbf{r}')(\mathbf{q};\mathbf{s})}\begin{bmatrix} j_1 & j_2 \\ \vdots & \vdots \\ j_{2i-1} & j_{2i+1} \\ j_{2i} & j_{2i+2} \\ \vdots & \vdots \\ j_{2n-1} & j_{2n} \end{bmatrix} A_{(\mathbf{p};\mathbf{r})(\mathbf{q};\mathbf{s})}\begin{bmatrix} j_1 & j_2 \\ \vdots & \vdots \\ j_{2i-1} & j_{2i} \\ j_{2i+1} & j_{2i+2} \\ \vdots & \vdots \\ j_{2n-1} & j_{2n} \end{bmatrix}$$

Alternative basis states (odd, even) & transformations (q-3nj recoupling coefficients)







Expression of the Jones polynomial as v.e.v. (trace) of the Wilson operator associated with the (plat closure of the) colored braid **σ (::::::)**

$$F(\mathcal{L}) = \prod_{i=1}^{n} [2j_i + 1]_q \times {}^{1}\langle \mathbf{0}; \mathbf{0} | U \left[\sigma \begin{pmatrix} \hat{j}_1 & \hat{j}_1^* & \cdots & \hat{j}_n & \hat{j}_n^* \\ \hat{l}_1 & \hat{l}_1^* & \cdots & \hat{l}_n & \hat{l}_n^* \end{pmatrix} \right] | \mathbf{0}; \mathbf{0} \rangle^{\mathbf{j}}.$$

$[2j_i + 1]_q$ is the q-dimension of the representation j_i

For each link L presented as the plat closure of a colored 2n-strand braid and for a fixed **q=2Πi/k** there exists a **SNQ automata** whose computational graph is **'isomorphic'** to the diagram of the braid

Encoding Kaul states (I)

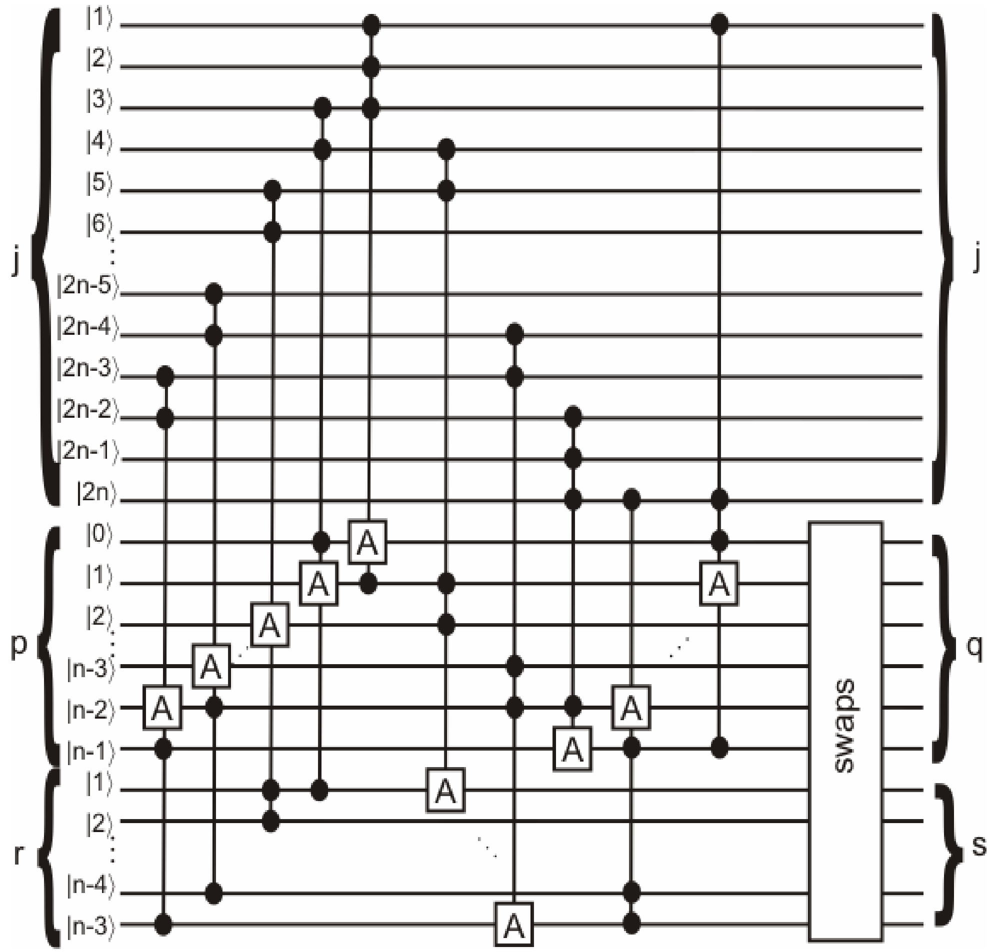
qubits

$$\propto n \lceil \log(k+1) \rceil$$

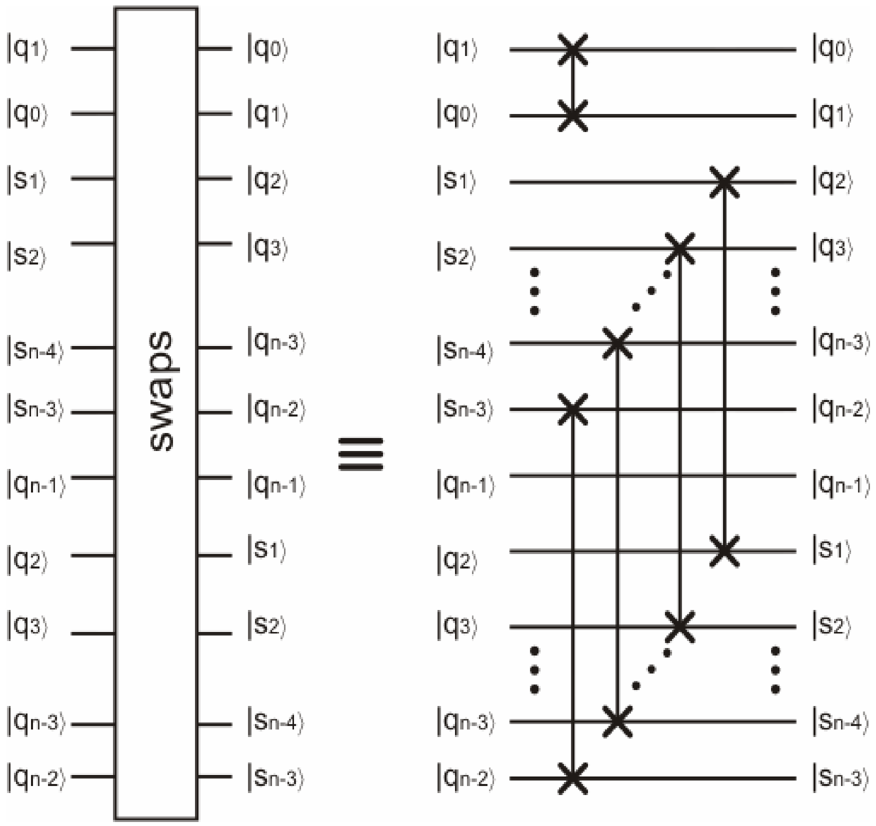
gates

$$\propto n \times poly(k)$$

Here n is the index of the braid group and k is CS coupling constant

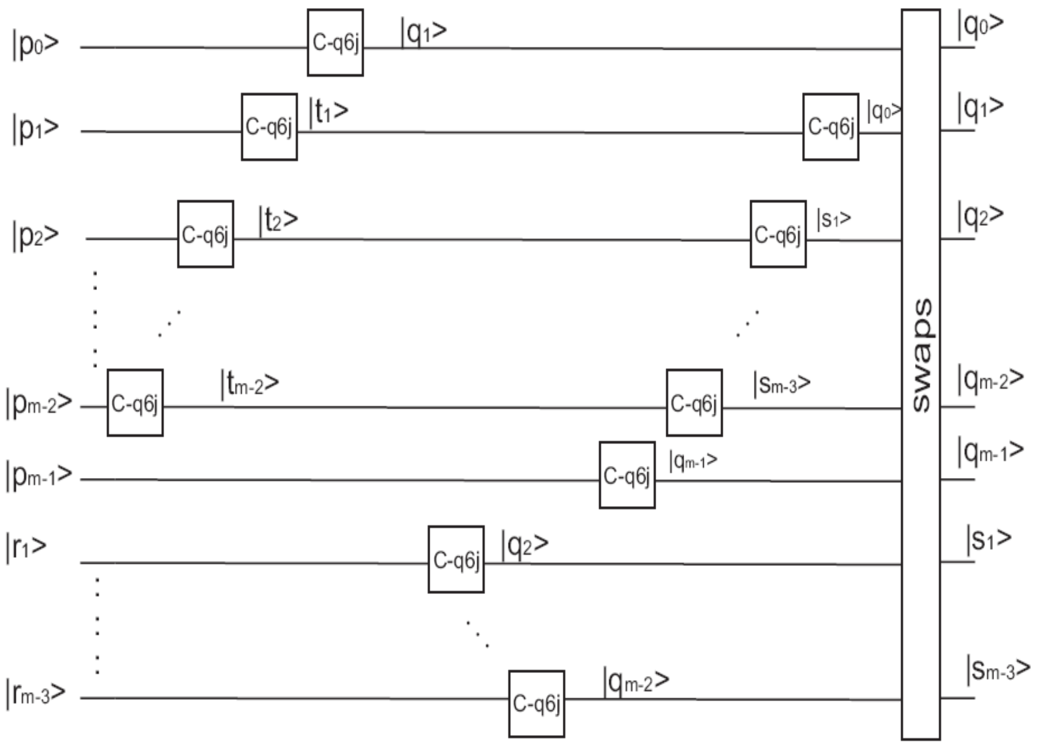


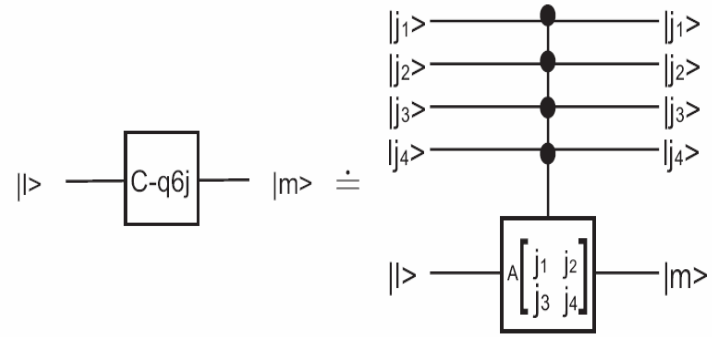
Encoding Kaul states (II)

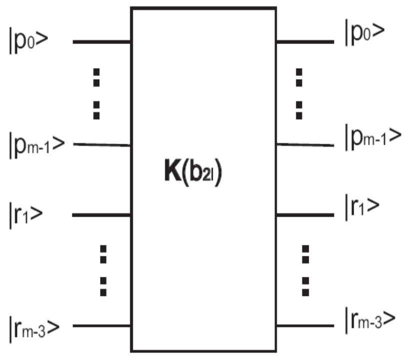


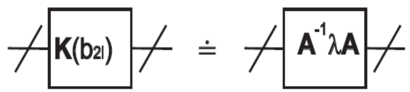
Quantum circuits for

U (σi) and U (q-6j)

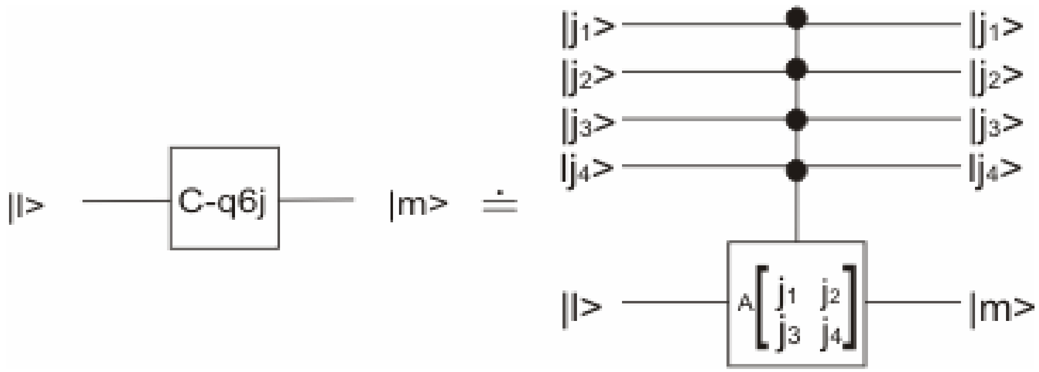






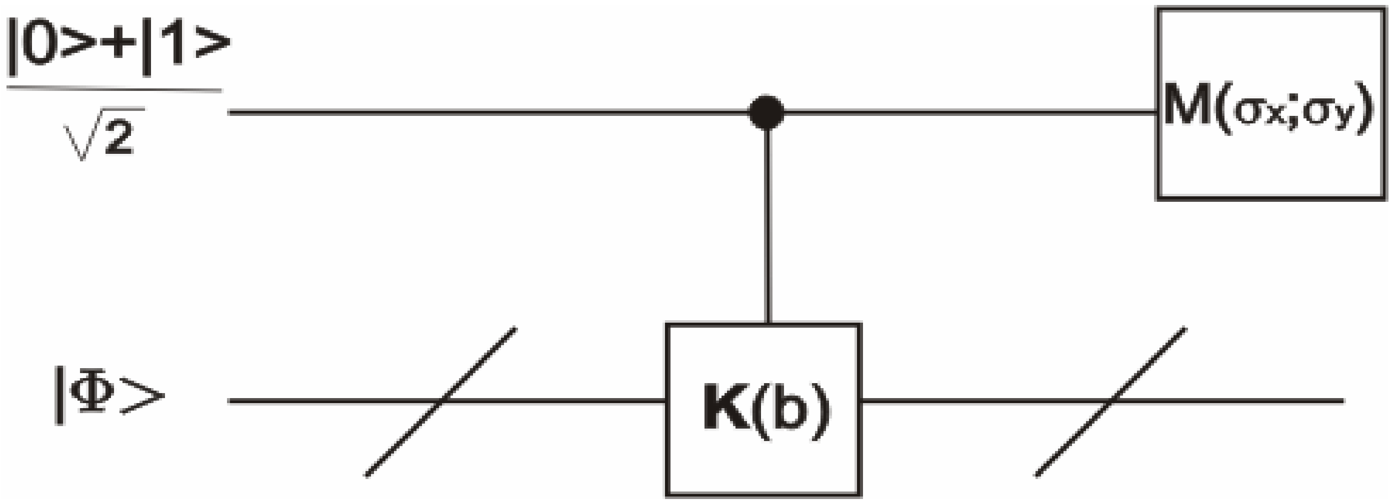


U (q-6j)



The unitary gate acting on the last register is block-diagonal and its dimension is fixed by the coupling constant **k**. It can be efficiently compiled by elementary unitary gates.

U (σi)



Measuring an auxiliary qubit entangled with the system we can obtain an approximate evaluation of the Jones polynomial efficiently

Combinatorial invariants of 3-manifolds

- Any closed 3-dimensional manifold **M** can be presented as the complement of a framed knot (link) **L** embedded in the 3-sphere **S**

$$\mathbf{M} \approx \mathbf{S} \setminus \mathbf{L}$$

- The associated Chern-Simons quantum partition functional is a topological invariant (Reshetikhin-Turaev) that can be expressed as a

  weighted sum of colored Jones polynomial

$$\mathbf{J}\,(\mathbf{L}, \mathbf{q};\, \mathbf{j_1}, \mathbf{j_2}, \ldots, \mathbf{j_N})$$

Efficient quantum algorithms for these invariants in Garnerone, Marzuoli, Rasetti, quant-ph/0703037

3-manifolds
as complements
of knots