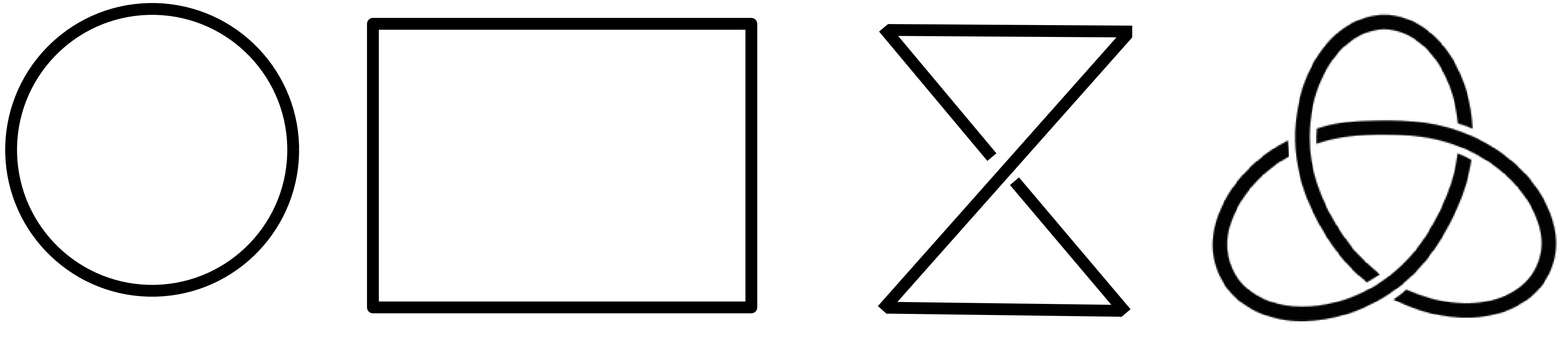
Topological Quantum Computing
What gives?

Henrique Ennes
CEMRACS 2025
05/08/2025

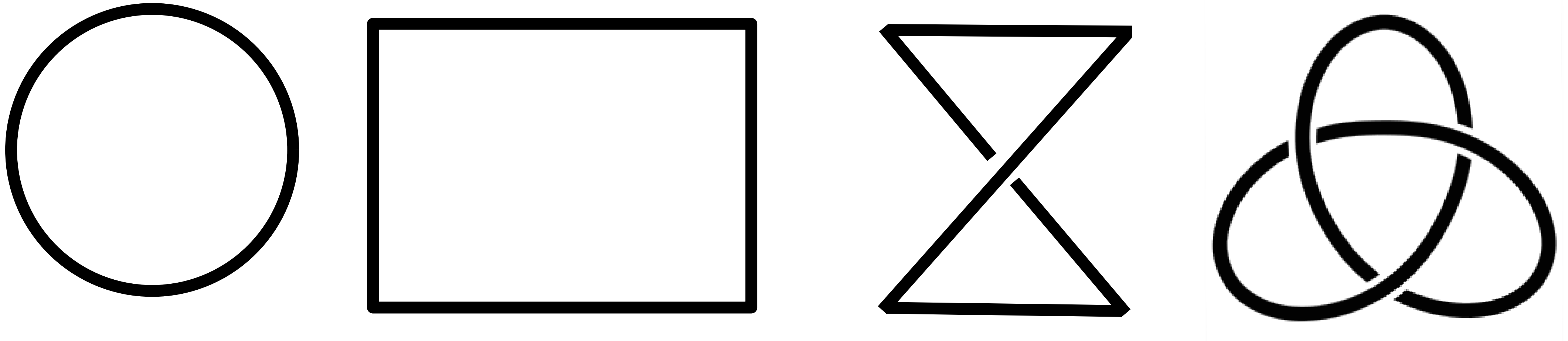
Knots

Knots are embeddings of the circle in $\mathbb{R}^3$.



Knots

Knots are embeddings of the circle in $\mathbb{R}^3$.



Two knots will be called *isotopic* if we can bring one to the other without tearing them apart.

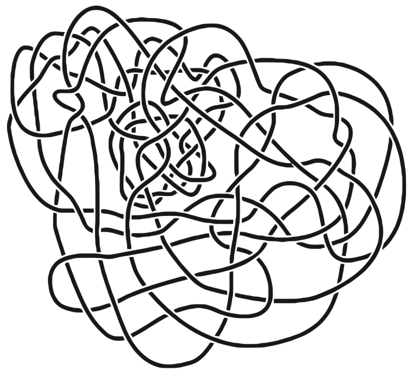
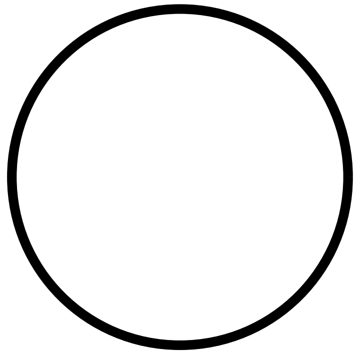
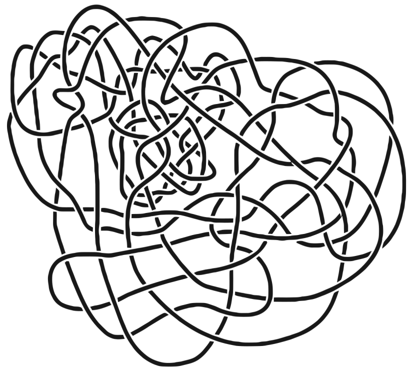
ISOTOPIC

NON-ISOTOPIC

UNIVERSITÉ CÔTE D'AZUR Inria

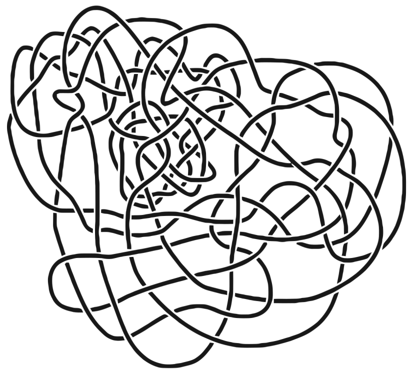
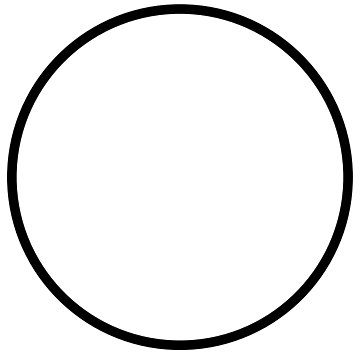
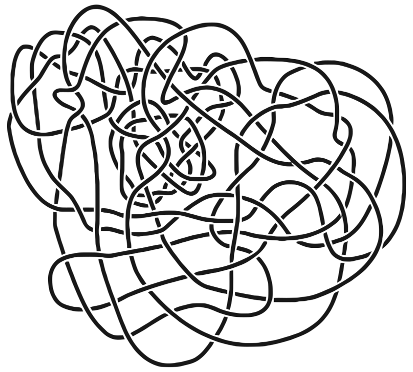
Knots

The problem of telling isotopic knots apart is computationally very hard.

PROBLEM			STATUS
	“ = ”		NP ∩ coNP
	“ = ”		DECIDABLE

Knots

The problem of telling isotopic knots apart is computationally very hard.

PROBLEM			STATUS
	" = "		NP $\cap$ coNP
	" = "		DECIDABLE

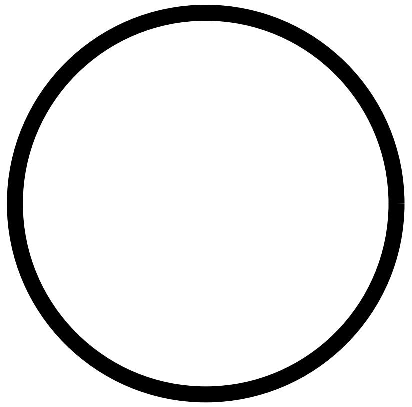
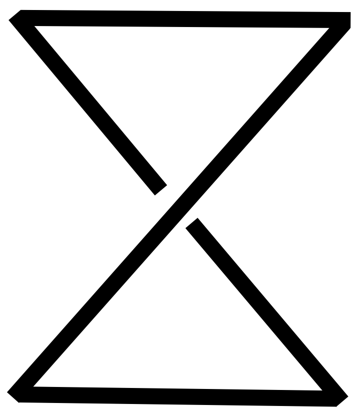
We can use **invariants** to get approximations to this problem

$$K \text{ is isotopic to } K' \implies \langle K \rangle = \langle K' \rangle$$

UNIVERSITÉ CÔTE D'AZUR Inria

Knots

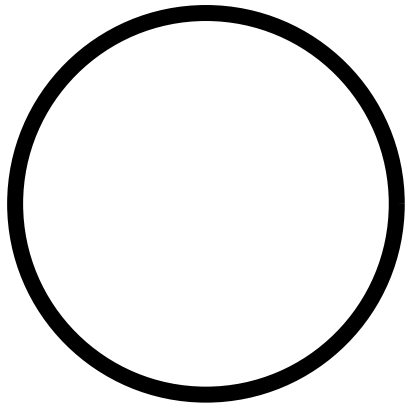
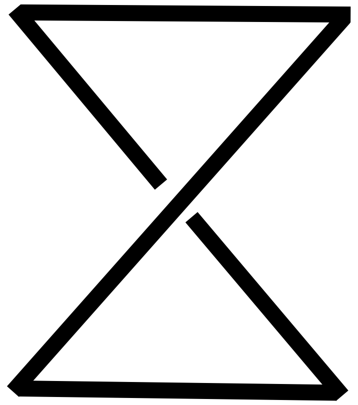
Polynomials give a nice list of invariants

$V_t = \Bigg($  $\Bigg) = 1$ $\quad$ $V_t = \Bigg($  $\Bigg) = 1$

$V_t = \Bigg($  $\Bigg) = t + t^3 - t^4$

Knots

Polynomials give a nice list of invariants

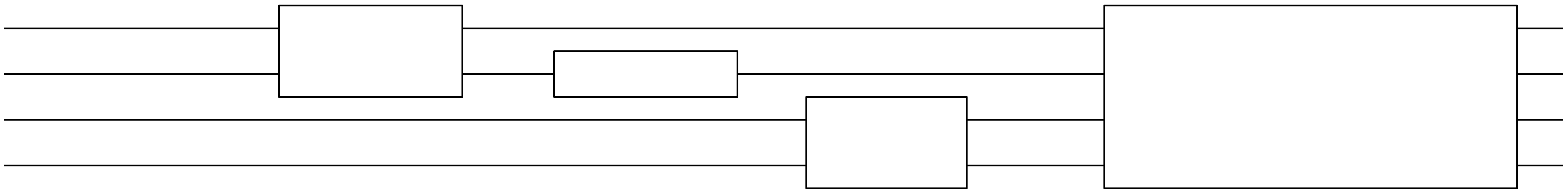
$V_t = \Big($  $\Big) = 1$ $\qquad V_t = \Big($  $\Big) = 1$

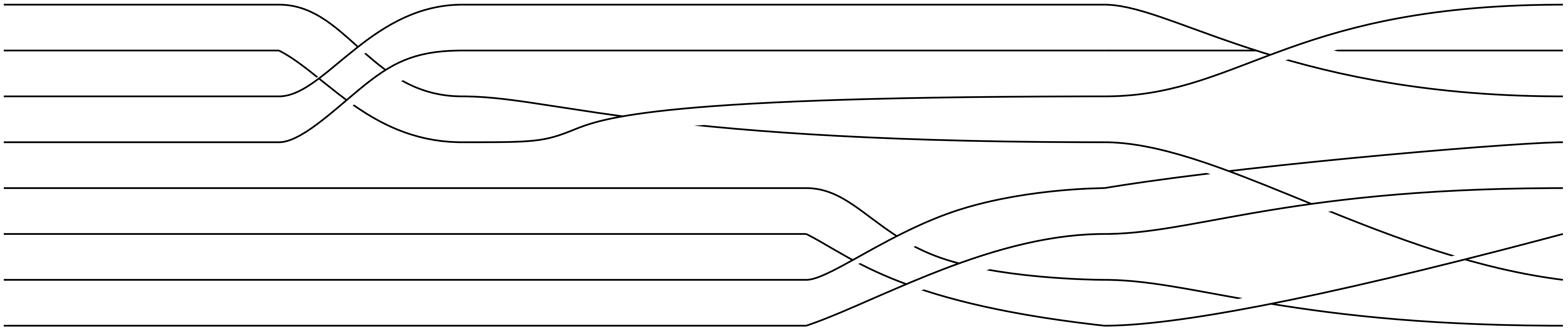
$V_t = \Big($  $\Big) = t + t^3 - t^4$

Theorem (Vertigan, Kuperberg):
Computing (or even well-approximating) the Jones polynomial at some values of t is #P-hard.

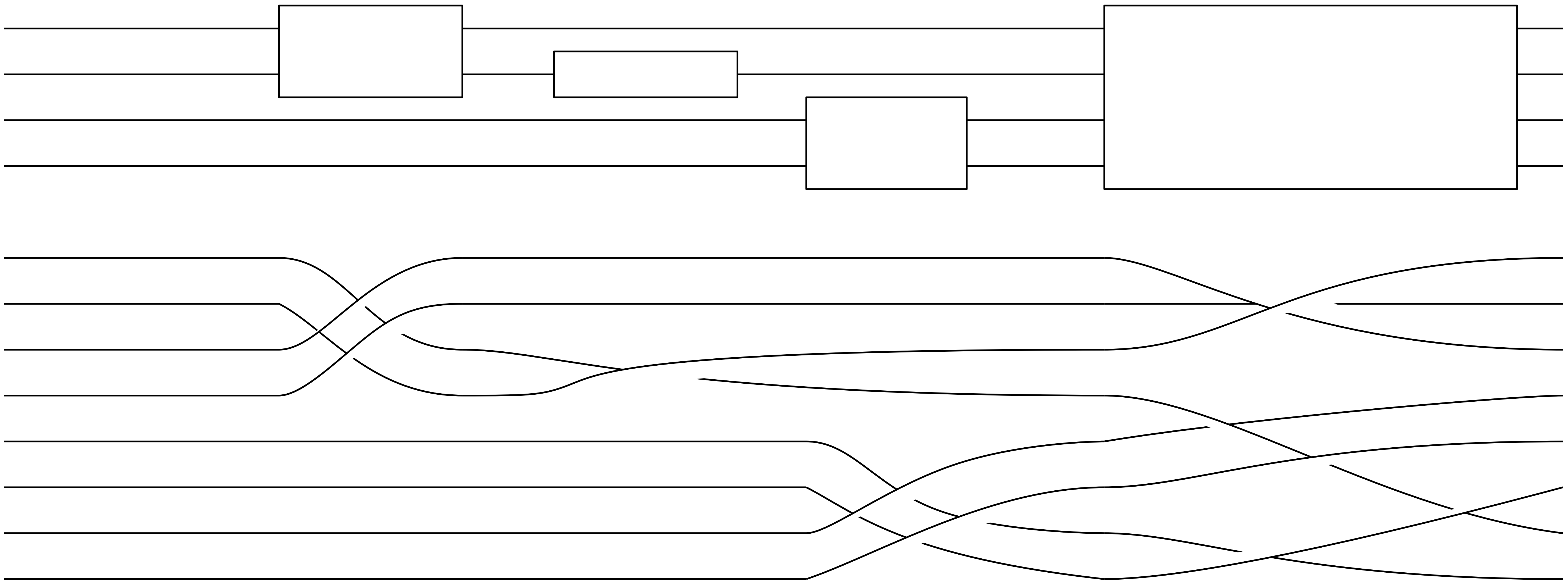
UNIVERSITÉ CÔTE D'AZUR Inria

And where is quantum?





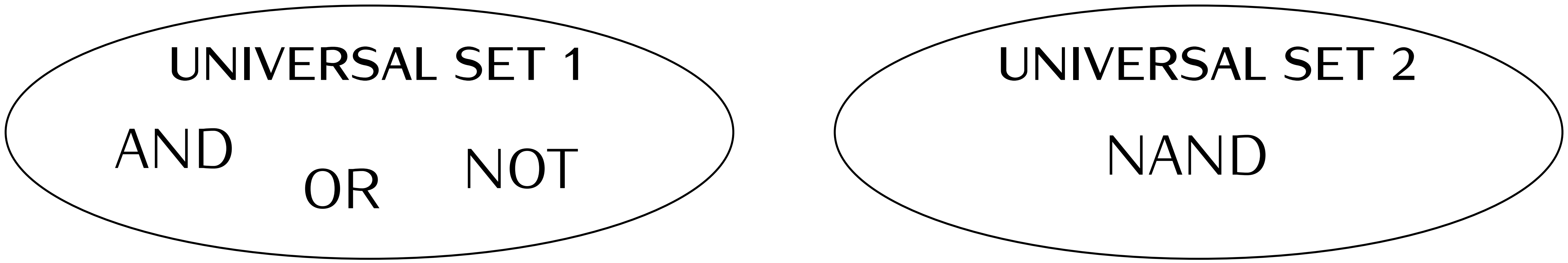
And where is quantum?



$$|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2 \approx |V_t(L)|^2/|t^{1/2}+t^{-1/2}|^{4n}$$

Solovay-Kitaev Theorem

We call a set of classical gates $\mathcal{G}$ **universal** if every Boolean function can be written using it.



Solovay-Kitaev Theorem

We call a set of classical gates $\mathcal{G}$ **universal** if every Boolean function can be written using it.

UNIVERSAL SET 1

AND OR NOT

UNIVERSAL SET 2

NAND

We call a set of quantum gates $\mathcal{G}$ **universal** if every matrix $U \in \mathrm{PU}(4)$ can be **approximated** up to any error ϵ using it.

UNIVERSAL SET 1

H CNOT $\pi/8$

UNIVERSAL SET 2

TOFFOLI X H

Solovay-Kitaev Theorem

Solovay-Kitaev Theorem

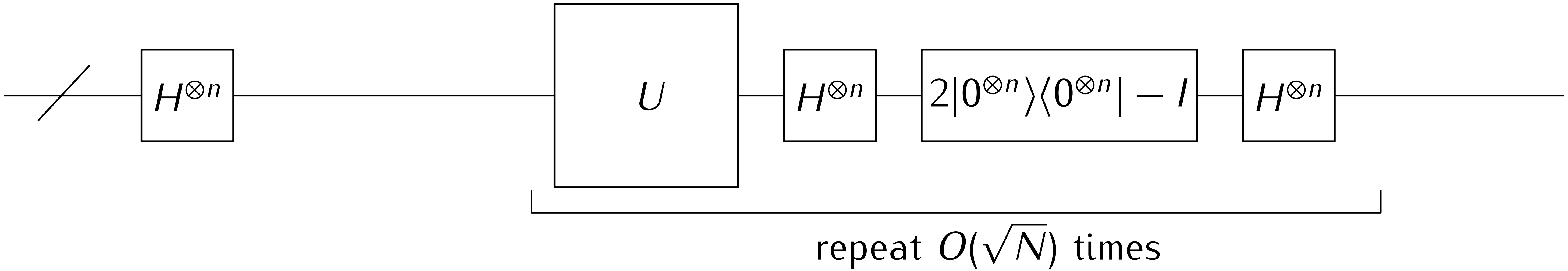
Let $\mathcal{G} = \{G_1, \ldots, G_g, G_1^{-1}, \ldots, G_g^{-1}\}$ be a finite set of matrix generators such that $\langle \mathcal{G} \rangle$ is dense in PU(4). Then

- $\mathcal{G}$ is universal;
- any 2-qubit operation can be approximated using $O(\log^{1.44\ldots}(1/\epsilon))$ many gates.

Solovay-Kitaev Theorem

Solovay-Kitaev Theorem
Let $\mathcal{G} = \{G_1, \dots, G_g, G_1^{-1}, \dots, G_g^{-1}\}$ be a finite set of matrix generators such that $\langle \mathcal{G} \rangle$ is dense in PU(4). Then

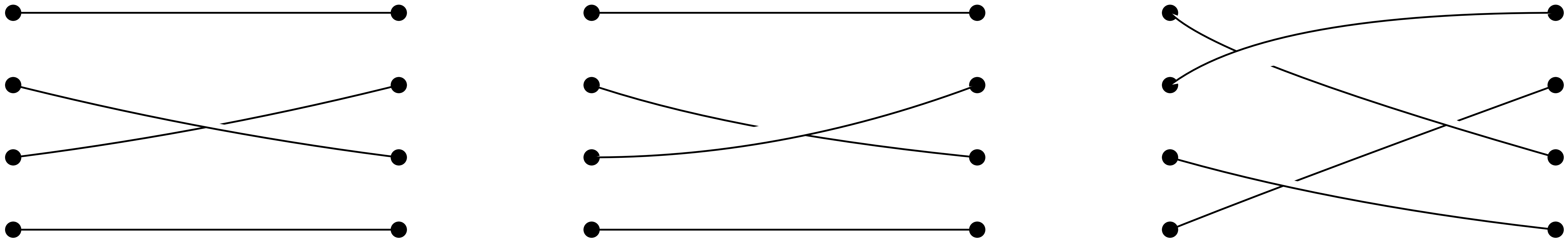
- $\mathcal{G}$ is universal;
- any 2-qubit operation can be approximated using $O(\log^{1.44\dots}(1/\epsilon))$ many gates.



By changing the gates to $\mathcal{G}$, we need only $O(\sqrt{N}\log^c(N/\epsilon))$ gates for an error of at most ϵ instead of $O(N/\epsilon)$ =CLASSICAL TIME.

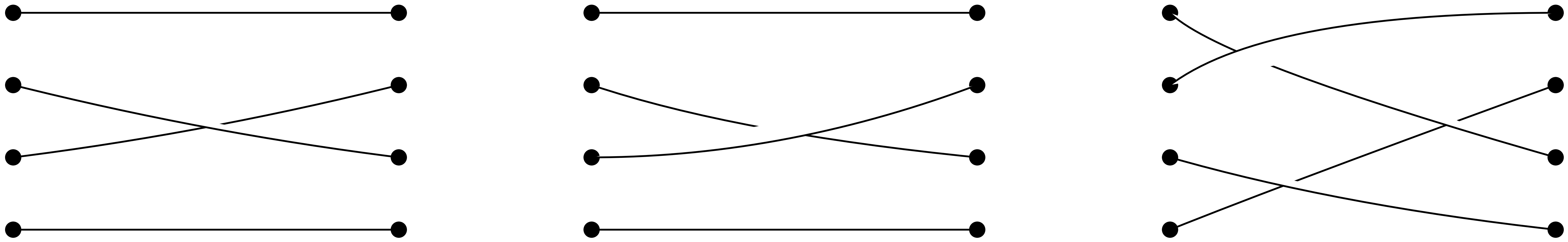
A group for knots

Let us consider the **braids** of n strands, B_n

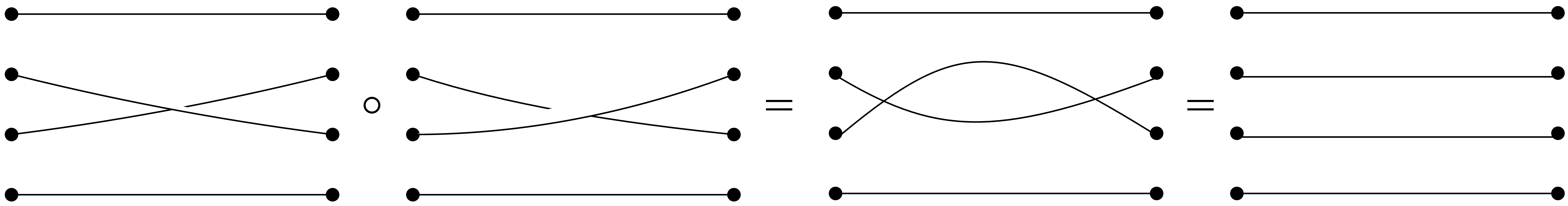


A group for knots

Let us consider the **braids** of n strands, B_n

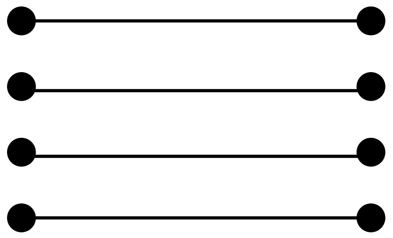
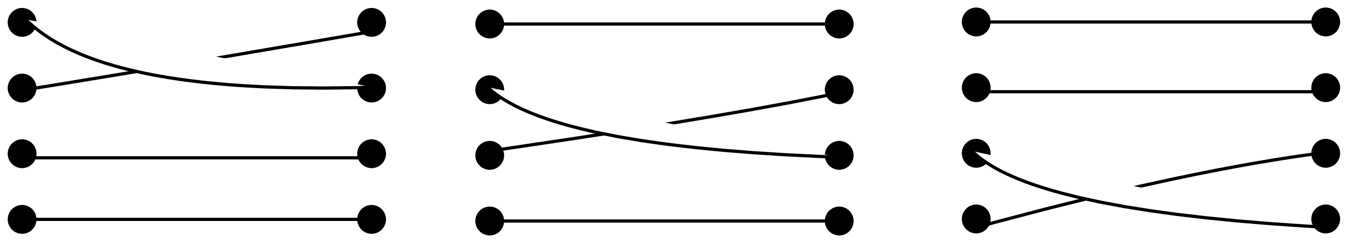
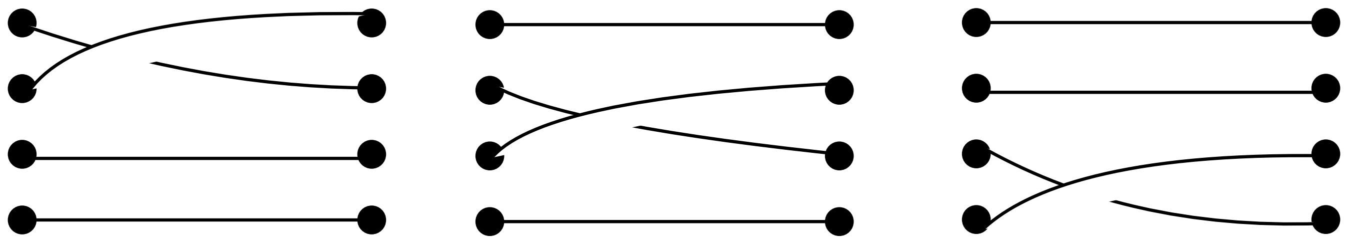


We can consider the composition of braids



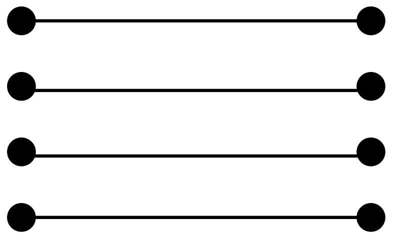
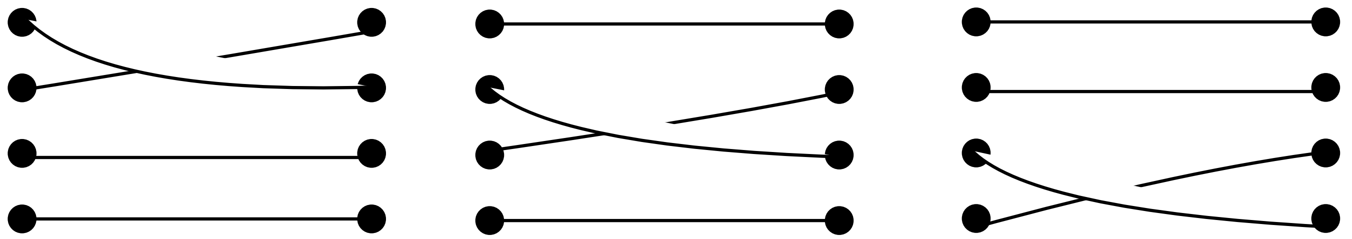
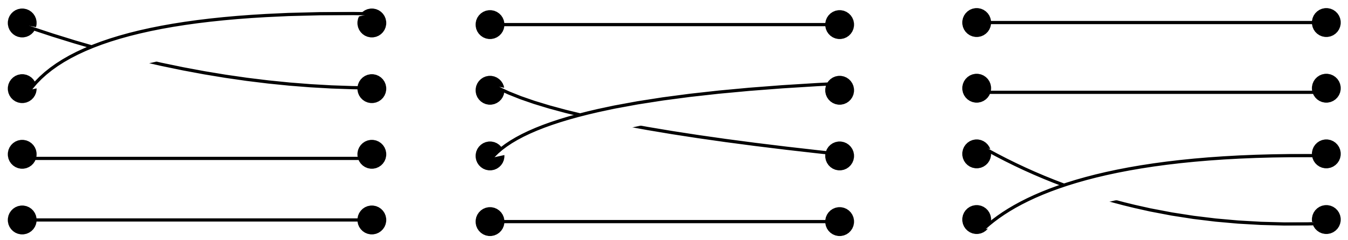
A group for knots

The n braid group B_n has

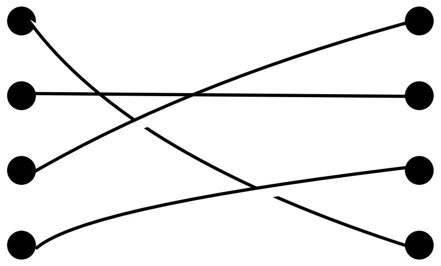
- identity 
- generators $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ 
- inverses 

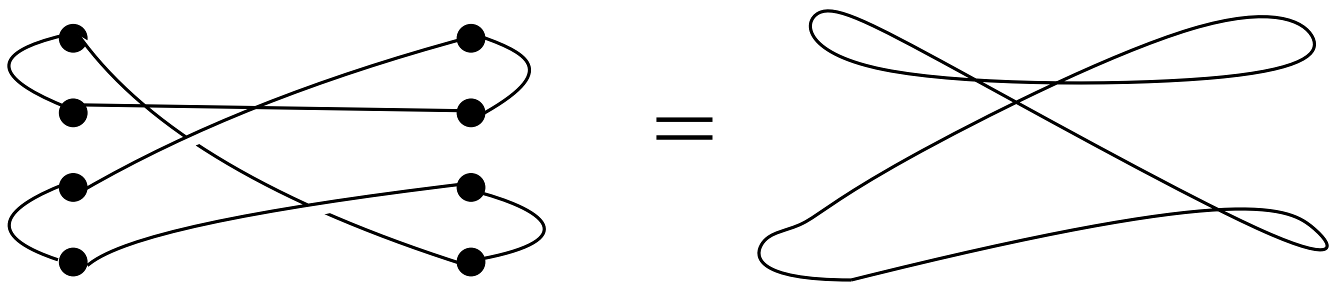
A group for knots

The n braid group B_n has

- identity 
- generators $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ 
- inverses 

Every knot can be obtained by closing braids

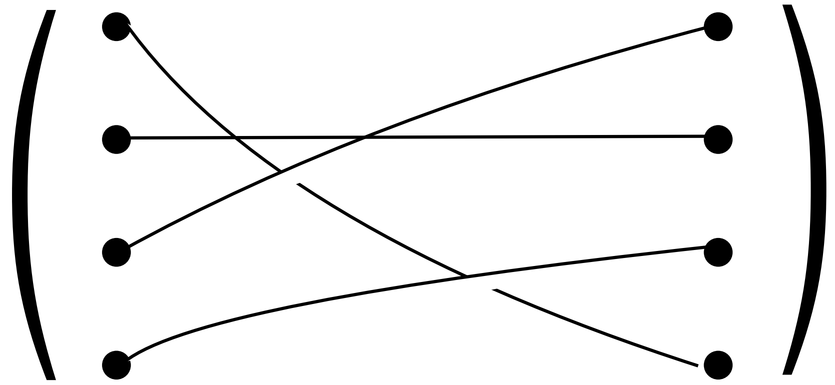




$b \in B_n$

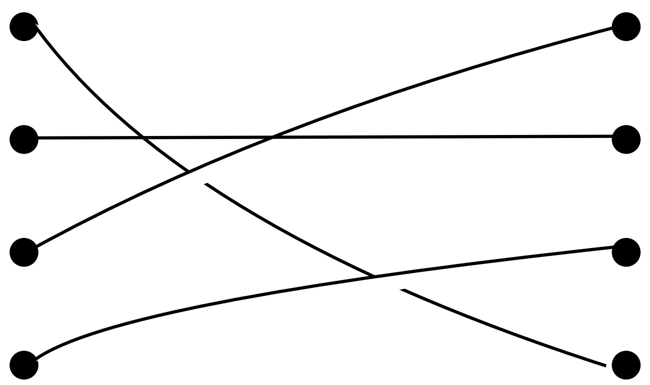
A group for knots

The **(unitary) Jones representations** of the braid groups B_n at value t are homomorphisms $\rho_{n,t} : B_n \to \mathrm{PU}(n')$

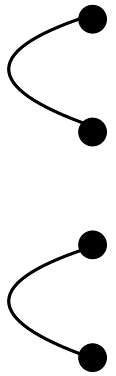
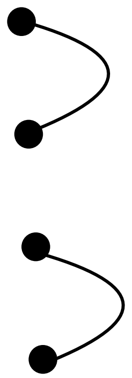
$\rho_{n,t}$  $= U$

A group for knots

The **(unitary) Jones representations** of the braid groups B_n at value t are homomorphisms $\rho_{n,t} : B_n \to \mathrm{PU}(n')$

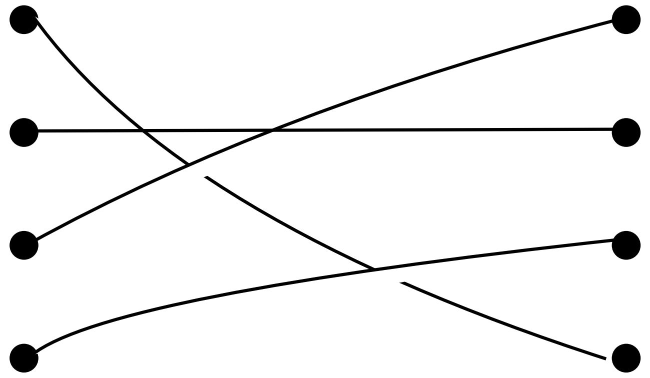
$\rho_{n,t}\Big($  $\Big) = U$

If we vectorize the closure

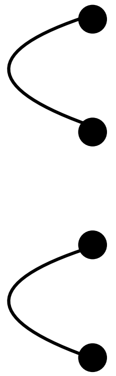
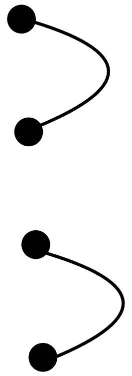
 $\mapsto \langle 0| \in (\mathbb{C}^{n'})^*$  $\mapsto |0\rangle \in \mathbb{C}^{n'}$

A group for knots

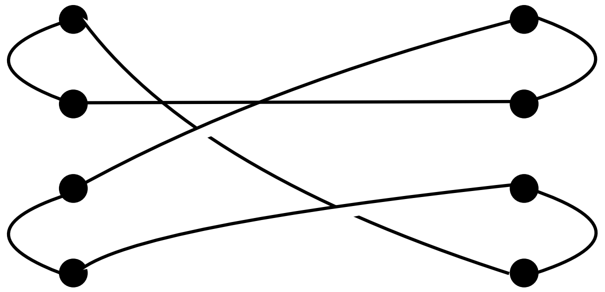
The **(unitary) Jones representations** of the braid groups B_n at value t are homomorphisms $\rho_{n,t} : B_n \to \mathrm{PU}(n')$

$\rho_{n,t}\Big($  $\Big) = U$

If we vectorize the closure

 $\mapsto \langle 0| \in (\mathbb{C}^{n'})^*$  $\mapsto |0\rangle \in \mathbb{C}^{n'}$

we have Jones polynomials at t (up to a factor)

$V_{n,t}\Big($  $\Big) = \frac{1}{-(t^{1/2}+t^{-1/2})t^c}\langle 0|U|0\rangle$

UNIVERSITÉ CÔTE D'AZUR Inria

Topological quantum computing

Theorem (Freedman, Larsen, Wang):
When t is certain roots of the unity, $\rho_{n,t}(B_n)$ is dense in $\mathrm{PU}(n')$ for all $n \geq 4$.

Topological quantum computing

Theorem (Freedman, Larsen, Wang):
When t is certain roots of the unity, $\rho_{n,t}(B_n)$ is dense in $\mathrm{PU}(n')$ for all $n \geq 4$.

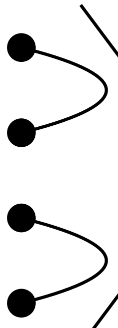
Given a circuit $C = U_1 \circ \cdots \circ U_m$ on n qubits, we can find a knot whose Jones polynomial is ϵ-close to $\langle 0^{\otimes n} | C | 0^{\otimes n} \rangle$.

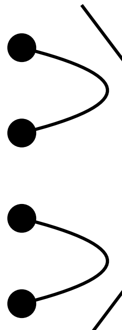
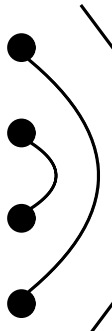
Topological quantum computing

Theorem (Freedman, Larsen, Wang):
When t is certain roots of the unity, $\rho_{n,t}(B_n)$ is dense in $\mathrm{PU}(n')$ for all $n \geq 4$.

Given a circuit $C = U_1 \circ \cdots \circ U_m$ on n qubits, we can find a knot whose Jones polynomial is ϵ-close to $\langle 0^{\otimes n} | C | 0^{\otimes n} \rangle$.

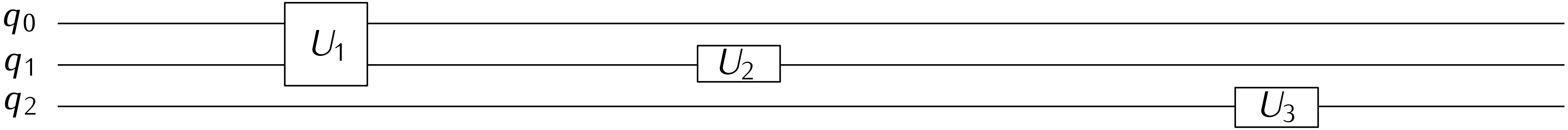
1. Represent $\mathbb{C}^2$ with a basis

$|0\rangle \mapsto \frac{1}{t^{1/2}+t^{-1/2}}$ |  $\rangle$

$|1\rangle \mapsto \frac{1}{\sqrt{(t+1+t^{-1})(t^{1/2}+t^{-1/2})}}$ |  $\rangle$ $+ \frac{1}{\sqrt{(t+1+t^{-1})(t^{1/2})}}$ |  $\rangle$

Topological quantum computing

2. Apply Solovay-Kitaev to represent each gate of the circuit with $\rho_{4n,t}(\sigma_i)$

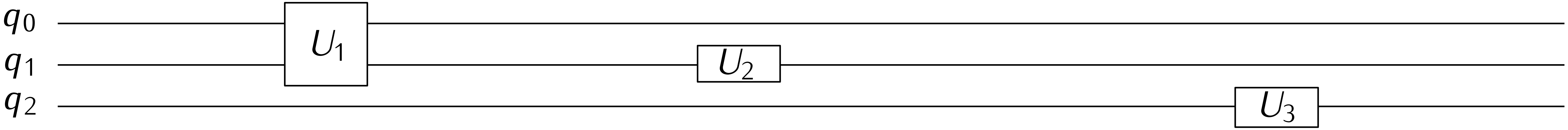


Solovay-Kitaev's output

$\rho_{12,t}(\sigma_1 \sigma_4 \sigma_7^{-1})$ $\rho_{12,t}(\sigma_5)$ $\rho_{12,t}(\sigma_{11}^{-1} \sigma_{10})$

Topological quantum computing

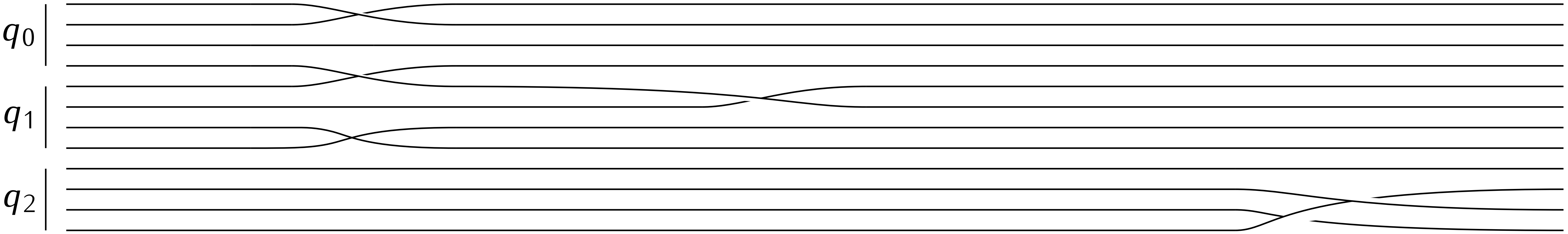
2. Apply Solovay-Kitaev to represent each gate of the circuit with $\rho_{4n,t}(\sigma_i)$



Solovay-Kitaev's output

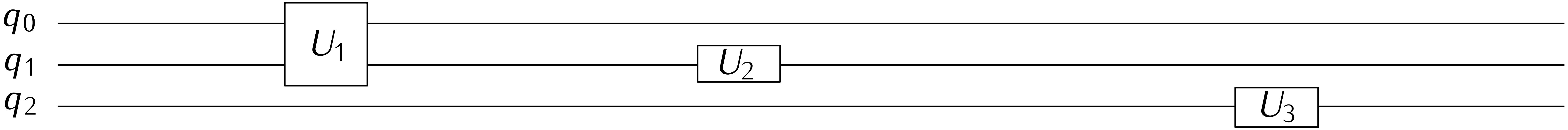
$\rho_{12,t}(\sigma_1 \sigma_4 \sigma_7^{-1})$ $\quad$ $\rho_{12,t}(\sigma_5)$ $\quad$ $\rho_{12,t}(\sigma_{11}^{-1} \sigma_{10})$

3. Find the braid given by the σ_i



Topological quantum computing

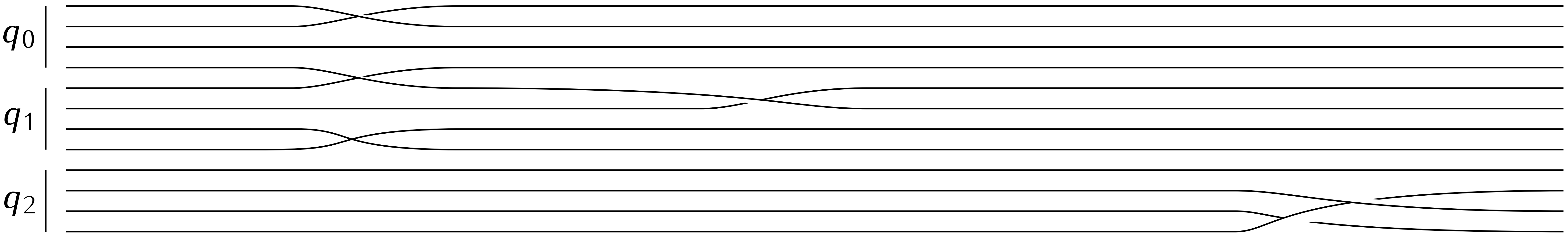
2. Apply Solovay-Kitaev to represent each gate of the circuit with $\rho_{4n,t}(\sigma_i)$



Solovay-Kitaev's output

$\rho_{12,t}(\sigma_1\sigma_4\sigma_7^{-1})$ $\rho_{12,t}(\sigma_5)$ $\rho_{12,t}(\sigma_{11}^{-1}\sigma_{10})$

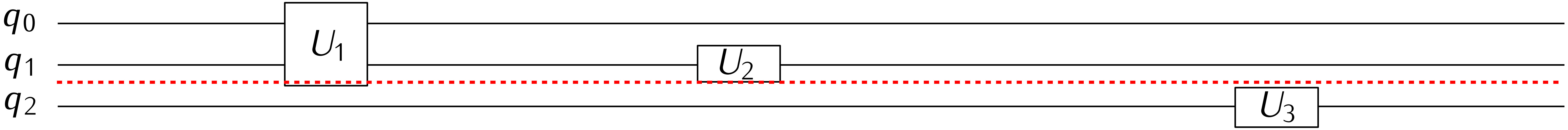
3. Find the braid given by the σ_i



4. $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2 \approx C|V_t(L)|^2$

Topological quantum computing

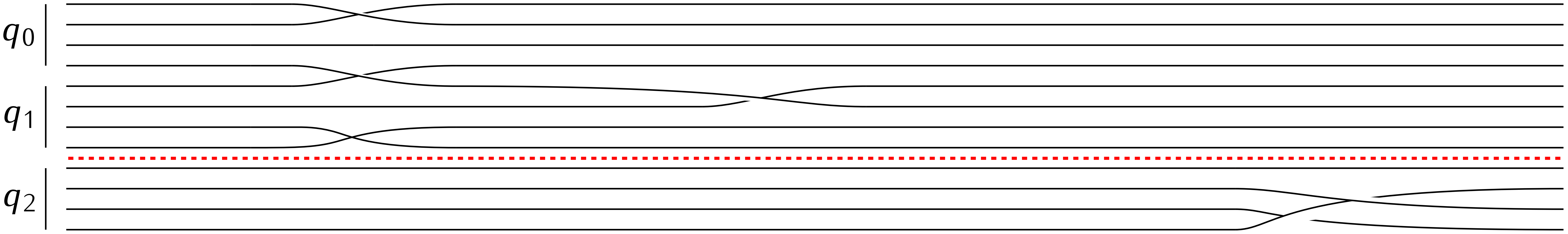
2. Apply Solovay-Kitaev to represent each gate of the circuit with $\rho_{4n,t}(\sigma_i)$



Solovay-Kitaev's output

$\rho_{12,t}(\sigma_1 \sigma_4 \sigma_7^{-1})$ $\rho_{12,t}(\sigma_5)$ $\rho_{12,t}(\sigma_{11}^{-1} \sigma_{10})$

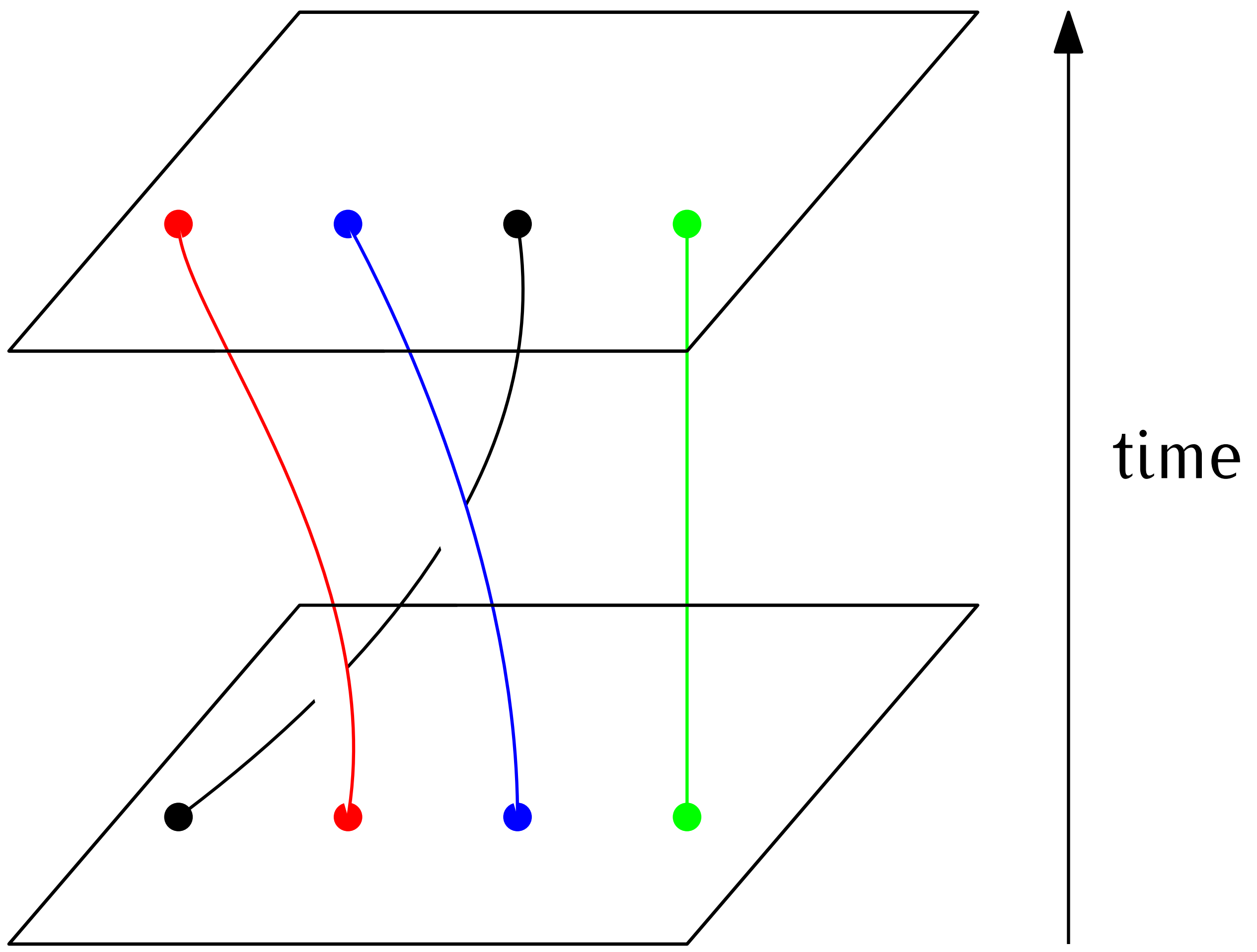
3. Find the braid given by the σ_i



4. $|\langle 0^{\otimes n} | C | 0^{\otimes n} \rangle|^2 \approx C |V_t(L)|^2$

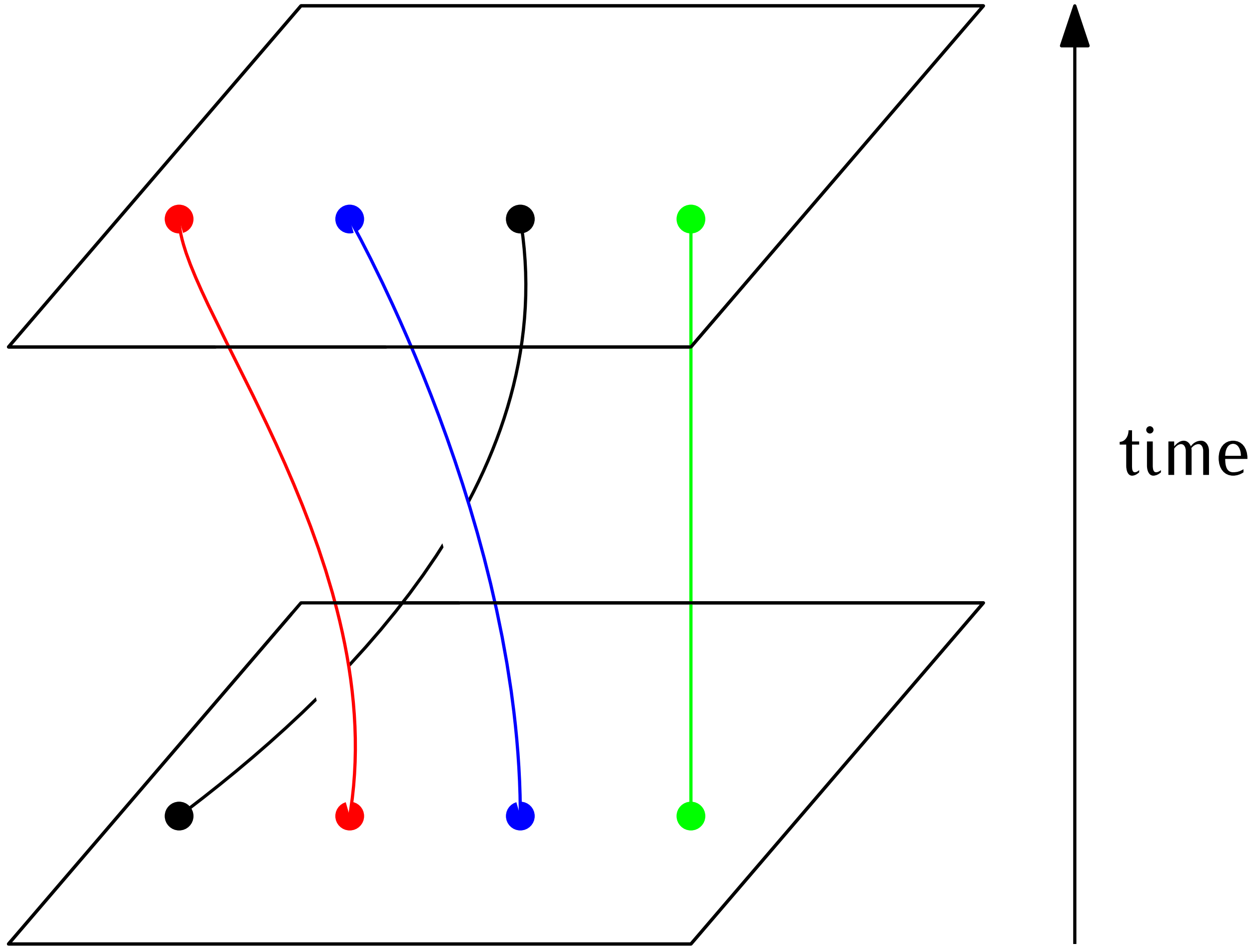
Topological quantum computing

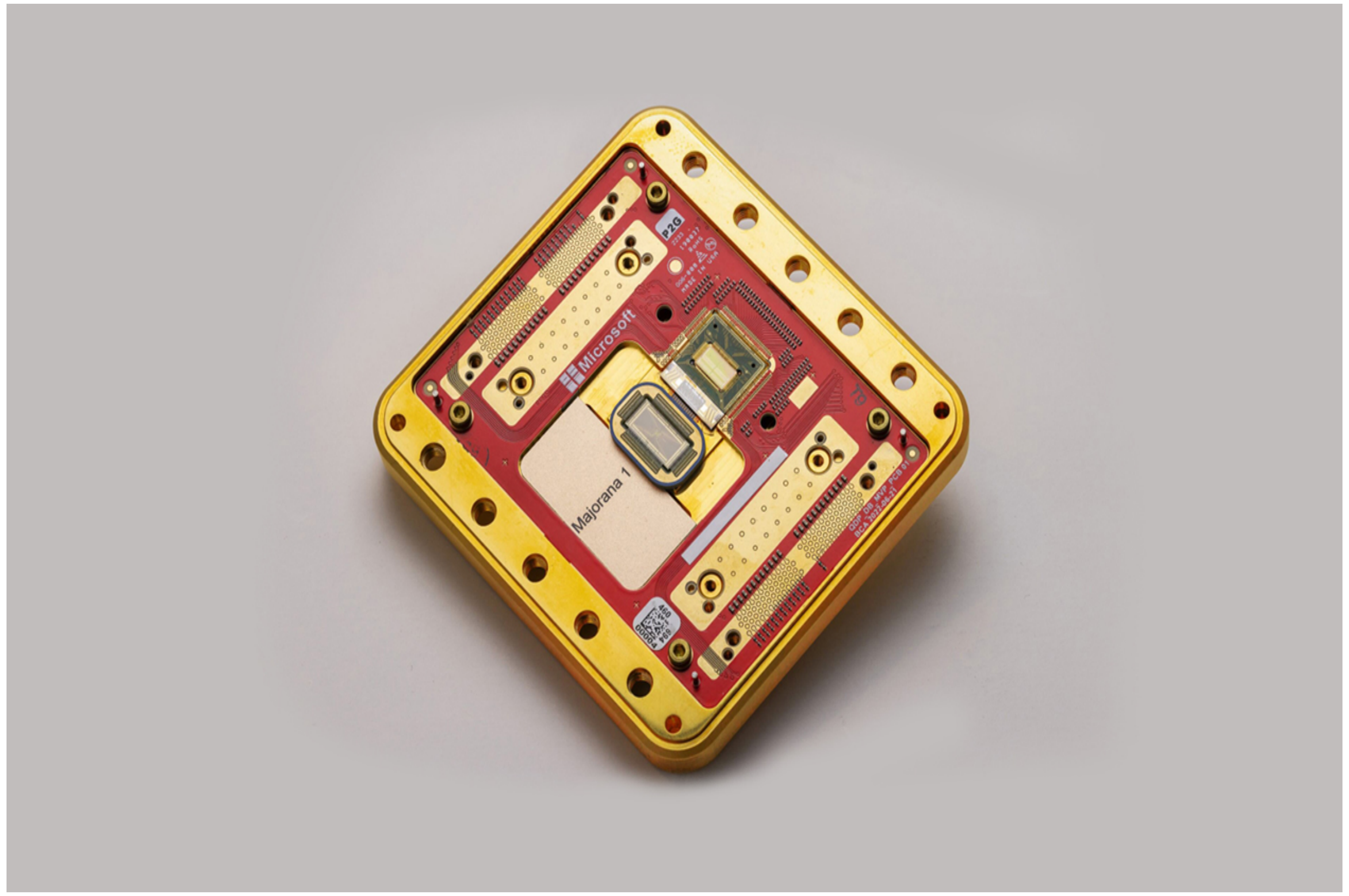
Anyons are (quasi) particles whose behavior are very tied to Jones polynomials.



Topological quantum computing

Anyons are (quasi) particles whose behavior are very tied to Jones polynomials.





The bad news

Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

The bad news

Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

Consider a logic term with free variables

$$T : (x \land \neg y) \lor z$$

The bad news

Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

Consider a logic term with free variables

$$T : (x \wedge \neg y) \vee z$$

- P: given an assignment, telling whether the assignment gives a TRUE statement.

The bad news

Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

Consider a logic term with free variables

$$T : (x \wedge \neg y) \vee z$$

- P: given an assignment, telling whether the assignment gives a TRUE statement.
- NP-hard: for a given term, telling whether there exists **one** assignment that makes the sentence TRUE.

UNIVERSITÉ CÔTE D'AZUR Inria

The bad news

Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

Consider a logic term with free variables

$$T : (x \land \neg y) \lor z$$

- P: given an assignment, telling whether the assignment gives a TRUE statement.
- NP-hard: for a given term, telling whether there exists **one** assignment that makes the sentence TRUE.
- #P-hard: for a given term, **counting** how many assignments make the term TRUE.

UNIVERSITÉ CÔTE D'AZUR Inria

The bad news

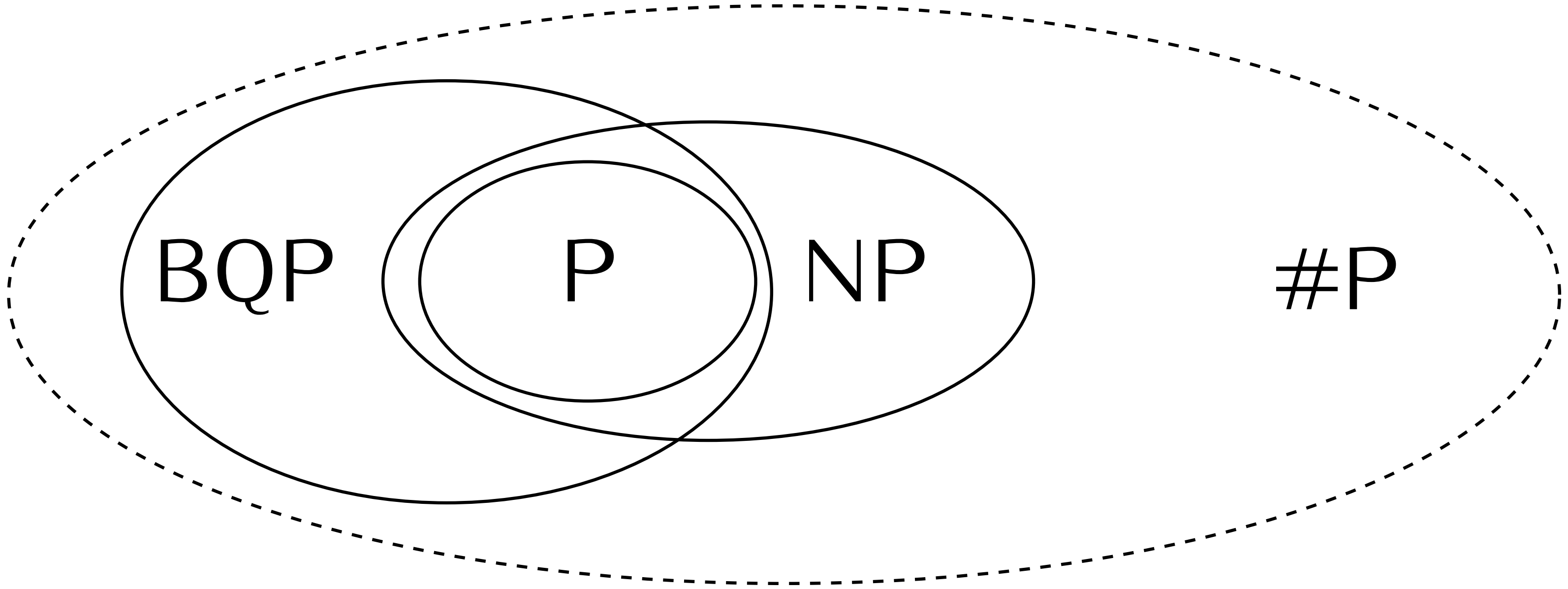
Theorem (Aaronson):

A good approximation of $|\langle 0^{\otimes n}|C|0^{\otimes n}\rangle|^2$ is #P-hard.

Consider a logic term with free variables

$$T : (x \land \neg y) \lor z$$

- P: given an assignment, telling whether the assignment gives a TRUE statement.
- NP-hard: for a given term, telling whether there exists **one** assignment that makes the sentence TRUE.
- #P-hard: for a given term, **counting** how many assignments make the term TRUE.



UNIVERSITÉ CÔTE D'AZUR Inria

Merci!