Quantum complexity theory

A very brief introduction, with some topology

Clément Maria

INRIA Sophia Antipolis-Méditerranée

QuantAzur seminar

Classical complexity

Some complexity classes (more or less formally)

Definition (Computing)

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n \geq 0} \{0,1\}^n$.

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n\geq 0}\{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n \geq 0}\{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

The complexity is measures as a function of the length n of the input $x \in \{0,1\}^n$.

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n \geq 0} \{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

The complexity is measures as a function of the length n of the input $x \in \{0,1\}^n$.

- **P**: *class of problems L solvable in polynomial time by a classical deterministic computer.*

  Ex: given a graph G and two nodes u, v, is there a (u, v) path of length $\leq k$?

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n\geq 0}\{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

The complexity is measures as a function of the length n of the input $x \in \{0,1\}^n$.

- **P**: *class of problems L solvable in polynomial time by a classical deterministic computer.*

  Ex: given a graph G and two nodes u, v, is there a (u, v) path of length $\leq k$?

  Fix a language $L \in \mathbf{P}$; there exists an "algorithm" and a polynomial p s.t. for any input $x \in \{0,1\}^n$, the algorithm returns *yes* if $x \in L$, and *no* otherwise, in at most $p(n)$ logical operations.

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n\geq 0}\{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

The complexity is measures as a function of the length n of the input $x \in \{0,1\}^n$.

- **NP**: *class of problems L where the yes-instances can be solved in polynomial time, when given a hint of polynomial size.*

  Ex: given a graph G, is there a Hamiltonian cycle (cycle visiting all nodes exactly once) ?
  $\longrightarrow$ the hint is the sequence of nodes forming the Hamiltonian cycle (in a *yes*-instance).
  Hard to find one, easy to verify one is valid.

Some complexity classes (more or less formally)

Definition (Computing)

A **problem** is a language $L \subseteq \{0,1\}^* = \cup_{n\geq 0}\{0,1\}^n$.
Deciding a language L consists of deciding membership of any input word $x \in \{0,1\}^n$ of length n to L:

INPUT $x \in \{0,1\}^n$, **OUTPUT** *yes* if $x \in L$, and *no* o.w.

The complexity is measures as a function of the length n of the input $x \in \{0,1\}^n$.

- **#P**: *class of counting problems.*

  Ex: given a graph, how many Hamiltonian cycles are there ?

Directly from the definitions: $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{P}^{\#\mathbf{P}}$.

Quantum computing

Quantum states

Consider the $\mathbb{C}$-vector space $\mathbb{C}^2$ of basis: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Definition (Qubits)

$|0\rangle$ and $|1\rangle$ are qubits.

Quantum states

Consider the $\mathbb{C}$-vector space $\mathbb{C}^2$ of basis: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Definition (Qubits)

$|0\rangle$ and $|1\rangle$ are qubits. An n-qubit state is, for $b_j \in \{0, 1\}$:

$$|b_1 b_2 \cdots b_n\rangle := |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}.$$

Quantum states

Consider the $\mathbb{C}$-vector space $\mathbb{C}^2$ of basis: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Definition (Qubits)

$|0\rangle$ and $|1\rangle$ are qubits. An n-qubit state is, for $b_j \in \{0,1\}$:

$$|b_1 b_2 \cdots b_n\rangle := |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}.$$

$\longrightarrow$ so far, quite similar to classical words $x \in \{0,1\}^n$.

Quantum states

Consider the $\mathbb{C}$-vector space $\mathbb{C}^2$ of basis: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Definition (Qubits)

$|0\rangle$ and $|1\rangle$ are qubits. An n-qubit state is, for $b_j \in \{0, 1\}$:

$$|b_1 b_2 \cdots b_n\rangle := |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}.$$

Definition (Quantum state)

A quantum state on n qubits is the superposition:

$$\alpha_0 |0\rangle + \cdots + \alpha_{2^n-1} |2^n - 1\rangle, \quad \sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1,$$

or equivalently a norm 1 vector of $\mathbb{C}^{2^n}$.

Quantum gates & measurement

A quantum gate is a **unitary matrix** $U : \mathbb{C}^{2k} \to \mathbb{C}^{2k}, \quad \text{i.e., } U^{-1} = U^*.$

Quantum gates & measurement

A quantum gate is a **unitary matrix** $U : \mathbb{C}^{2k} \to \mathbb{C}^{2k}$, i.e., $U^{-1} = U^*$.

Examples on 1 qubit, in the basis $\{|0\rangle, |1\rangle\}$:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ swaps bits,} \qquad R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \text{ phase gate}$$

Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\quad H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, HH|0\rangle = |0\rangle$.

Quantum gates & measurement

A quantum gate is a **unitary matrix** $U : \mathbb{C}^{2k} \to \mathbb{C}^{2k}$, i.e., $U^{-1} = U^*$.

Examples on 1 qubit, in the basis $\{|0\rangle, |1\rangle\}$:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ swaps bits,} \qquad R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \text{ phase gate}$$

Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\quad H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, HH|0\rangle = |0\rangle$.

Example on 2 qubits, in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$\rightarrow$ flips the second **target** qubit iff the first **control** qubit is 1.

Quantum gates & measurement

A quantum gate is a **unitary matrix** $U : \mathbb{C}^{2k} \to \mathbb{C}^{2k}$, i.e., $U^{-1} = U^*$.

Examples on 1 qubit, in the basis $\{|0\rangle, |1\rangle\}$:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ swaps bits,} \qquad R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \text{ phase gate}$$

Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\quad H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, HH|0\rangle = |0\rangle$.

Example on 2 qubits, in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

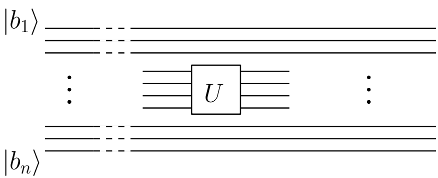
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

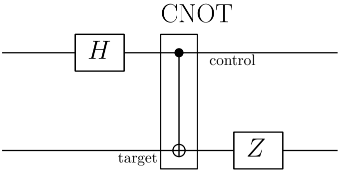
$\to$ flips the second **target** qubit iff the first **control** qubit is 1.

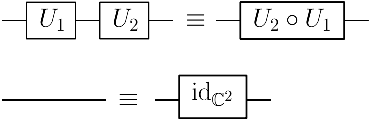
Measuring a quantum state $\sum_{j=0}^{2^n-1} \alpha_j |j\rangle$ returns the (non-superposed) state $|j\rangle$ with probability $|\alpha_i|^2$. (there exist more general projections)

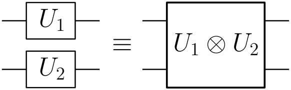
Quantum circuits

Horizontal collection of wires, one per qubit, on which gates are applied from left to right, followed by a final measurement.









can be mixed with "classical" computations.

Quantum complexity

Quantum complexity classes

- **BQP**: the class of “efficiently solvable problem on a quantum computer”.

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

Quantum complexity classes

- **BQP**: the class of “efficiently solvable problem on a quantum computer”.

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,
  - For any $x \in L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \geq \frac{2}{3}$,

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,
  - For any $x \in L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \geq \frac{2}{3}$,
  - For any $x \notin L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \leq \frac{1}{3}$.

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,
  - For any $x \in L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \geq \frac{2}{3}$,
  - For any $x \notin L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \leq \frac{1}{3}$.

  $\longrightarrow$ there is a probably of error, that can be made exponentially small by repeating the computation.

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,
  - For any $x \in L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \geq \frac{2}{3}$,
  - For any $x \notin L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \leq \frac{1}{3}$.

  $\longrightarrow$ there is a probably of error, that can be made exponentially small by repeating the computation.

  Naturally, $\mathbf{P} \subseteq \mathbf{BQP}$.

Quantum complexity classes

- **BQP**: the class of "efficiently solvable problem on a quantum computer".

  Formally, a language $L \in \mathbf{BQP}$ is there exists a *polynomial-time unirform* family of quantum circuits $\{Q_n : n \geq 1\}$, such that:

  - The circuit Q_n takes n-qubits as input, and outputs 1 bit,
  - For any $x \in L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \geq \frac{2}{3}$,
  - For any $x \notin L$ of length n, $\Pr(Q_n(|x\rangle) = 1) \leq \frac{1}{3}$.

  $\longrightarrow$ there is a probably of error, that can be made exponentially small by repeating the computation.

  Naturally, **P** $\subseteq$ **BQP**.

- There is a quantum counterpart to **NP** called **QMA**, with a rich theory of complexity (complete problems, etc). The hint is a quantum state.

The Solovay-Kitaev theorem

• The **infinite** set of all 1-qubit operations plus the 2-qubits CNOT gate is universal, meaning any other unitary can be implemented with them.

The Solovay-Kitaev theorem

• The **infinite** set of all 1-qubit operations plus the 2-qubits CNOT gate is universal, meaning any other unitary can be implemented with them.

Furthermore, one can restrict *efficiently* the set of quantum gate to a (small) **finite** set of gates, allowing an arbitrary small error:

The Solovay-Kitaev theorem

• The **infinite** set of all 1-qubit operations plus the 2-qubits CNOT gate is universal, meaning any other unitary can be implemented with them.

Furthermore, one can restrict *efficiently* the set of quantum gate to a (small) **finite** set of gates, allowing an arbitrary small error:

Theorem (Solovay-Kitaev)

Let G be a **finite** *set of elements (and their inverses) of* $\mathbf{SU(d)}$*, and assume the group* $\langle G \rangle$ *they generate is* **dense** *in* $\mathbf{SU(d)}$*.*
Then, there exists a constant c such that, for any $\varepsilon > 0$ and element $M \in \mathbf{SU(d)}$, there exists $O(\log^c(1/\varepsilon))$ many elements $U_1, \dots, U_{O(\log^c(1/\varepsilon))}$ of G such that:

$$||U_{O(\log^c(1/\varepsilon))} \cdots U_1 - M|| < \varepsilon$$

The Solovay-Kitaev theorem

• The **infinite** set of all 1-qubit operations plus the 2-qubits CNOT gate is universal, meaning any other unitary can be implemented with them.

Furthermore, one can restrict *efficiently* the set of quantum gate to a (small) **finite** set of gates, allowing an arbitrary small error:

Theorem (Solovay-Kitaev)

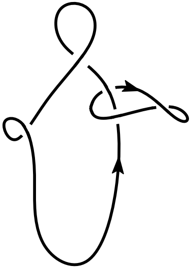
Let G be a **finite** *set of elements (and their inverses) of $\mathbf{SU(d)}$, and assume the group $\langle G\rangle$ they generate is* **dense** *in $\mathbf{SU(d)}$.*
Then, there exists a constant c such that, for any $\varepsilon > 0$ and element $M \in \mathbf{SU(d)}$, there exists $O(\log^c(1/\varepsilon))$ many elements $U_1, \dots, U_{O(\log^c(1/\varepsilon))}$ of G such that:

$$||U_{O(\log^c(1/\varepsilon))} \cdots U_1 - M|| < \varepsilon$$

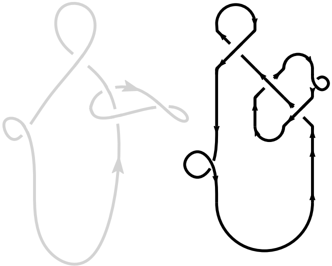
$\Longrightarrow$ there are finite sets of gates dense in $\mathbf{SU(2)}$. Several finite sets of gates are used depending on applications.

Quantum topology

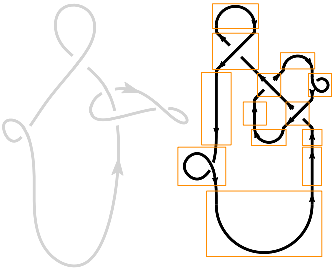
Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]



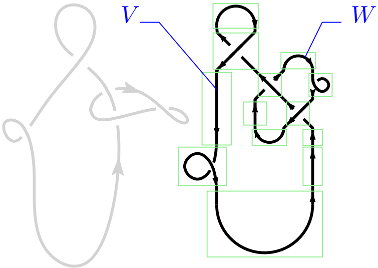
Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]



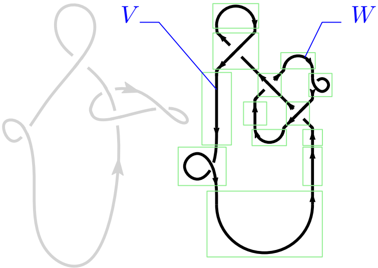
Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]

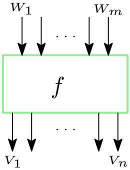


Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]



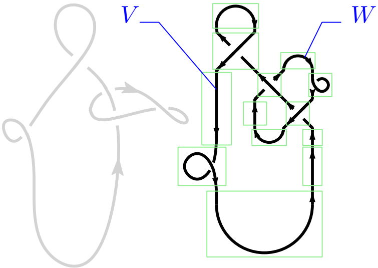
Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]

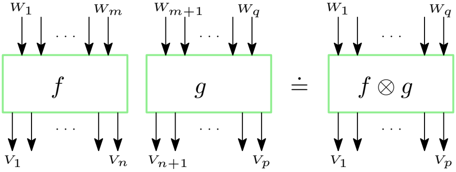




$$f\colon V_1 \otimes \ldots \otimes V_n \to W_1 \otimes \ldots \otimes W_m$$

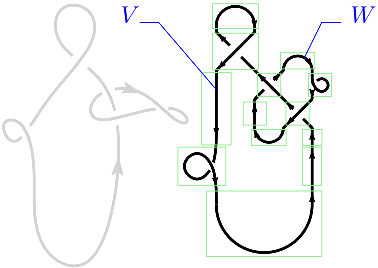
Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]

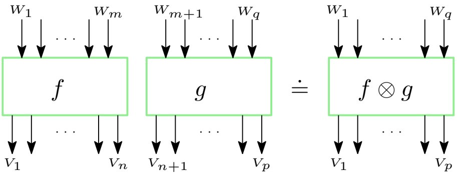


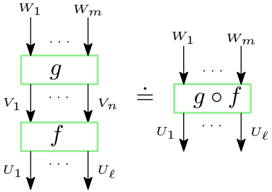


$f \otimes g \colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]



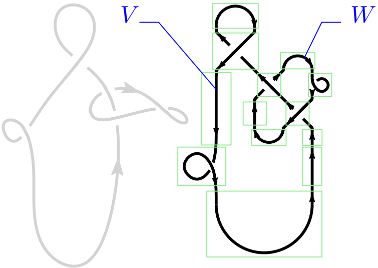




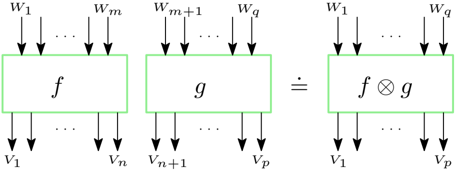
$f \otimes g \colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

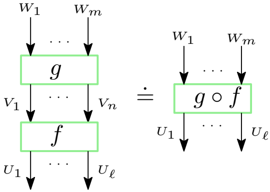
$g \circ f \colon U_1 \otimes \ldots \otimes U_\ell$

Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]



V  $\doteq \mathrm{id}_V \colon V \to V$ $\qquad$ V  $\doteq \mathrm{id}_{V^*}$

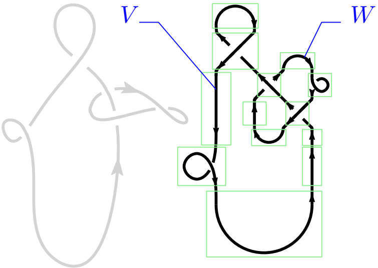


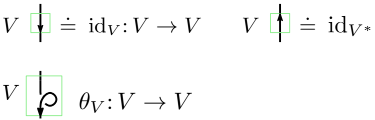


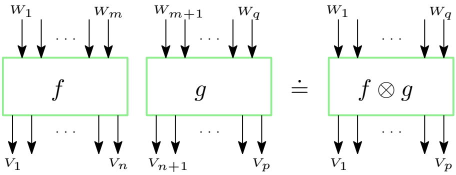
$f \otimes g \colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

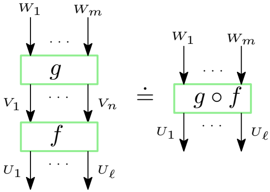
$g \circ f \colon U_1 \otimes \ldots \otimes U_\ell$

Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]





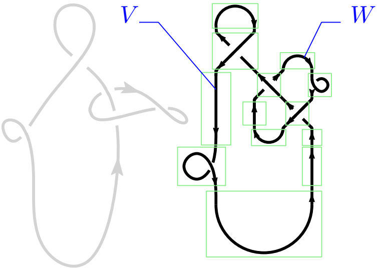




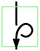
$f \otimes g\colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

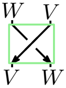
$g \circ f\colon U_1 \otimes \ldots \otimes U_\ell$

Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]

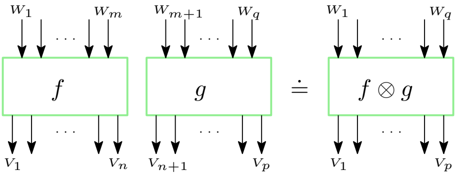


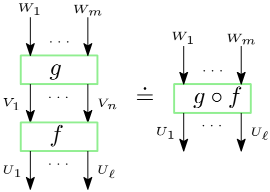
V  $\doteq \mathrm{id}_V\colon V \to V$ $\quad$ V  $\doteq \mathrm{id}_{V^*}$

V  $\theta_V\colon V \to V$



$c_{V,W}\colon V \otimes W \to W \otimes V$

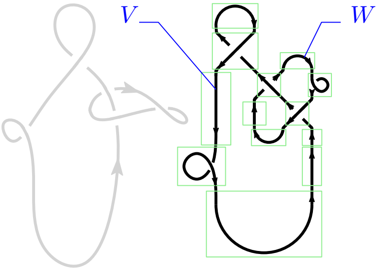


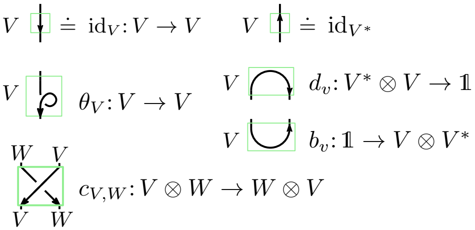


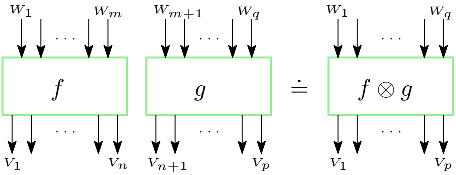
$f \otimes g\colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

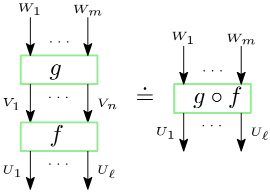
$g \circ f\colon U_1 \otimes \ldots \otimes U_\ell$

Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]





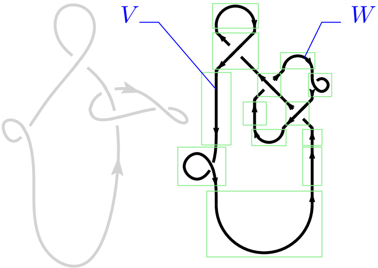




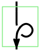
$f \otimes g \colon V_1 \otimes \ldots \otimes V_p \to W_1 \otimes \ldots W_q$

$g \circ f \colon U_1 \otimes \ldots \otimes U_\ell$

Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]

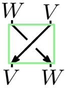


V  $\doteq \mathrm{id}_V\colon V \to V$ V  $\doteq \mathrm{id}_{V^*}$

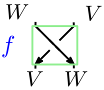
V  $\theta_V\colon V \to V$

V  $d_v\colon V^* \otimes V \to \mathbb{1}$

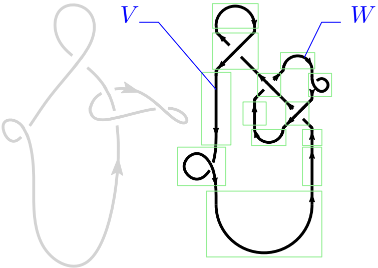
V  $b_v\colon \mathbb{1} \to V \otimes V^*$



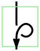
$c_{V,W}\colon V \otimes W \to W \otimes V$



Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]

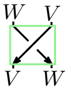


V  $\doteq \ \mathrm{id}_V \colon V \to V$ V  $\doteq \ \mathrm{id}_{V^*}$

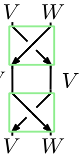
V  $\theta_V \colon V \to V$

V  $d_v \colon V^* \otimes V \to \mathbb{1}$

V  $b_v \colon \mathbb{1} \to V \otimes V^*$

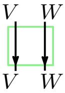


$c_{V,W} \colon V \otimes W \to W \otimes V$

$c_{W,V}$ 

f

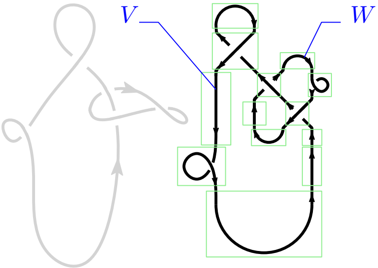
$\doteq$

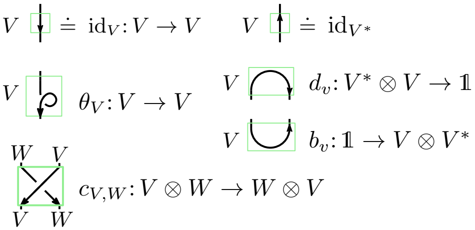


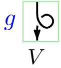
$\mathrm{id}_{V \otimes W}$

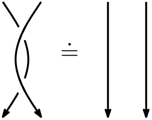
 $\doteq$ 

Penrose functor: Diagram $\to$ (algebraic) invariant
[Sketch of construction]

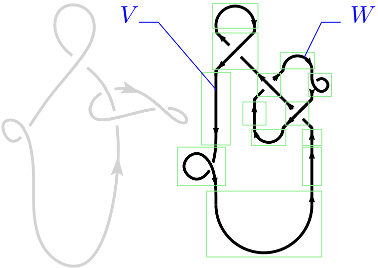




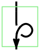




Penrose functor: Diagram → (algebraic) invariant
[Sketch of construction]

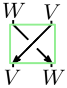


V  $\doteq$ $\mathrm{id}_V\colon V \to V$ V  $\doteq$ id_{V^*}

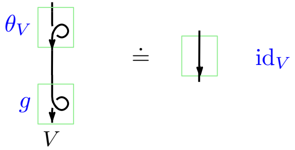
V  $\theta_V\colon V \to V$

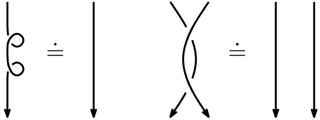
V  $d_v\colon V^* \otimes V \to \mathbb{1}$

V  $b_v\colon \mathbb{1} \to V \otimes V^*$

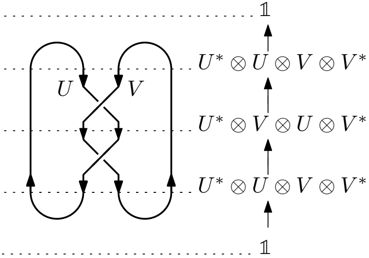


$c_{V,W}\colon V \otimes W \to W \otimes V$





Penrose functor: Diagram $\to$ (algebraic) invariant



$d_U \otimes d_{V^*}$

$\mathrm{id}_{U^*} \otimes c_{U,V} \otimes \mathrm{id}_{V^*}$

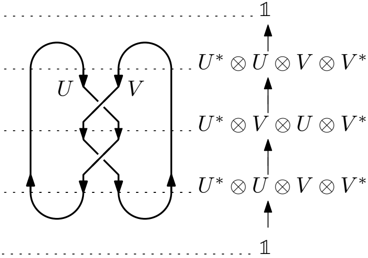
$\mathrm{id}_{U^*} \otimes c_{V,U} \otimes \mathrm{id}_{V^*}$

$b_{U^*} \otimes b_V$

Theorem (Reshetikhin, Turaev)

A ribbon category associates to every coloured *ribbon diagram a morphism* $\mathbb{1} \to \mathbb{1}$. *It is an isotopy invariant.*

Penrose functor: Diagram → (algebraic) invariant



$d_U \otimes d_{V^*}$

$\mathrm{id}_{U^*} \otimes c_{U,V} \otimes \mathrm{id}_{V^*}$

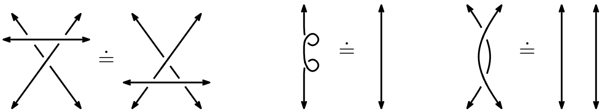
$\mathrm{id}_{U^*} \otimes c_{V,U} \otimes \mathrm{id}_{V^*}$

$b_{U^*} \otimes b_V$

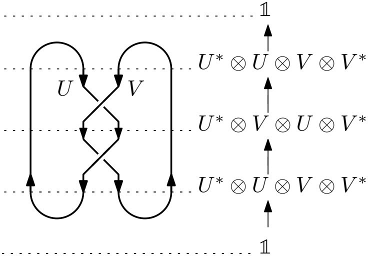
Theorem (Reshetikhin, Turaev)

A ribbon category associates to every coloured *ribbon diagram a morphism $\mathbb{1} \to \mathbb{1}$. It is an isotopy invariant.*

Proof: any isotopy of ribbon diagrams may be described by a sequence of *Reidemeister moves*. $\longrightarrow$ inv. by design.



Penrose functor: Diagram $\to$ (algebraic) invariant



$d_U \otimes d_{V^*}$

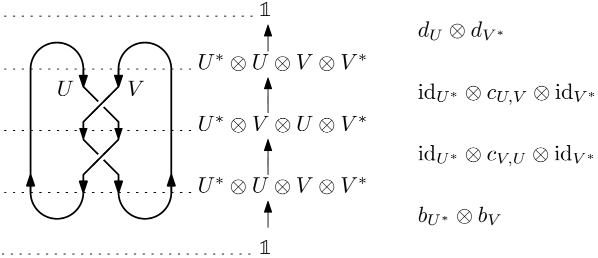
$\mathrm{id}_{U^*} \otimes c_{U,V} \otimes \mathrm{id}_{V^*}$

$\mathrm{id}_{U^*} \otimes c_{V,U} \otimes \mathrm{id}_{V^*}$

$b_{U^*} \otimes b_V$

These invariants have a rich computational complexity, around the classes **#P** and **BQP**. They create links between classical and quantum complexity, and offer topological tools for their study.

Penrose functor: Diagram $\to$ (algebraic) invariant

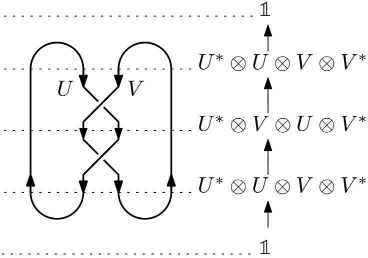


These invariants have a rich computational complexity, around the classes **#P** and **BQP**. They create links between classical and quantum complexity, and offer topological tools for their study.

$$\tau(K)$$

$$\mathbf{BQP} \quad \subseteq \quad \mathbf{PostBQP} \quad = \mathbf{PP} \quad \text{and} \quad \mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$$

Penrose functor: Diagram → (algebraic) invariant



$d_U \otimes d_{V^*}$

$\mathrm{id}_{U^*} \otimes c_{U,V} \otimes \mathrm{id}_{V^*}$

$\mathrm{id}_{U^*} \otimes c_{V,U} \otimes \mathrm{id}_{V^*}$

$b_{U^*} \otimes b_V$

These invariants have a rich computational complexity, around the classes **#P** and **BQP**. They create links between classical and quantum complexity, and offer topological tools for their study.

$$\tau(K)$$

$$\mathbf{BQP} \subseteq \mathbf{PostBQP} = \mathbf{PP} \quad \text{and} \quad \mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$$

Thank you!