Title: Estimating Jones polynomials is a complete problem for one clean qubit.

Date: Oct 31, 2007 04:00 PM

URL: http://pirsa.org/07100034

Abstract: The one clean qubit model is a model of quantum computation in which all but one qubit starts in the maximally mixed state. One clean qubit computers are believed to be strictly weaker than standard quantum computers, but still capable of solving some classically intractable problems. I\'ll discuss my recent work in collaboration with Peter Shor which shows that evaluating a certain approximation to the Jones polynomial at a fifth root of unity for the trace closure of a braid is a complete problem for the one clean qubit complexity class.

Estimating Jones Polynomials is a Complete Problem for One Clean Qubit

Stephen P. Jordan
in collaboration with Peter Shor

[ArXiv:0707.2831] (2007)

DTO

Outline

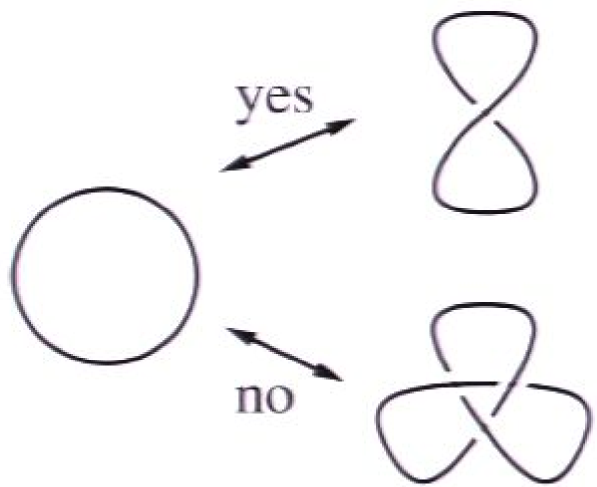
- Jones polynomials and knot theory
- One Clean Qubit model
- Sketch of Completeness Proof

Knots And Links

- A knot is an embedding of the circle into $\mathbb{R}^3$
- A link is an embedding of one or more circles into $\mathbb{R}^3$

Distinguishing Knots

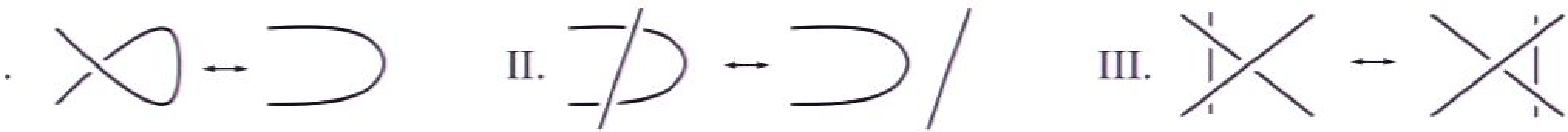
- Are two knots equivalent?



- This seems to be hard. Equivalence to the unknot was shown to be computable in 1968 and contained in NP in 1998.

Reidemeister Moves

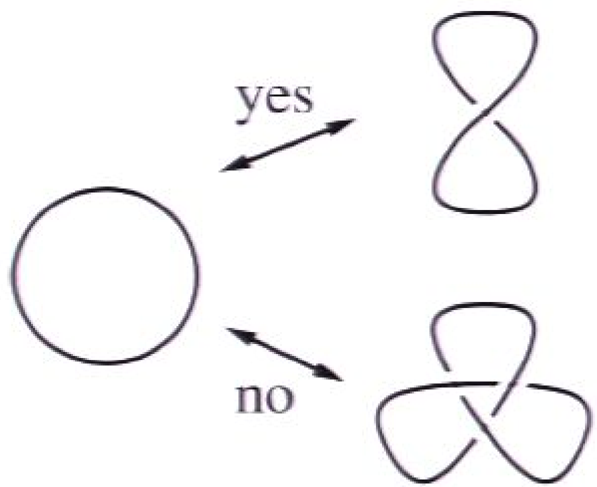
- Two knots are equivalent if and only if one can be reached from the other by a sequence of Reidemeister moves



- This gives us a more combinatorial way to think about knot theory.

Distinguishing Knots

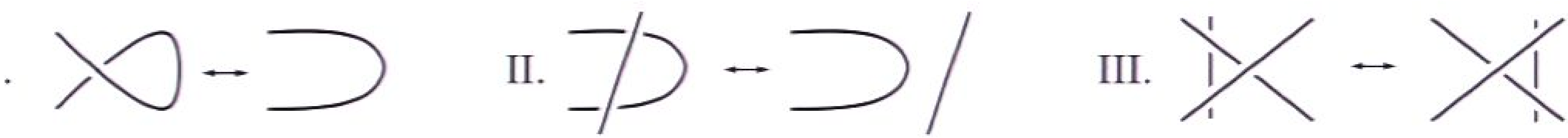
- Are two knots equivalent?



- This seems to be hard. Equivalence to the unknot was shown to be computable in 1968 and contained in NP in 1998.

Reidemeister Moves

- Two knots are equivalent if and only if one can be reached from the other by a sequence of Reidemeister moves



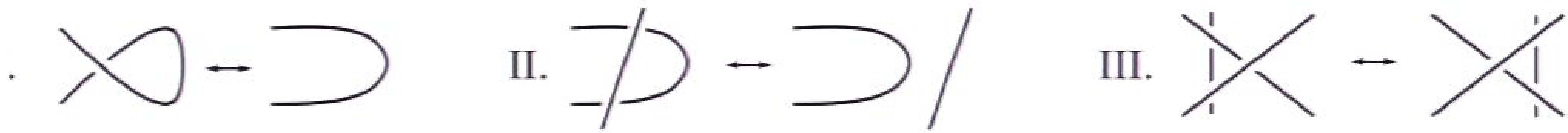
- This gives us a more combinatorial way to think about knot theory.

Knot Invariants

- function on knots
- gives the same value for equivalent knots
- may not distinguish all knots
- Jones polynomial
  - distinguishes many knots
  - is #P-hard to compute exactly

Reidemeister Moves

- Two knots are equivalent if and only if one can be reached from the other by a sequence of Reidemeister moves



- This gives us a more combinatorial way to think about knot theory.

Knot Invariants

- function on knots
- gives the same value for equivalent knots
- may not distinguish all knots
- Jones polynomial
  - distinguishes many knots
  - is #P-hard to compute exactly

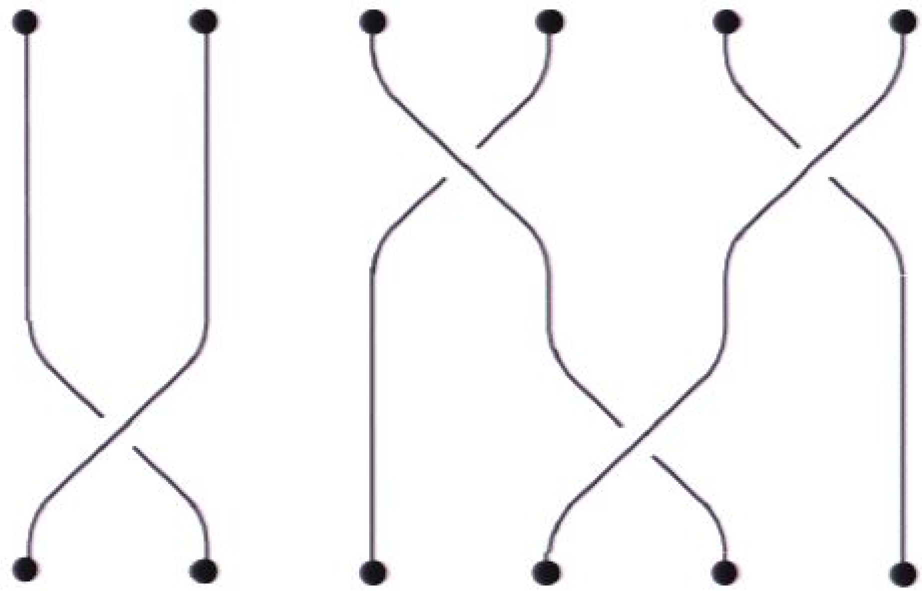
Jones Polynomial Examples

V  $= 1$

V  $= t + t^3 - t^4$

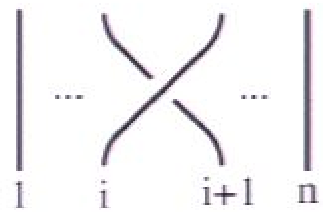
Describing Knots

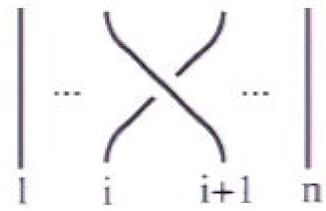
- knots are continuous objects
- they can be described in the discrete language of the braid group



Braid Groups

- The braids on *n* strands form a group B_n generated by:

$\sigma_i =$ 

$\sigma_i^{-1} =$ 

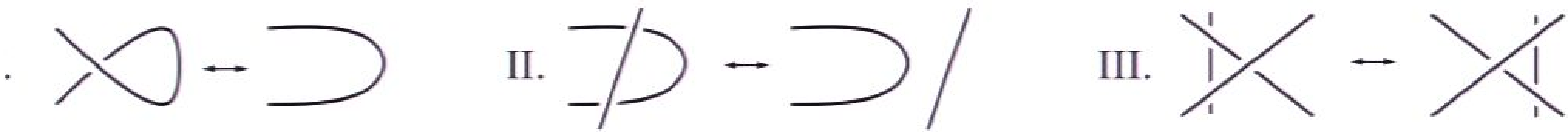
- with the relations:

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

$$\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i \quad \text{for all } i$$

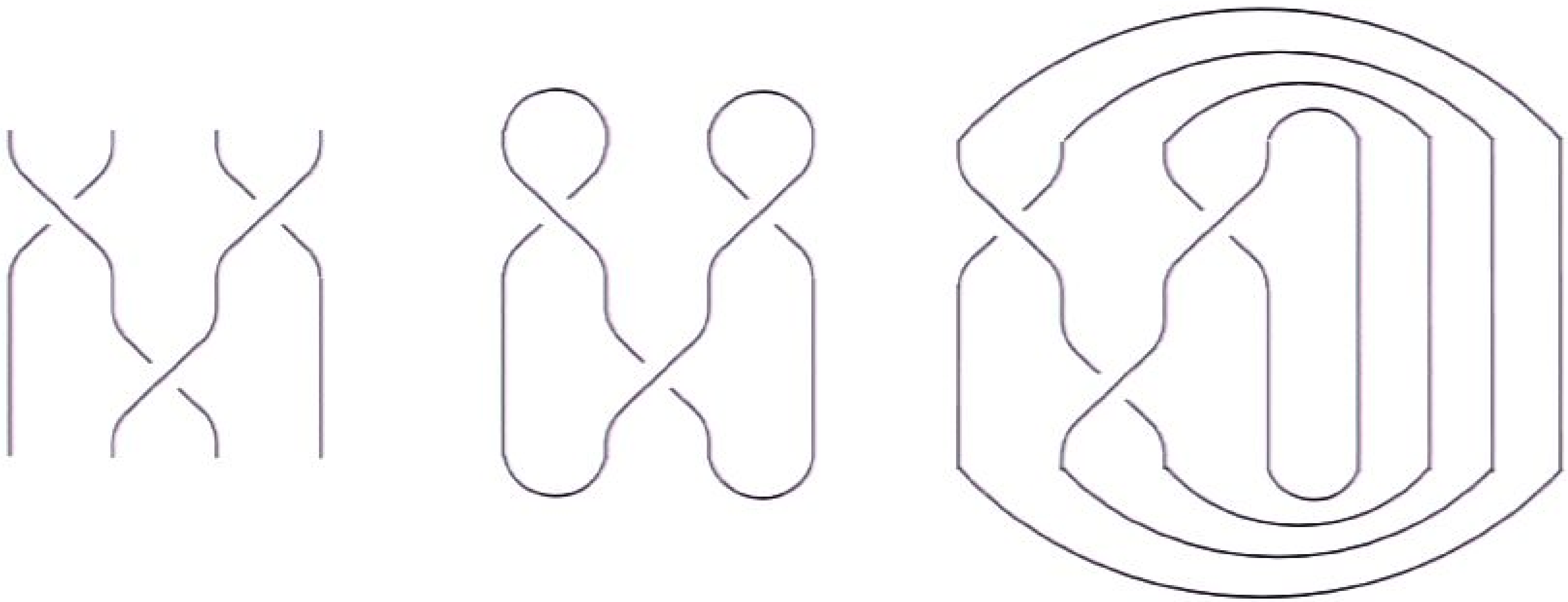
Reidemeister Moves

- Two knots are equivalent if and only if one can be reached from the other by a sequence of Reidemeister moves



- This gives us a more combinatorial way to think about knot theory.

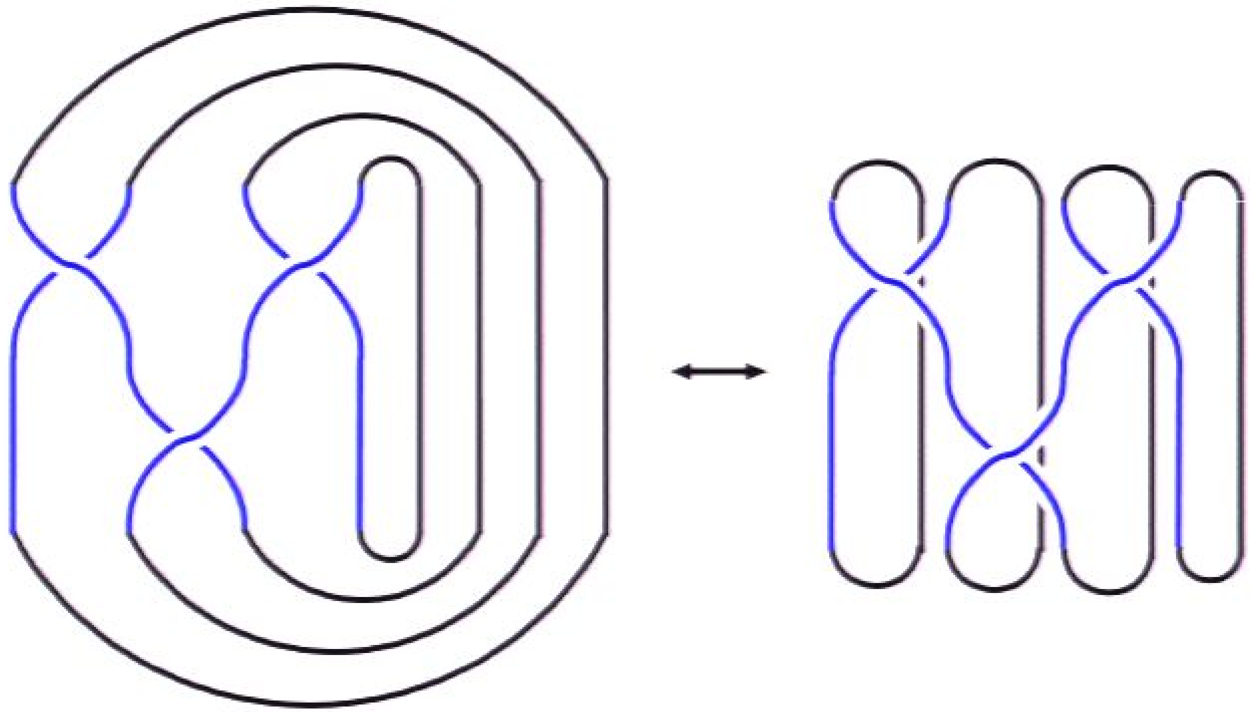
Braid Closures



plat

trace

Alexander's Theorem

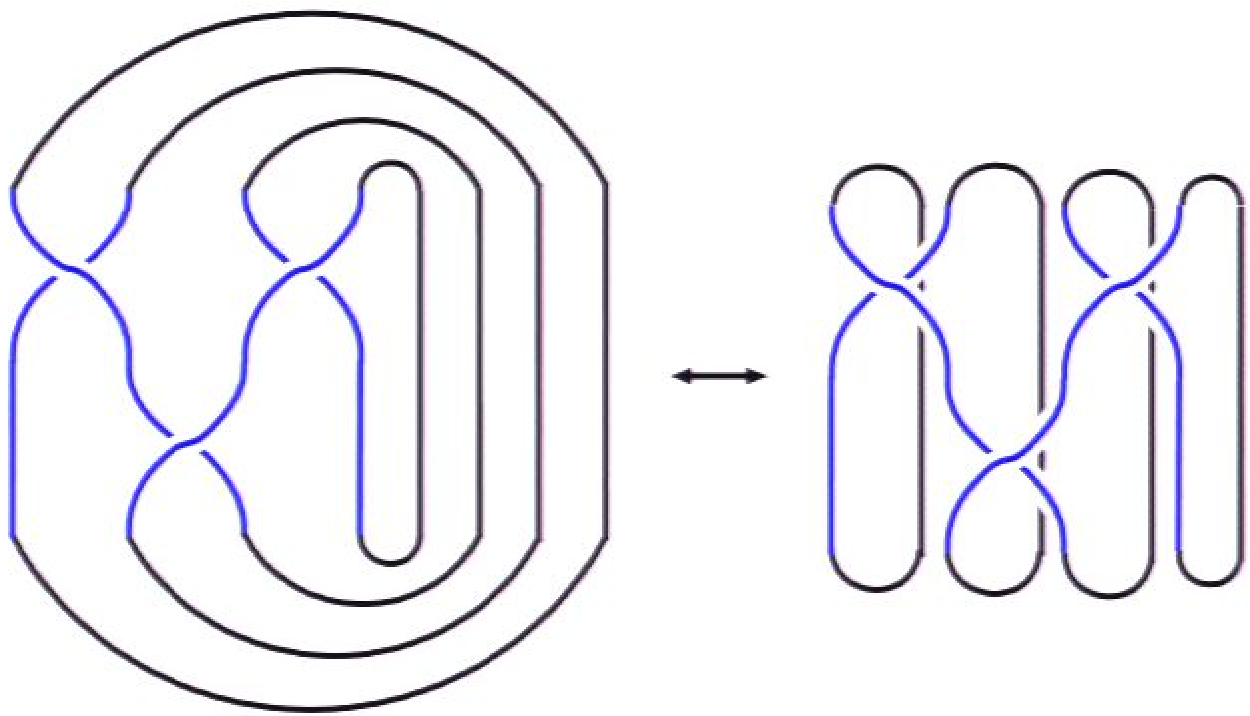


Quantum Complexity

- a certain additive approximation to the Jones polynomial of the plat closure of a braid is BQP-complete ($t = e^{i2\pi/k}$)*
- trace closure: approximable in BQP
- Open question:
  - what is the complexity of approximating the Jones polynomial of the trace closure of a braid?
- Answer (Shor, Jordan): DQC1-complete

*Aharonov, Jones, Landau, Arad, Freedman, Kitaev, Larsen, Wang, Witten, Wocjan, Yard

Alexander's Theorem

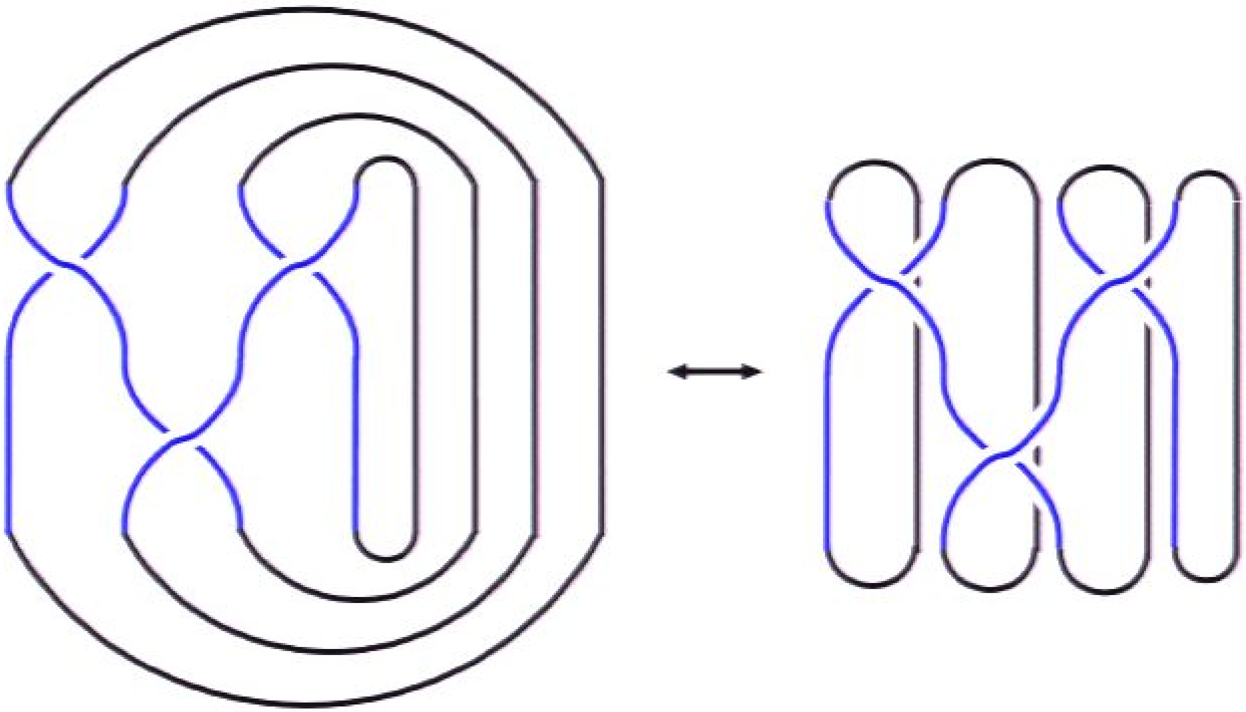


Quantum Complexity

- a certain additive approximation to the Jones polynomial of the plat closure of a braid is BQP-complete ($t = e^{i2\pi/k}$)*
- trace closure: approximable in BQP
- Open question:
  - what is the complexity of approximating the Jones polynomial of the trace closure of a braid?
- Answer (Shor, Jordan): DQC1-complete

*Aharonov, Jones, Landau, Arad, Freedman, Kitaev, Larsen, Wang, Witten, Wocjan, Yard

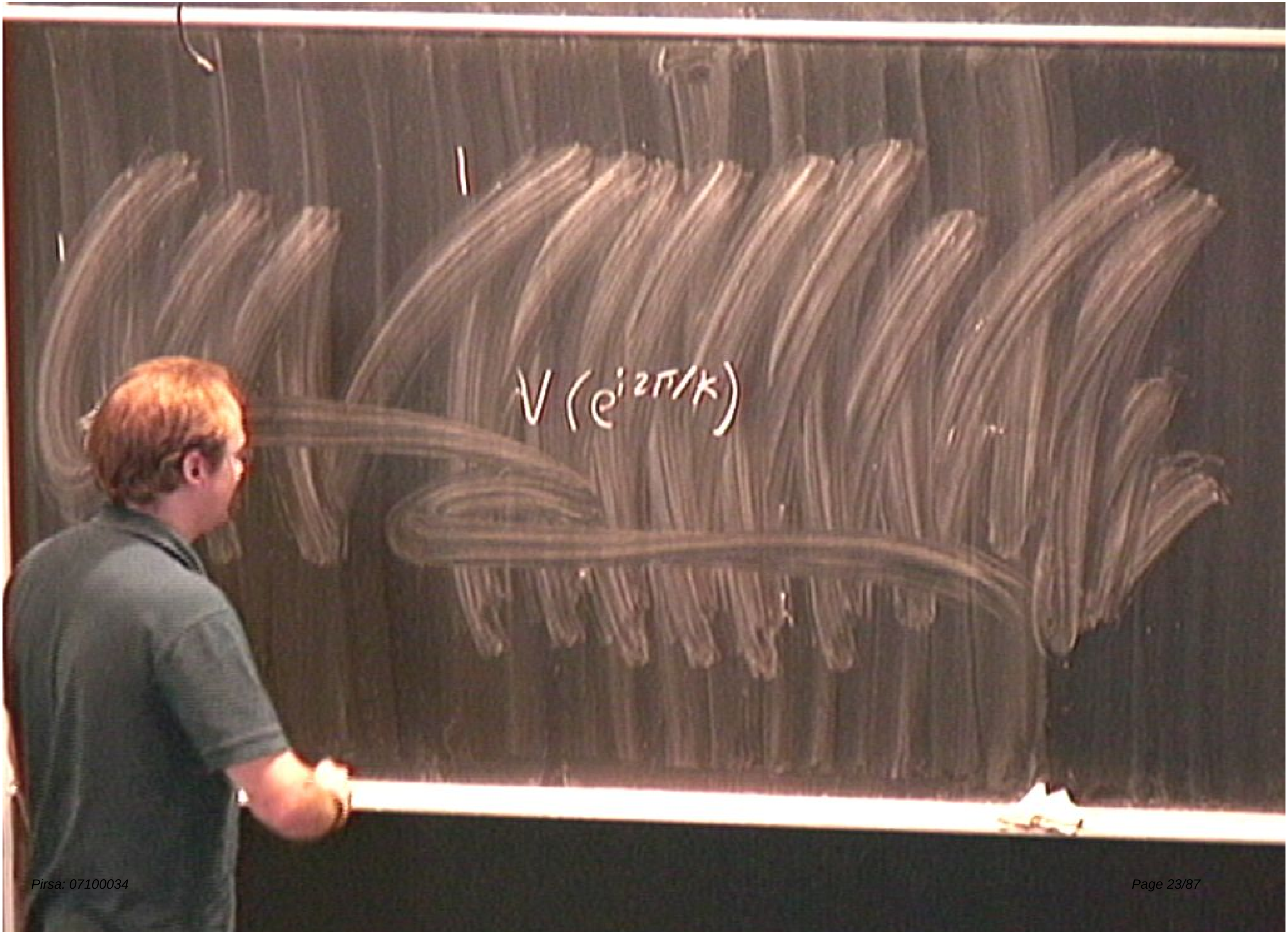
Alexander's Theorem

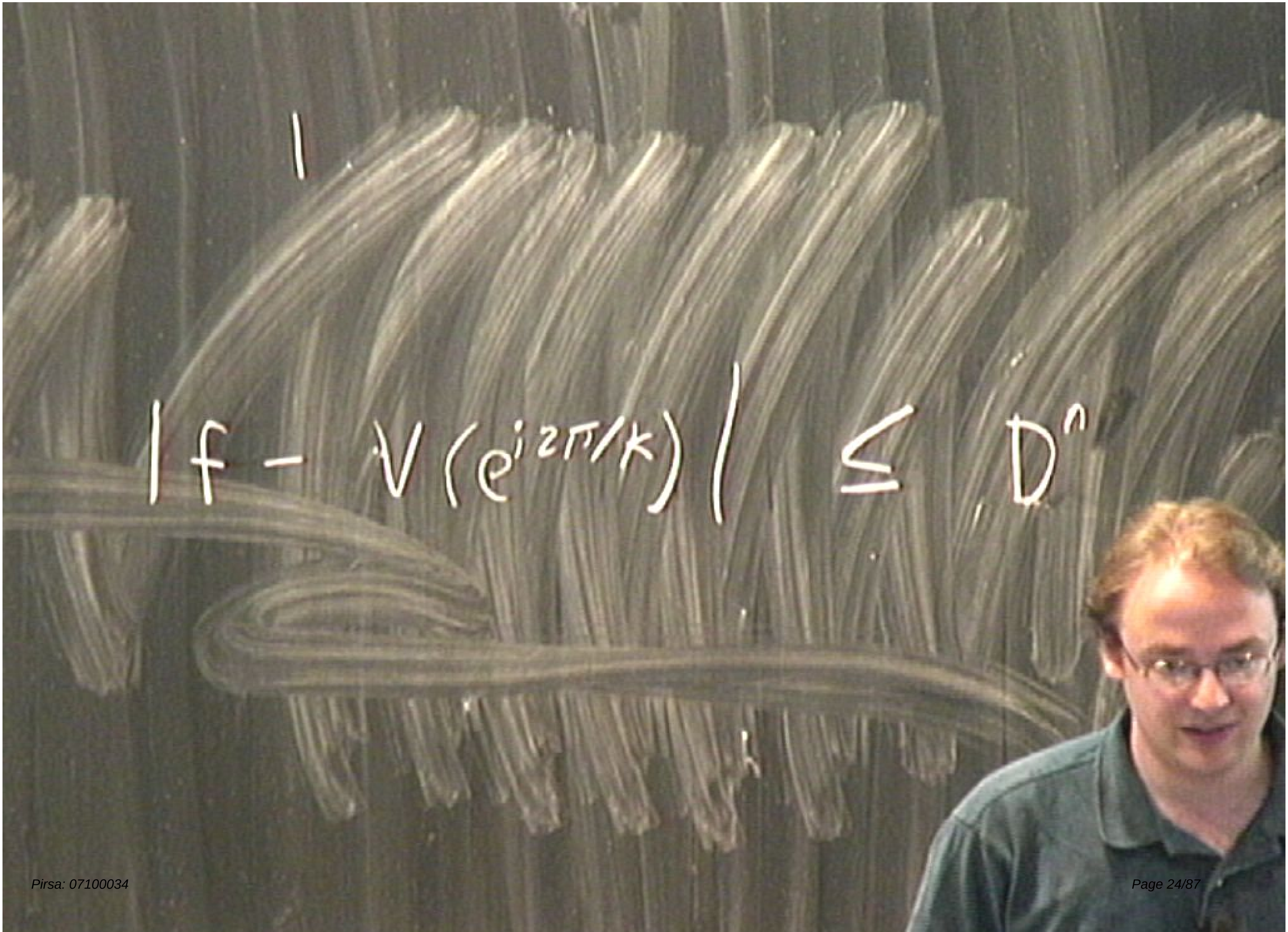


Quantum Complexity

- a certain additive approximation to the Jones polynomial of the plat closure of a braid is BQP-complete ($t = e^{i2\pi/k}$)*
- trace closure: approximable in BQP
- Open question:
  - what is the complexity of approximating the Jones polynomial of the trace closure of a braid?
- Answer (Shor, Jordan): DQC1-complete

*Aharonov, Jones, Landau, Arad, Freedman, Kitaev, Larsen, Wang, Witten, Wocjan, Yard


$V(e^{i2\pi/k})$


$|f - V(e^{i2\pi/k})| \leq D^n$

Quantum Complexity

- a certain additive approximation to the Jones polynomial of the plat closure of a braid is BQP-complete ($t = e^{i2\pi/k}$)*
- trace closure: approximable in BQP
- Open question:
  - what is the complexity of approximating the Jones polynomial of the trace closure of a braid?
- Answer (Shor, Jordan): DQC1-complete

*Aharonov, Jones, Landau, Arad, Freedman, Kitaev, Larsen, Wang, Witten, Wocjan, Yard

One Clean Qubit

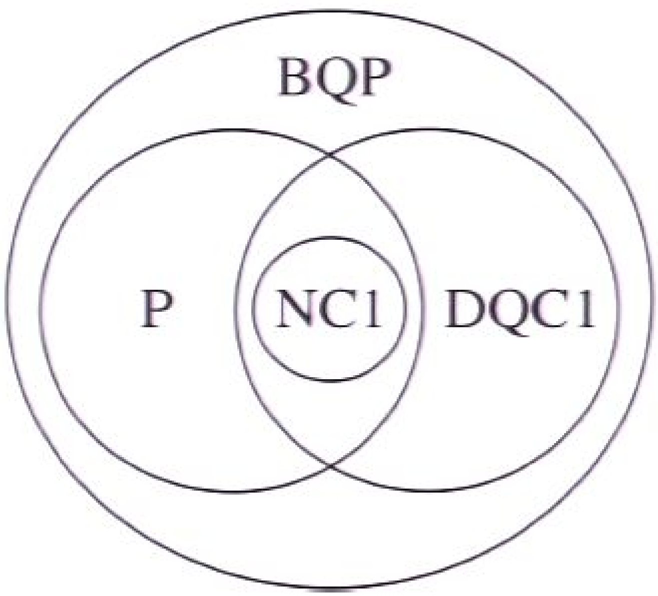
- One qubit starts in pure state, all the rest start in maximally mixed state
- Idealized model of high entropy quantum computer such as NMR
- general mixed states can be converted to clean and maximally mixed qubits by algorithmic cooling

One Clean Qubit

- One qubit starts in pure state, all the rest start in maximally mixed state
- Idealized model of high entropy quantum computer such as NMR
- general mixed states can be converted to clean and maximally mixed qubits by algorithmic cooling

DQC1

- the class of problems solvable by polynomial size quantum circuits using one clean qubit

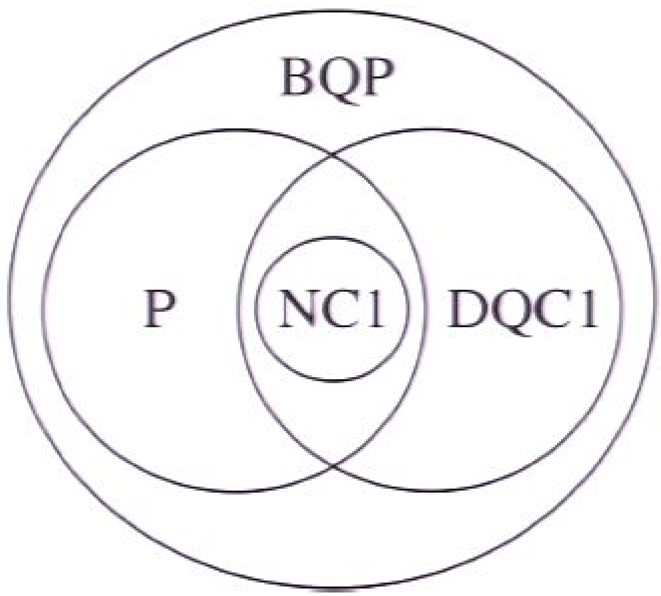


Main Result

- Approximating the Jones polynomial of the trace closure of a braid is DQC1-complete ($t = -e^{i3\pi/5}$)
  - can be efficiently computed on a one clean qubit computer
  - the problem of simulating a one clean qubit computer is reducible to this Jones polynomial problem
- This is one of only three DQC1 algorithms thought to provide exponential speedup

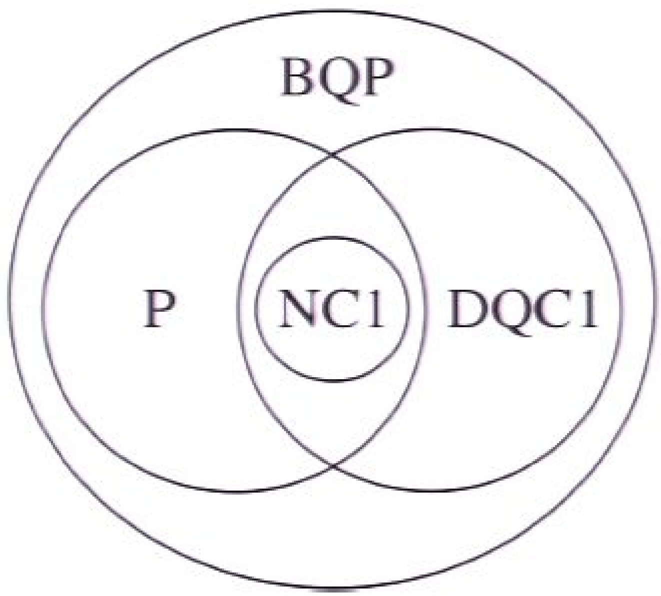
DQC1

- the class of problems solvable by polynomial size quantum circuits using one clean qubit



DQC1

- the class of problems solvable by polynomial size quantum circuits using one clean qubit



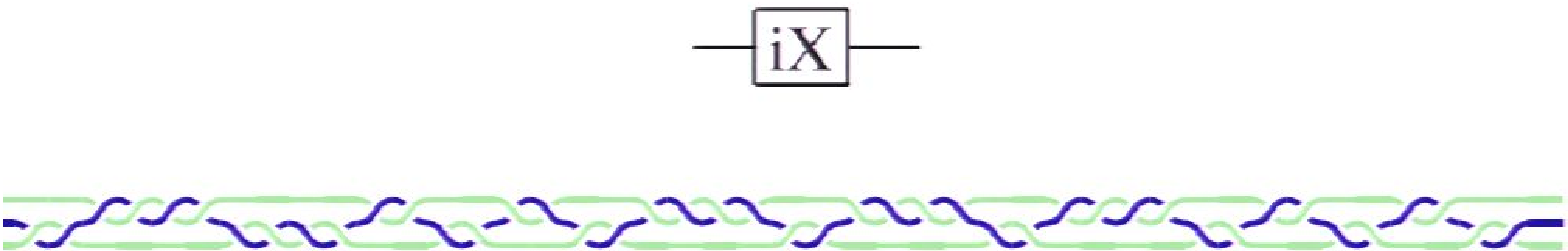
Main Result

- Approximating the Jones polynomial of the trace closure of a braid is DQC1-complete ($t = -e^{i3\pi/5}$)
  - can be efficiently computed on a one clean qubit computer
  - the problem of simulating a one clean qubit computer is reducible to this Jones polynomial problem
- This is one of only three DQC1 algorithms thought to provide exponential speedup

Jones Representation

- The trace of the Jones representation of a braid gives the Jones polynomial of its trace closure
- A certain matrix element of the Jones representation of a braid gives the Jones polynomial its plat closure

- Jones representation is unitary for $t = e^{i2\pi/k}$
- It induces an approximate correspondence between quantum circuits and braids

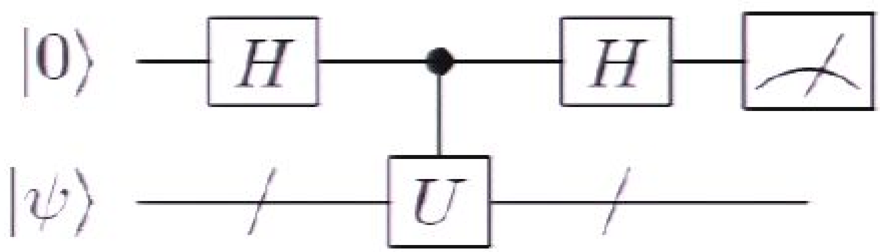


- matrix element: BQP-complete
- trace: DQC1-complete

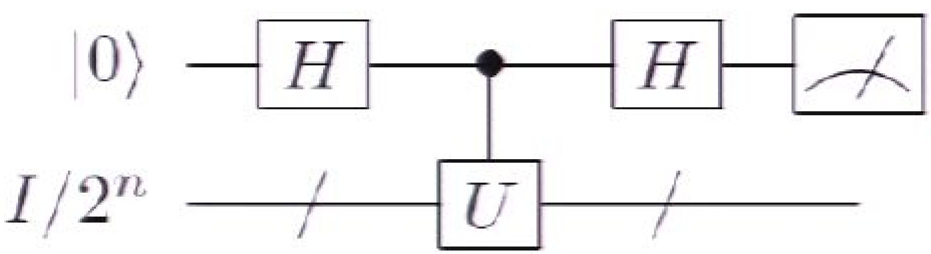
[picture from Hormozi *et al.* quant-ph/0610111]

Trace Estimation

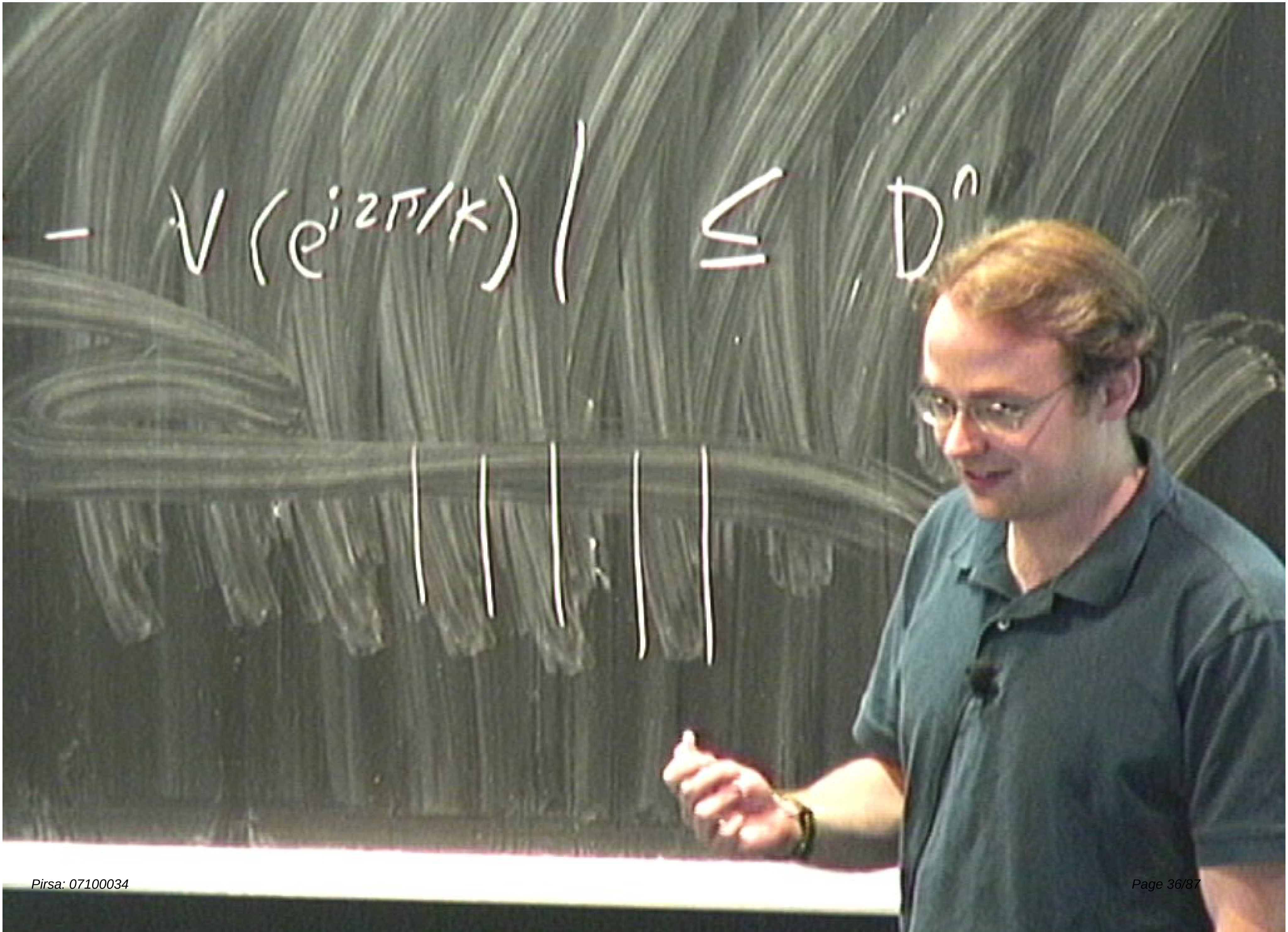
- One clean qubit computers can efficiently estimate the normalized trace of a quantum circuit to polynomial accuracy

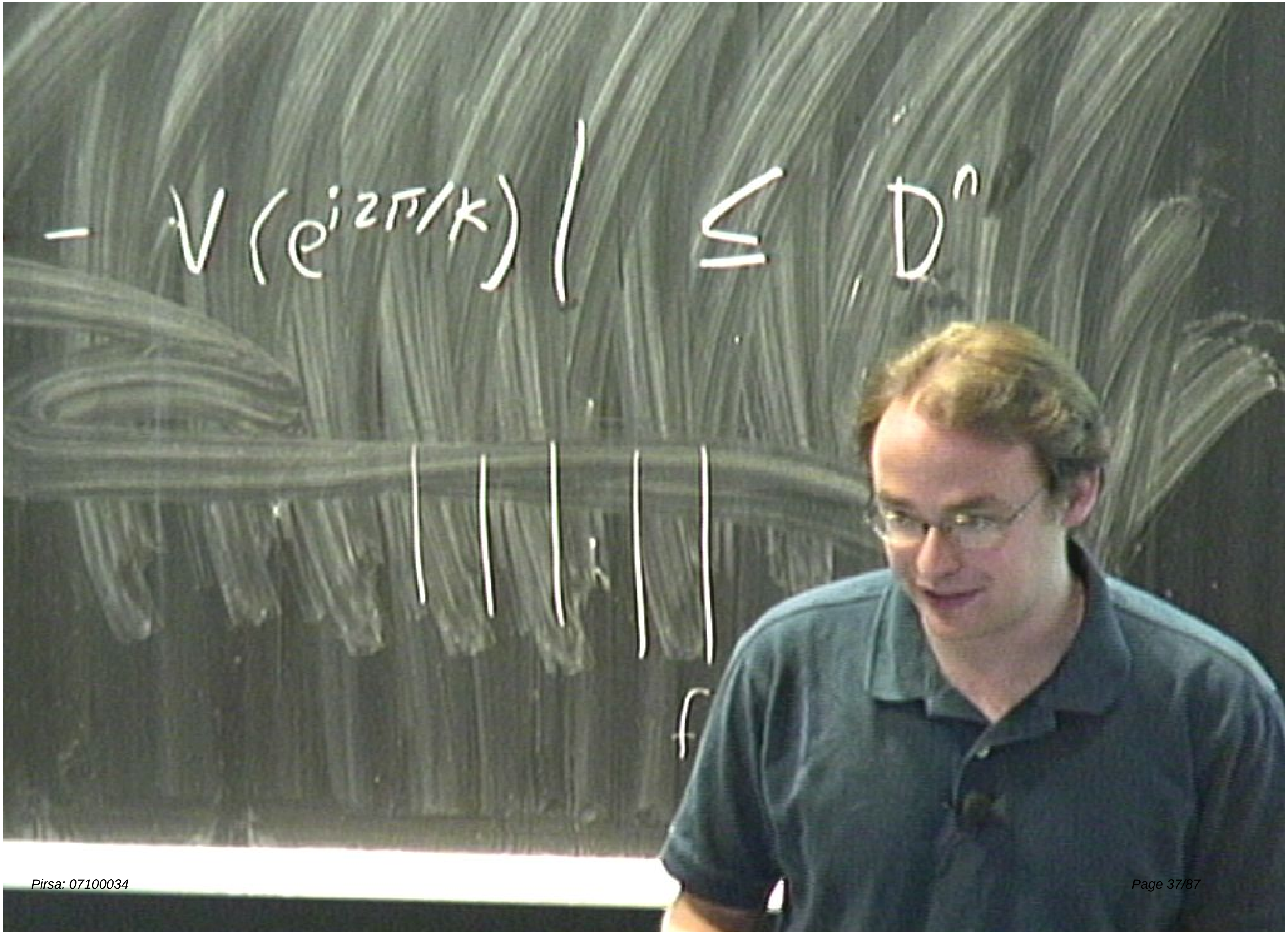


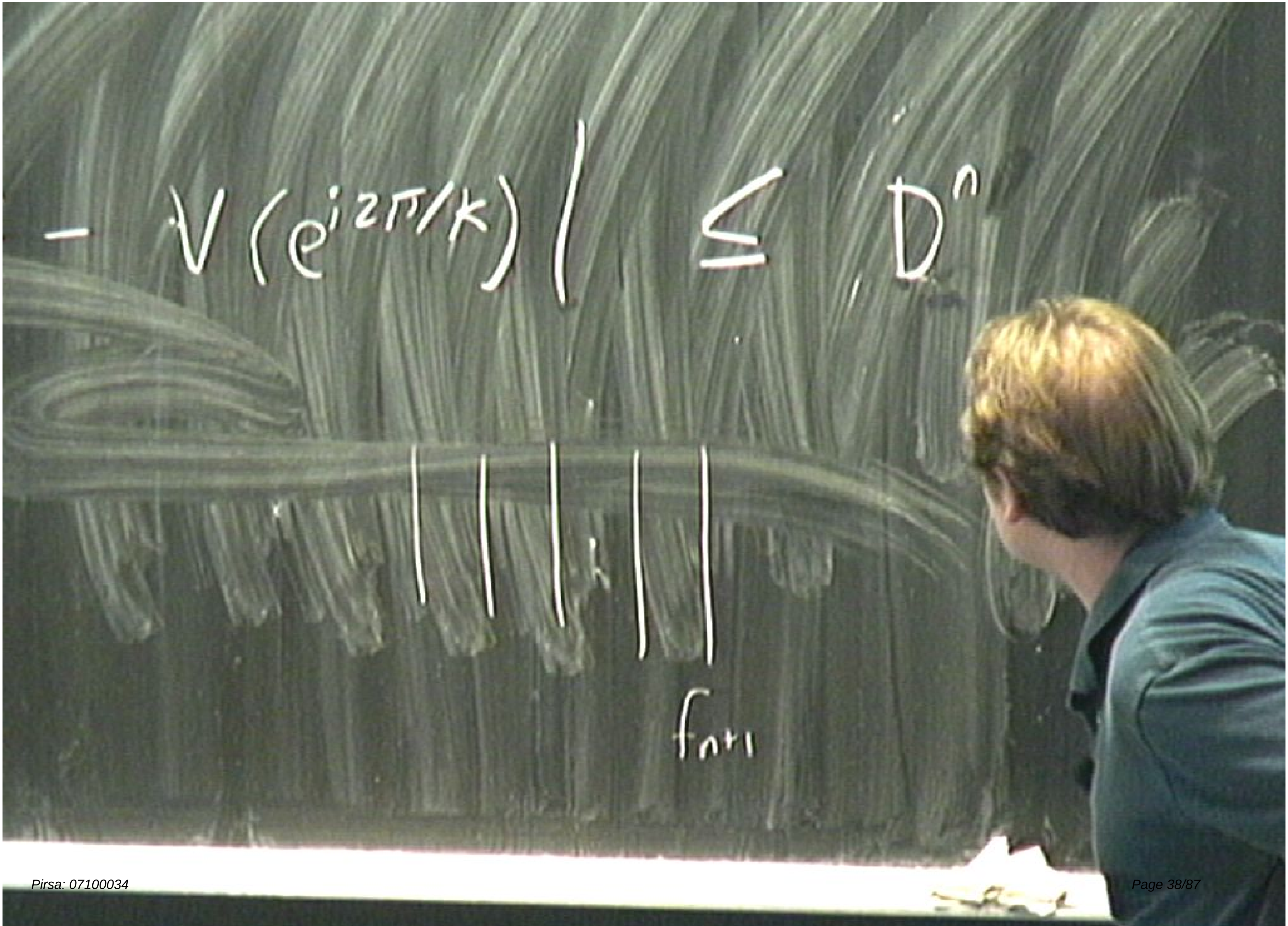
$$p_0 = \frac{1+\mathrm{Re}(\langle\psi|U|\psi\rangle)}{2}$$



$$p_0 = \frac{1+\mathrm{Re}(\mathrm{Tr}U)}{2^{n+1}}$$

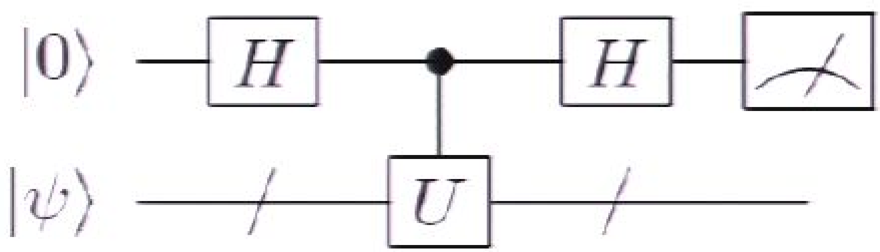

$- V(e^{i2\pi/k}) | \leq D^n$


$- V(e^{i2\pi/k}) | \leq D^n$

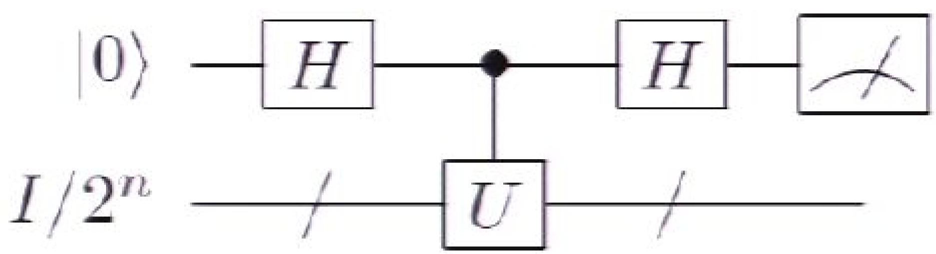

$- V(e^{i2\pi/k}) | \leq D^n$
f_{n+1}

Trace Estimation

- One clean qubit computers can efficiently estimate the normalized trace of a quantum circuit to polynomial accuracy



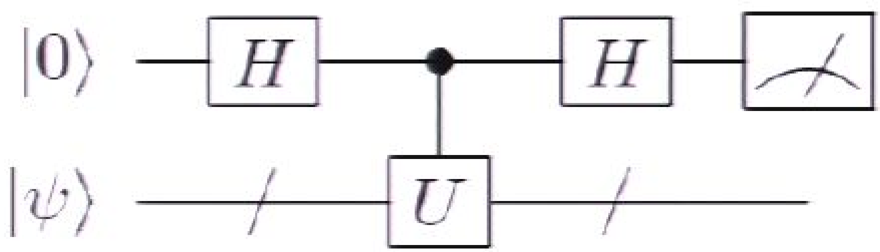
$$p_0 = \frac{1 + \mathrm{Re}(\langle\psi|U|\psi\rangle)}{2}$$



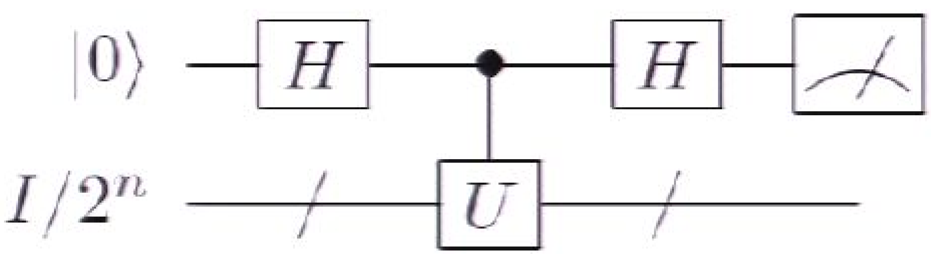
$$p_0 = \frac{1 + \mathrm{Re}(\mathrm{Tr}U)}{2^{n+1}}$$

Trace Estimation

- One clean qubit computers can efficiently estimate the normalized trace of a quantum circuit to polynomial accuracy



$$p_0 = \frac{1+\mathrm{Re}(\langle\psi|U|\psi\rangle)}{2}$$



$$p_0 = \frac{1+\mathrm{Re}(\mathrm{Tr}U)}{2^{n+1}}$$

Trace Estimation

- The problem of simulating a one clean qubit computer is reducible to trace estimation

$$p_0 = \mathrm{Tr}\left[(|0\rangle\langle 0| \otimes I)\rho \right]$$
$$\rho = \frac{1}{2^n} U(|0\rangle\langle 0| \otimes I)U^\dagger$$

- p_0 is proportional to the trace of the following nonunitary operator

$$(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^\dagger$$

Trace Estimation

- The problem of simulating a one clean qubit computer is reducible to trace estimation

$$p_0 = \mathrm{Tr}\left[(|0\rangle\langle 0| \otimes I)\rho\right]$$

$$\rho = \frac{1}{2^n} U(|0\rangle\langle 0| \otimes I)U^\dagger$$

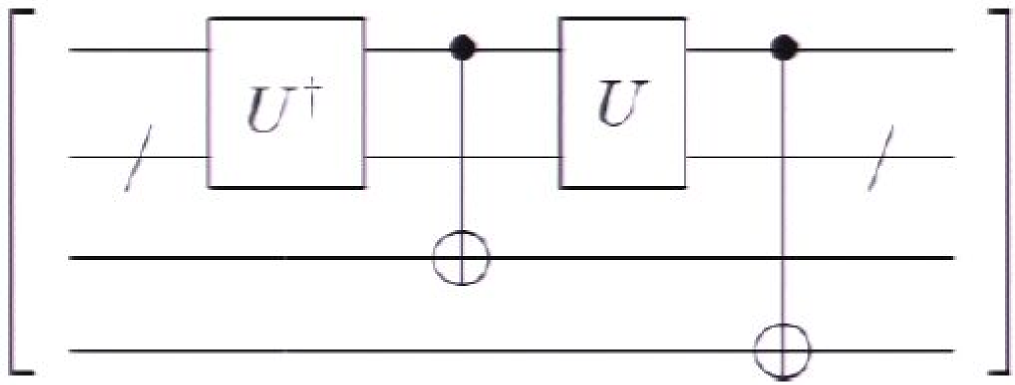
- p_0 is proportional to the trace of the following nonunitary operator

$$(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^\dagger$$

Trace Estimation

$$\mathrm{Tr}[(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^{\dagger}]$$

$$= \frac{1}{4}\mathrm{Tr}$$



- Trace estimation is DQC1 complete
- *log(n)* clean qubits give no more power than one clean qubit

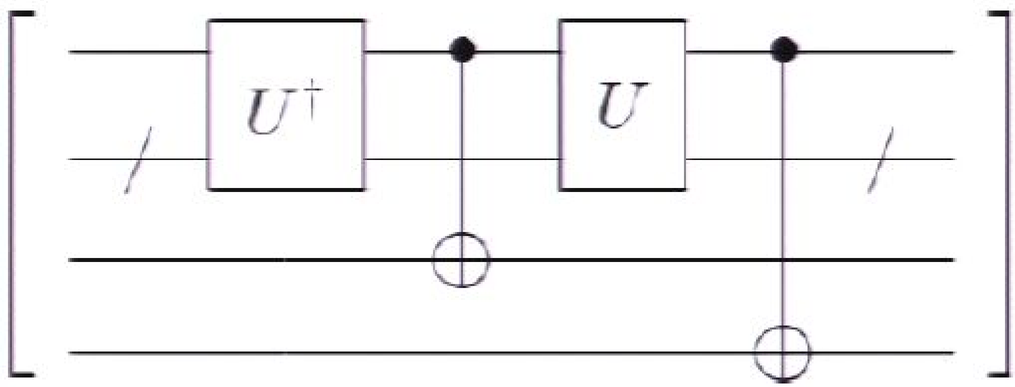
Part I: The algorithm

- The braid group representation acts on some vector space V.
- Make a correspondence between V and the qubits' Hilbert space, which allows the representation to be implemented efficiently by quantum circuits.
- Use trace estimation.

Trace Estimation

$$\mathrm{Tr}[(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^\dagger]$$

$$= \frac{1}{4}\mathrm{Tr}$$



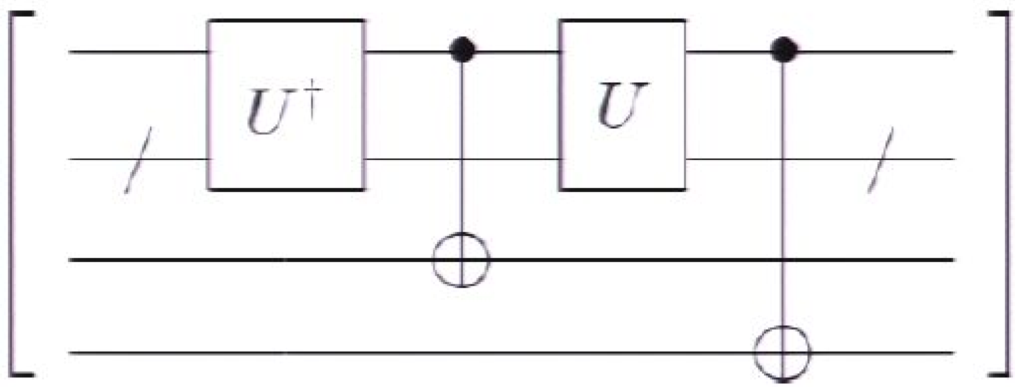
.

- Trace estimation is DQC1 complete
- *log(n)* clean qubits give no more power than one clean qubit

Trace Estimation

$$\mathrm{Tr}[(|0\rangle\langle 0| \otimes I)U(|0\rangle\langle 0| \otimes I)U^\dagger]$$

$$= \frac{1}{4}\mathrm{Tr}$$



- Trace estimation is DQC1 complete
- *log(n)* clean qubits give no more power than one clean qubit

Part I: The algorithm

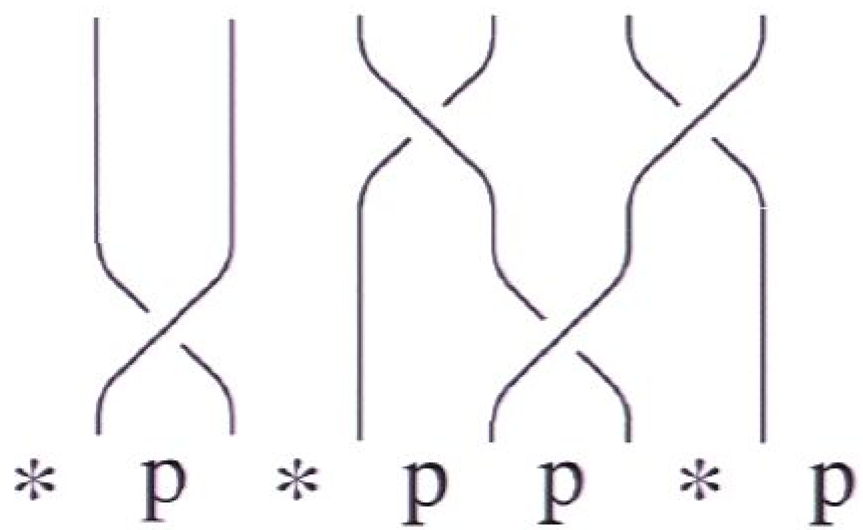
- The braid group representation acts on some vector space V.
- Make a correspondence between V and the qubits' Hilbert space, which allows the representation to be implemented efficiently by quantum circuits.
- Use trace estimation.

Part I: The algorithm

- The braid group representation acts on some vector space V.
- Make a correspondence between V and the qubits' Hilbert space, which allows the representation to be implemented efficiently by quantum circuits.
- Use trace estimation.

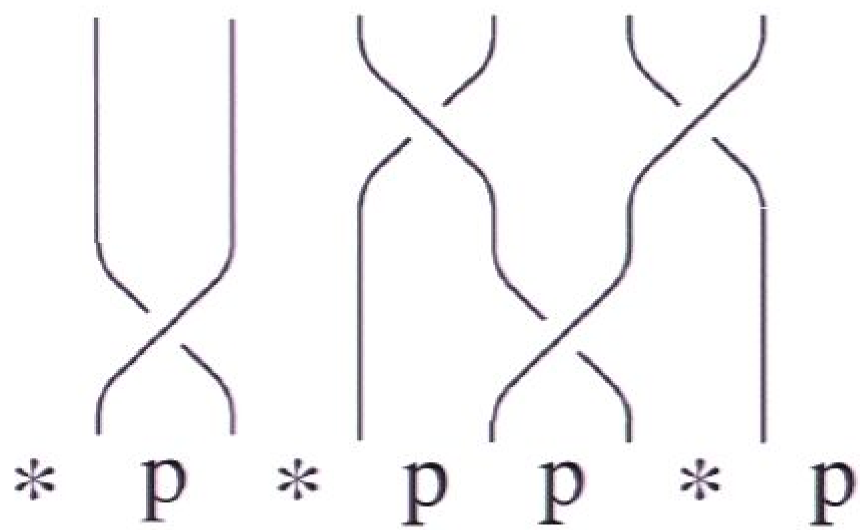
Fibonacci Representation

- the trace of this representation gives the Jones polynomial at $t = -e^{i3\pi/5}$
- for the plat closure, $t = -e^{i3\pi/5}$ is BQP-hard
- basis of V is $p*$ -strings

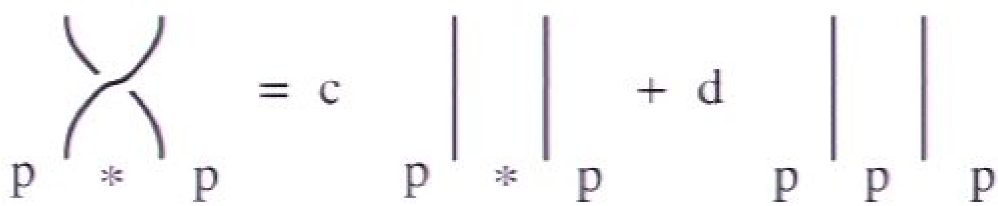


Fibonacci Representation

- the trace of this representation gives the Jones polynomial at $t = -e^{i3\pi/5}$
- for the plat closure, $t = -e^{i3\pi/5}$ is BQP-hard
- basis of V is $p*$ -strings



Fibonacci Representation



$$c = A^8\tau^2 - A^4\tau$$

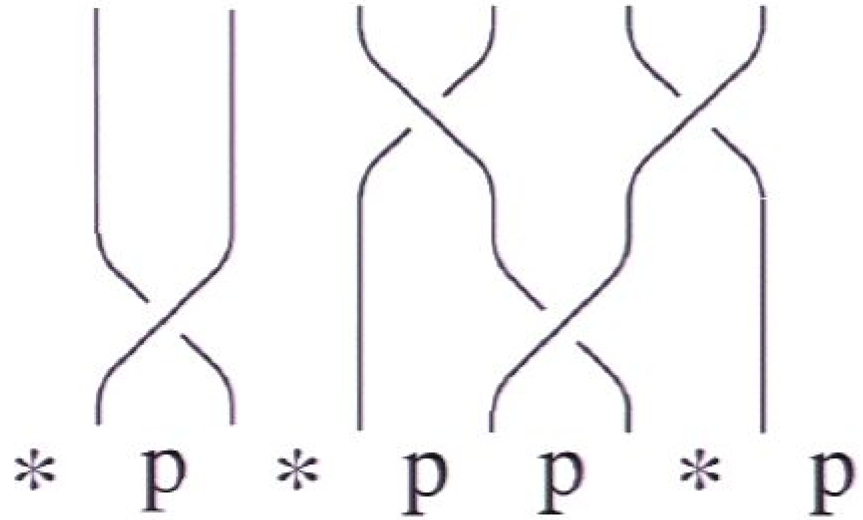
$$d = A^8\tau^{3/2} + A^4\tau^{3/2}$$

$$A = t^{-1/4} = e^{i3\pi/5}$$

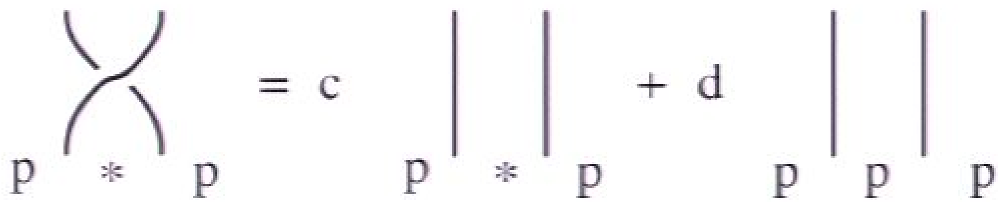
$$\tau = 2/(1+\sqrt{5})$$

Fibonacci Representation

- the trace of this representation gives the Jones polynomial at $t = -e^{i3\pi/5}$
- for the plat closure, $t = -e^{i3\pi/5}$ is BQP-hard
- basis of V is $p*$ -strings



Fibonacci Representation



$$c = A^8\tau^2 - A^4\tau$$

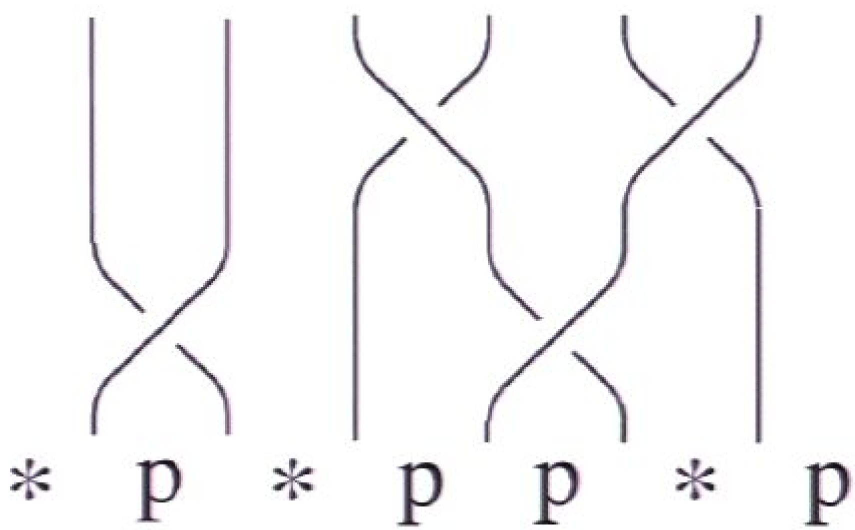
$$d = A^8\tau^{3/2} + A^4\tau^{3/2}$$

$$A = t^{-1/4} = e^{i3\pi/5}$$

$$\tau = 2/(1+\sqrt{5})$$

Fibonacci Representation

- the trace of this representation gives the Jones polynomial at $t = -e^{i3\pi/5}$
- for the plat closure, $t = -e^{i3\pi/5}$ is BQP-hard
- basis of V is $p*$ -strings



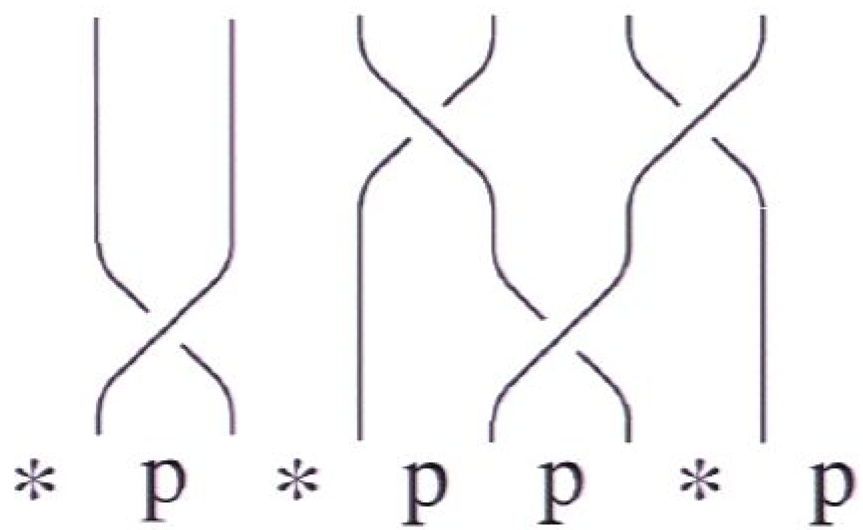
$$\leq \quad \left| f - V\left(e^{i2\pi/k}\right) \right| \quad \leq$$

$$\sigma_i \sigma_j = \sigma_j \sigma_i$$

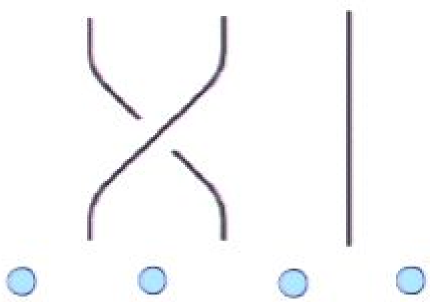
f_{n+1}

Fibonacci Representation

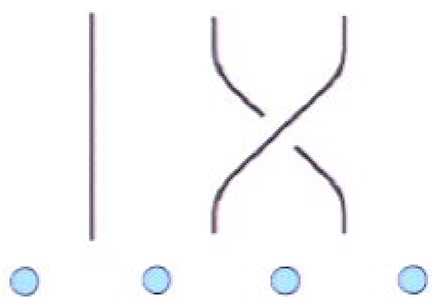
- the trace of this representation gives the Jones polynomial at $t = -e^{i3\pi/5}$
- for the plat closure, $t = -e^{i3\pi/5}$ is BQP-hard
- basis of V is $p*$ -strings



Fibonacci Representation

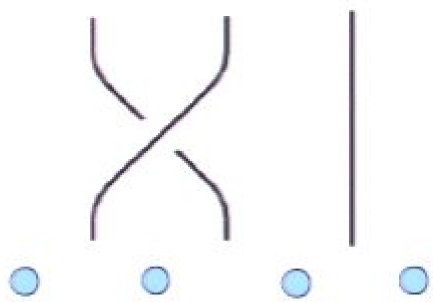


$$\rho_F^{(3)}(\sigma_1) = \begin{bmatrix} b & 0 & & & & & & \\ 0 & a & & & & & & \\ & & a & & & & & \\ & & & e & 0 & d & & \\ & & & 0 & a & 0 & & \\ & & & d & 0 & c & & \\ & & & & & & e & d \\ & & & & & & d & c \end{bmatrix} \begin{matrix} *p*p \\ *ppp \\ *pp* \\ pppp \\ pp*p \\ p*pp \\ ppp* \\ p*p* \end{matrix}$$

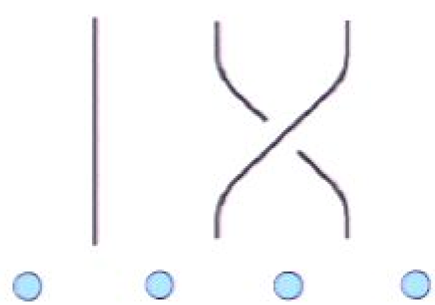


$$\rho_F^{(3)}(\sigma_2) = \begin{bmatrix} c & d & & & & & & \\ d & e & & & & & & \\ & & a & & & & & \\ & & & e & d & 0 & & \\ & & & d & c & 0 & & \\ & & & 0 & 0 & a & & \\ & & & & & & a & 0 \\ & & & & & & 0 & b \end{bmatrix} \begin{matrix} *p*p \\ *ppp \\ *pp* \\ pppp \\ pp*p \\ p*pp \\ ppp* \\ p*p* \end{matrix}$$

Fibonacci Representation



$$\rho_F^{(3)}(\sigma_1) = \begin{bmatrix} b & 0 & & & & & & \\ 0 & a & & & & & & \\ & & a & & & & & \\ & & & e & 0 & d & & \\ & & & 0 & a & 0 & & \\ & & & d & 0 & c & & \\ & & & & & & e & d \\ & & & & & & d & c \end{bmatrix} \begin{matrix} \text{*p*p} \\ \text{*ppp} \\ \text{*pp*} \\ \text{pppp} \\ \text{pp*p} \\ \text{p*pp} \\ \text{ppp*} \\ \text{p*p*} \end{matrix}$$



$$\rho_F^{(3)}(\sigma_2) = \begin{bmatrix} c & d & & & & & & \\ d & e & & & & & & \\ & & a & & & & & \\ & & & e & d & 0 & & \\ & & & d & c & 0 & & \\ & & & 0 & 0 & a & & \\ & & & & & & a & 0 \\ & & & & & & 0 & b \end{bmatrix} \begin{matrix} \text{*p*p} \\ \text{*ppp} \\ \text{*pp*} \\ \text{pppp} \\ \text{pp*p} \\ \text{p*pp} \\ \text{ppp*} \\ \text{p*p*} \end{matrix}$$

The Direct Mapping

- $*pp*p \longrightarrow 10010$
- the problem:
  - trace estimation is over all 2^n bitstrings
  - only an exponentially small fraction of these have no two adjacent ones

Trick

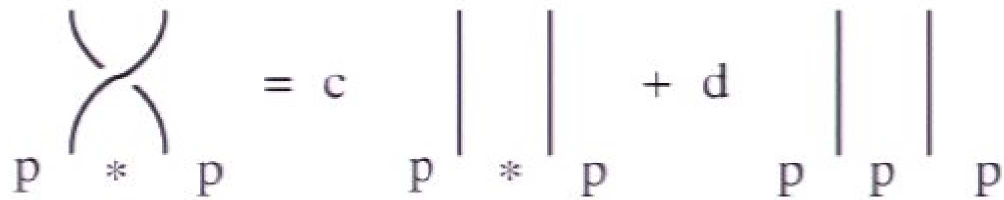
Treat

Zeckendorf Representation

$$\begin{array}{cccccc} 13 & 8 & 5 & 3 & 2 & 1 \\ p & p & * & p & p & * \end{array} \quad \leftrightarrow \quad 6$$

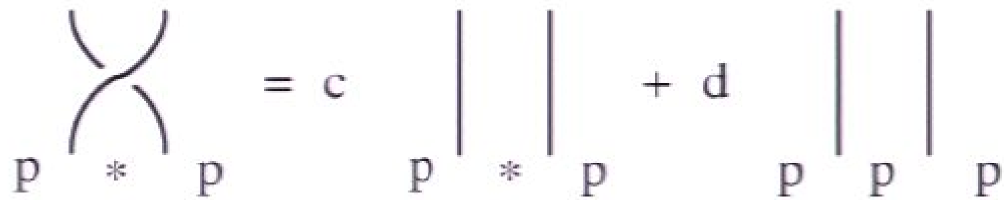
$$\begin{array}{c} p = 0 \\ * = 1 \end{array} \qquad \begin{array}{c} pp = 0 \\ p* = 1 \\ *p = 2 \end{array} \qquad \begin{array}{c} ppp = 0 \\ pp* = 1 \\ p*p = 2 \\ *pp = 3 \\ *p* = 4 \end{array}$$

- an elementary crossing performs a unitary transformation on three neighboring symbols



- in DQC1 the circuit is given a random bitstring
- by the Zeckendorf representation, most such bitstrings correspond to some $p*$ -string
- reversibly extract the relevant three symbols into a clean ancilla register
- transform them, then undo the extraction

- an elementary crossing performs a unitary transformation on three neighboring symbols



- in DQC1 the circuit is given a random bitstring
- by the Zeckendorf representation, most such bitstrings correspond to some $p*$ -string
- reversibly extract the relevant three symbols into a clean ancilla register
- transform them, then undo the extraction

Barrington's Theorem

- which reversible circuits can be implemented using O(1) ancillas?
- anything in NC1 can be done using 5-dimensional ancilla space!
- the standard arithmetic operations

$$+ - \times \div$$

are in NC1 as are comparisons

$$> = <$$

Extracting Symbols

- extracting the leftmost symbol is easy:
  $z(s) \geq f_{n-1}$ iff the leftmost symbol is $*$
  - flip ancilla to 1 if $z > f_{n-1}$
  - subtract f_{n-1} from z if ancilla is 1
- the general case can be reduced to the leftmost bit case by dividing the string into two pieces

$$\begin{array}{cccc|cccccc} 1 & 2 & 3 & 5 & 13 & 8 & 5 & 3 & 2 & 1 \\ * & p & p & * & p & p & * & p & p & p \end{array} \quad \leftrightarrow \quad (6,5)$$

Part II: DQC1-hardness

- we want to find a braid such that the trace of its Fibonacci representation is the trace of a given quantum circuit
- we will use a many to one encoding: many $p*$ -strings correspond to the same bitstring
- "many" must be independent of the bitstring to make the trace unweighted

Part II: DQC1-hardness

- we want to find a braid such that the trace of its Fibonacci representation is the trace of a given quantum circuit
- we will use a many to one encoding: many $p*$ -strings correspond to the same bitstring
- “many” must be independent of the bitstring to make the trace unweighted

The Direct Mapping

- $*pp*p \longrightarrow 10010$
- the problem:
  - trace estimation is over all 2^n bitstrings
  - only an exponentially small fraction of these have no two adjacent ones

Trick

Extracting Symbols

- extracting the leftmost symbol is easy:
  $z(s) \geq f_{n-1}$ iff the leftmost symbol is $*$
  - flip ancilla to 1 if $z > f_{n-1}$
  - subtract f_{n-1} from z if ancilla is 1
- the general case can be reduced to the leftmost bit case by dividing the string into two pieces

$$\begin{array}{cccc|cccccc} 1 & 2 & 3 & 5 & 13 & 8 & 5 & 3 & 2 & 1 \\ * & p & p & * & p & p & * & p & p & p \end{array} \quad \leftrightarrow \quad (6,5)$$

Part II: DQC1-hardness

- we want to find a braid such that the trace of its Fibonacci representation is the trace of a given quantum circuit
- we will use a many to one encoding: many $p*$ -strings correspond to the same bitstring
- "many" must be independent of the bitstring to make the trace unweighted

Encoding

- divide string into groups of three

$$ppp \longrightarrow 0$$
$$p * p \longrightarrow 1$$

- consider blocks of logarithmically many such groups
- each block corresponds to a bit
- the leftmost coding group within a block determines the bit value

$$pp * |p * p| * pp| * pp|ppp| * p*$$

Reduction of DQC1 to Jones

- construct a braid whose Fibonacci representation linearly transforms the encoded bitstring according to the quantum circuit
- the Jones polynomial for the trace closure will then be equal to the trace of the quantum circuit
- since trace estimation is DQC1-hard, then so is estimating the Jones polynomial

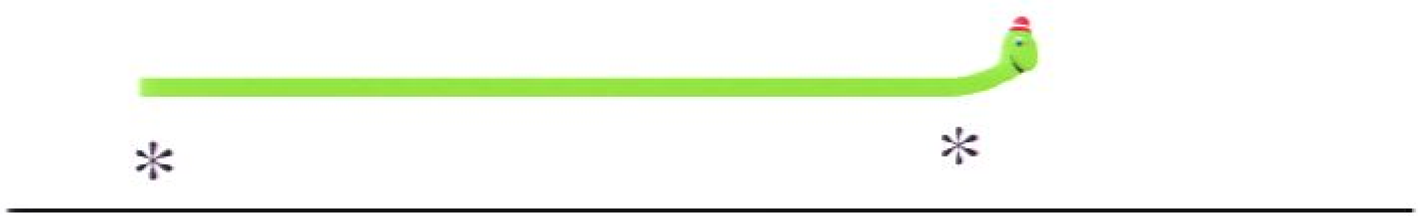
Solovay-Kitaev Theorem

- suppose you have:
  - a space of dimension d
  - a finite set of unitaries which generate a dense subgroup of SU(d)
- one can multiply these to approximate an arbitrary element of SU(d) within ϵ
- the length of the product is $\mathrm{polylog}(\epsilon)$

Density

- The Fibonacci representation is reducible and has blocks depending on the initial and final symbols
- the $*p, p*,$ and $**$ blocks are dense in the corresponding special unitary groups
- The pp block is not
- we can efficiently perform an arbitrary unitary on logarithmically many symbols using the Solovay-Kitaev theorem provided the first or last symbol is $*$

- to simulate a gate one needs to bring a $*$ within logarithmic distance of the encoded qubit(s) it acts upon
- we can use an encoded CNOT to guarantee two initial stars
- we bring these where they are needed using the inchworm



Summary

- One clean qubit computers can efficiently estimate the Jones polynomial of the trace closure of a braid at a fifth root of unity
- Any problem solvable on one clean qubit computers is reducible to this
- Assuming DQC1 $\not\subseteq$ P, this is an exponential speedup over classical computation

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ☑
  - DQC1 ☑
  - QMA [?]
  - Clifford [?]

More Open Questions

- What are the hard instances?
- Topological problems (e.g. unknot)
- Khovanov's invariant
- Implementing one clean qubit computers

Happy Halloween

More Open Questions

- What are the hard instances?
- Topological problems (e.g. unknot)
- Khovanov's invariant
- Implementing one clean qubit computers

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ✓
  - DQC1 ✓
  - QMA [?]
  - Clifford [?]

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ☑
  - DQC1 ☑
  - QMA ?
  - Clifford ?

Summary

- One clean qubit computers can efficiently estimate the Jones polynomial of the trace closure of a braid at a fifth root of unity
- Any problem solvable on one clean qubit computers is reducible to this
- Assuming DQC1 $\not\subseteq$ P, this is an exponential speedup over classical computation

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ✓
  - DQC1 ✓
  - QMA ?
  - Clifford ?

Summary

- One clean qubit computers can efficiently estimate the Jones polynomial of the trace closure of a braid at a fifth root of unity
- Any problem solvable on one clean qubit computers is reducible to this
- Assuming DQC1 $\not\subseteq$ P, this is an exponential speedup over classical computation

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ☑
  - DQC1 ☑
  - QMA [?]
  - Clifford [?]

Open Questions

- extend this to:
  - $t = e^{i2\pi m/k} \quad \text{for} \quad k \neq 5$
  - HOMFLY or Tutte polynomials
- knot invariants for other quantum complexity classes
  - BQP ☑
  - DQC1 ☑
  - QMA ?
  - Clifford ?