Title: QPV: An Overview and Reflections

Speakers: Harry Buhrman

Collection: QPV 2023: Advances in quantum position verification

Date: September 18, 2023 - 11:00 AM

URL: https://pirsa.org/23090010

QPV: An Overview and Reflections

HARRY BUHRMAN

18 September 2023

QPV 2023

PI, Waterloo

University of Amsterdam

QuSoft

Research Center for Quantum Software

Centrum Wiskunde & Informatica
Amsterdam

NET WORKS

Quantum Delta
the Netherlands

NWO

Quantum
Software
Consortium

QuSoft

Overview

- A bit of Introduction and notation
- No-go theorem
- Connection with:
  - Complexity theory
  - ADS/CFT
  - Cryptography
  - Catalytic computation
- Experiments
  - Towards implementation of QPV protocols

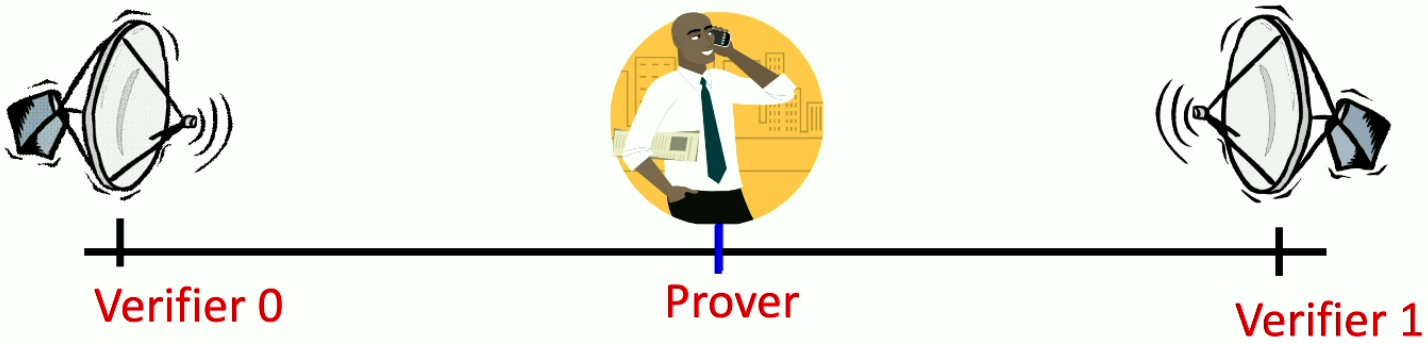
QuSoft

Work of many

- Rene Allerstorfer
- Philip Verduyn Lunell
- Kirsten Kanneworff
- Llorenc Escola Farras
- Ian George
- Damian Pitalua-Garcia
- Florian Speelman
- Adrian Kent
- Alex May
- Kfir Dolev
- Andreas Bluhm
- Nishanth Chandran
- Rafail Ostrovsky
- Gilles Brassard
- Matthias Christandl
- Christian Schaffner
- Serge Fehr
- Eric Chitambar
- Wolfgang Loeffler
- Paul Kwiat
- Anne Broadbent
- David Perez-Garcia
- Richard Cleve
- Bruno Loff
- Michal Coucky
- Ran Gelles
- Vipul Goyal
- Patrick Hayden

QuSoft

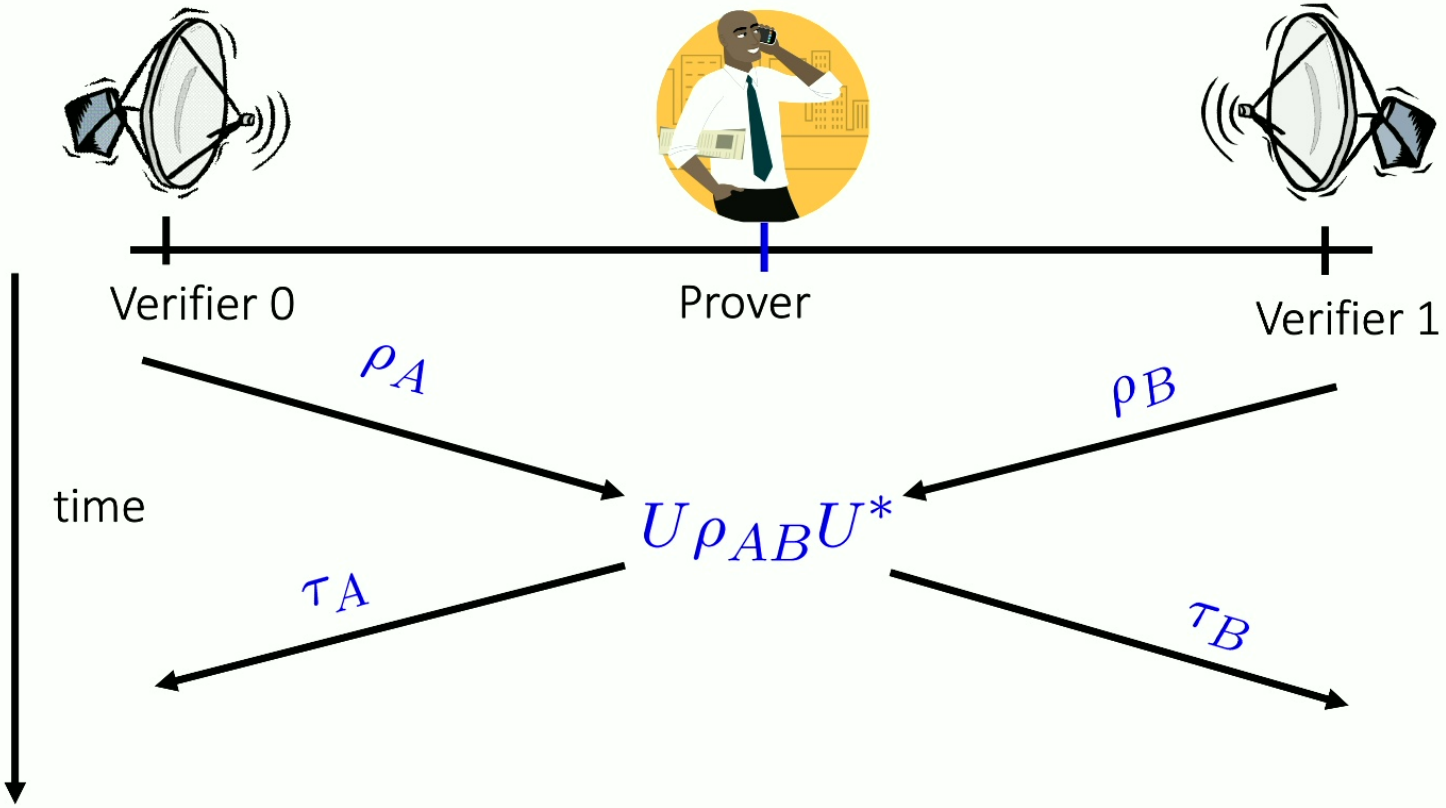
Position Verification



- Prover convince verifiers he is at particular position
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate
- no coalition of (fake) provers, not at the claimed position, can convince verifiers

QuSoft

Most General single round Protocol



QuSoft

Attacking Game

$$U\rho_{AB}U^* = \tau_{AB}$$

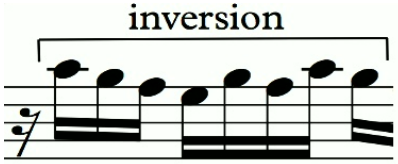
Share Entanglement

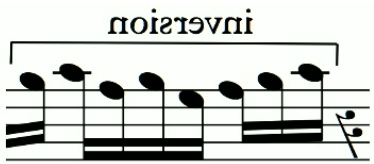
ρ_A ρ_B

σ_A σ_B

Independent messages

τ_A τ_B





Attacking Game

$$U\rho_{AB}U^* = \tau_{AB}$$

Share Entanglement

ρ_A

ρ_B

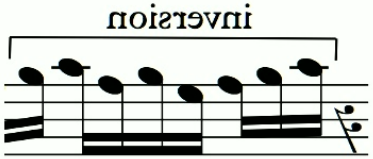
σ_A

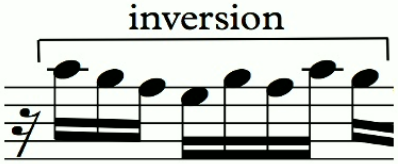
σ_B

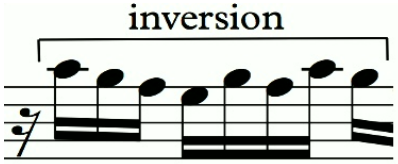
Independent messages

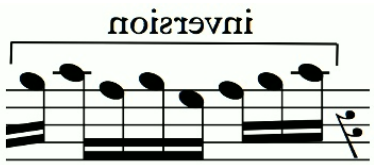
τ_A

τ_B









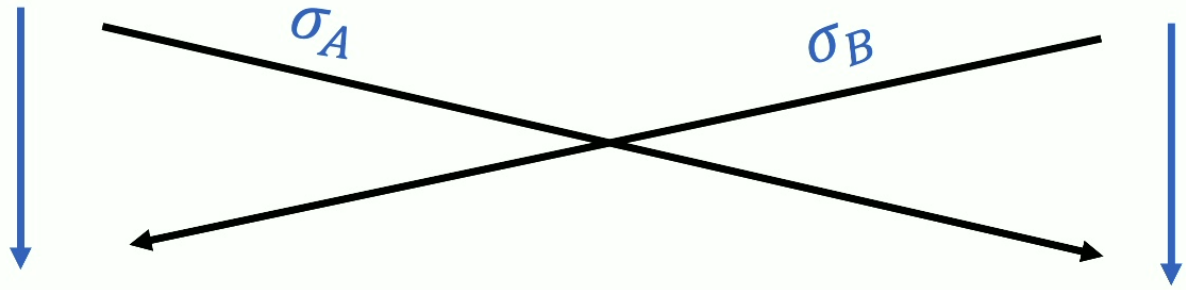
Attacking Game

$$U\rho_{AB}U^* = \tau_{AB}$$

Share Entanglement

ρ_A

ρ_B

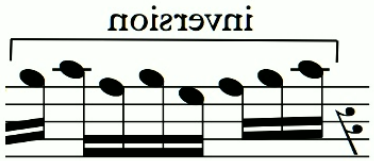


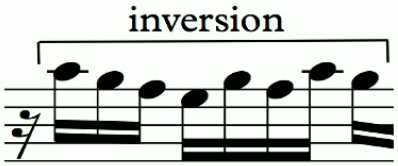
Independent messages

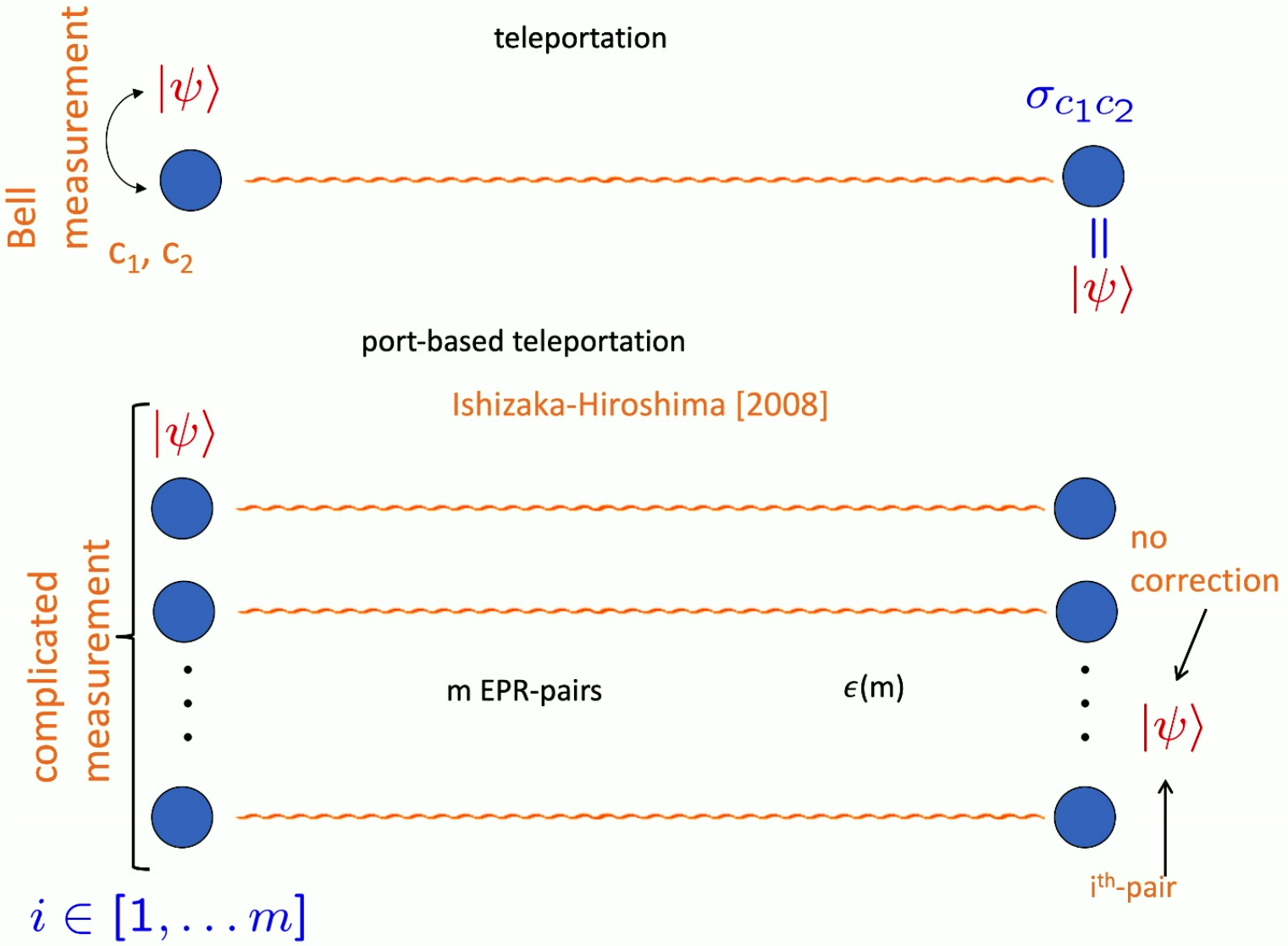
τ_A

τ_B

Can be won by Alice and Bob using exponential amount (in size of ρ_{AB}) of entanglement

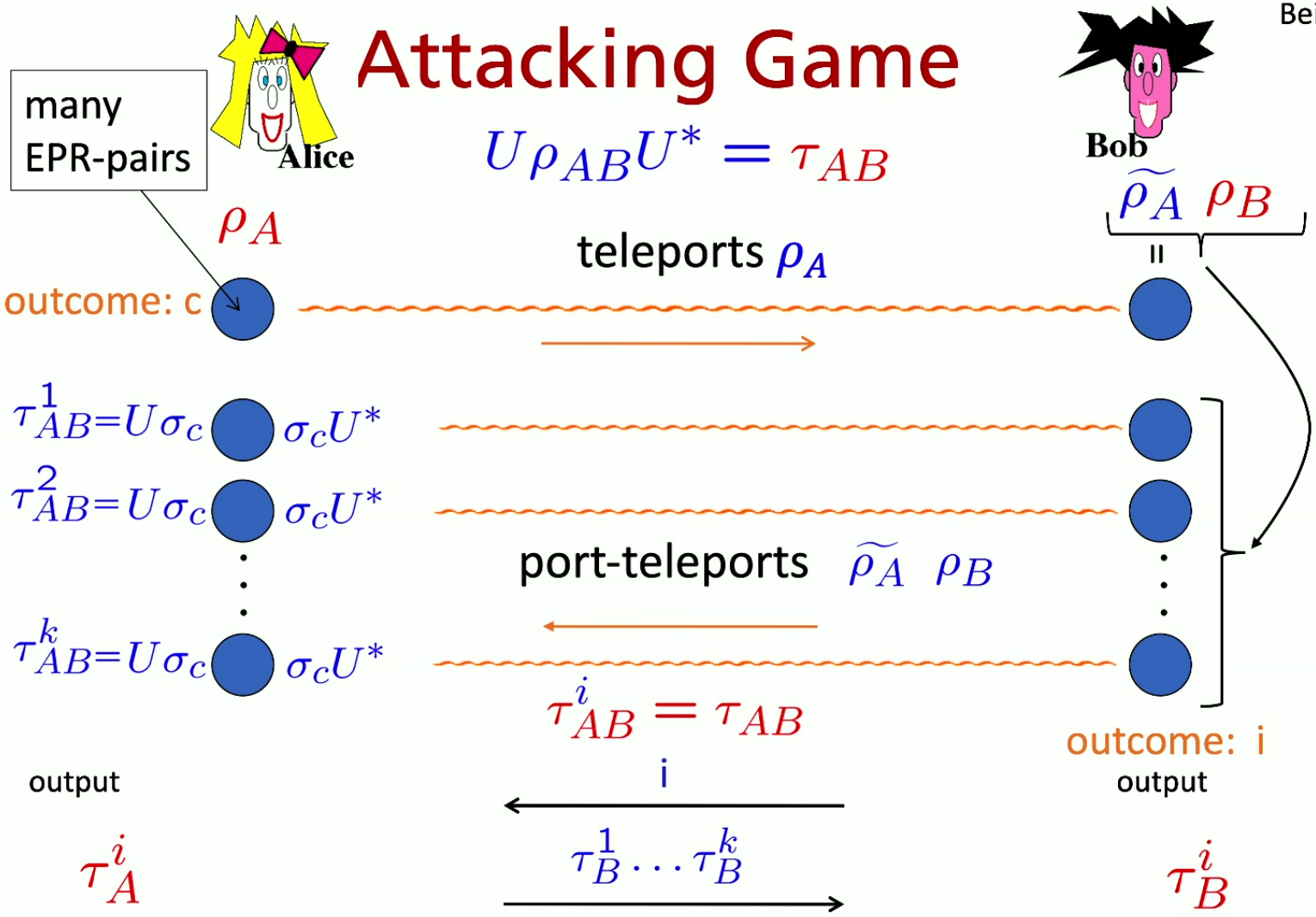





teleportation
Bell measurement
$|\psi\rangle$
c_1, c_2
$\sigma_{c_1 c_2}$
$|\psi\rangle$
port-based teleportation
Ishizaka-Hiroshima [2008]
$|\psi\rangle$
complicated measurement
m EPR-pairs
ϵ(m)
no correction
$|\psi\rangle$
i^{th}-pair
$i \in [1, \ldots m]$

Beigi & König'11

Attacking Game



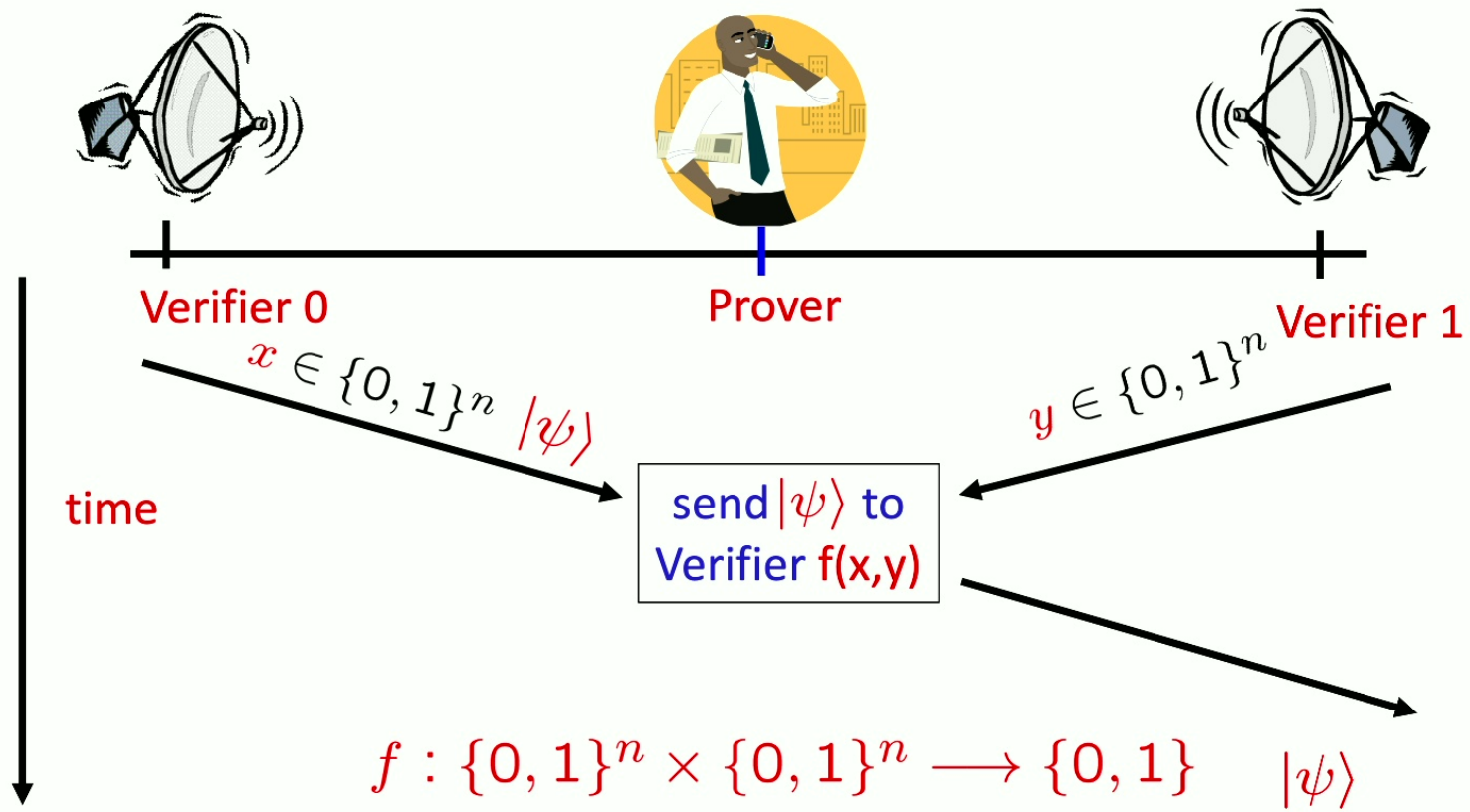
No-Go Theorem

- Any position-verification protocol can be broken
  - uses double-exponential EPR-pairs [B-Chandran-Fehr-Gelles-Goyal-Ostrovsky-Schaffner'10]
  - reduced to single-exponential [Beigi-König'11]
- Question 1: is this optimal?
  - exist a protocol:
  - attack requires many EPR-pairs
  - honest prover & verifiers efficient
- Question 2: Realize protocols experimentally
  - deal with imperfections and errors

QuSoft

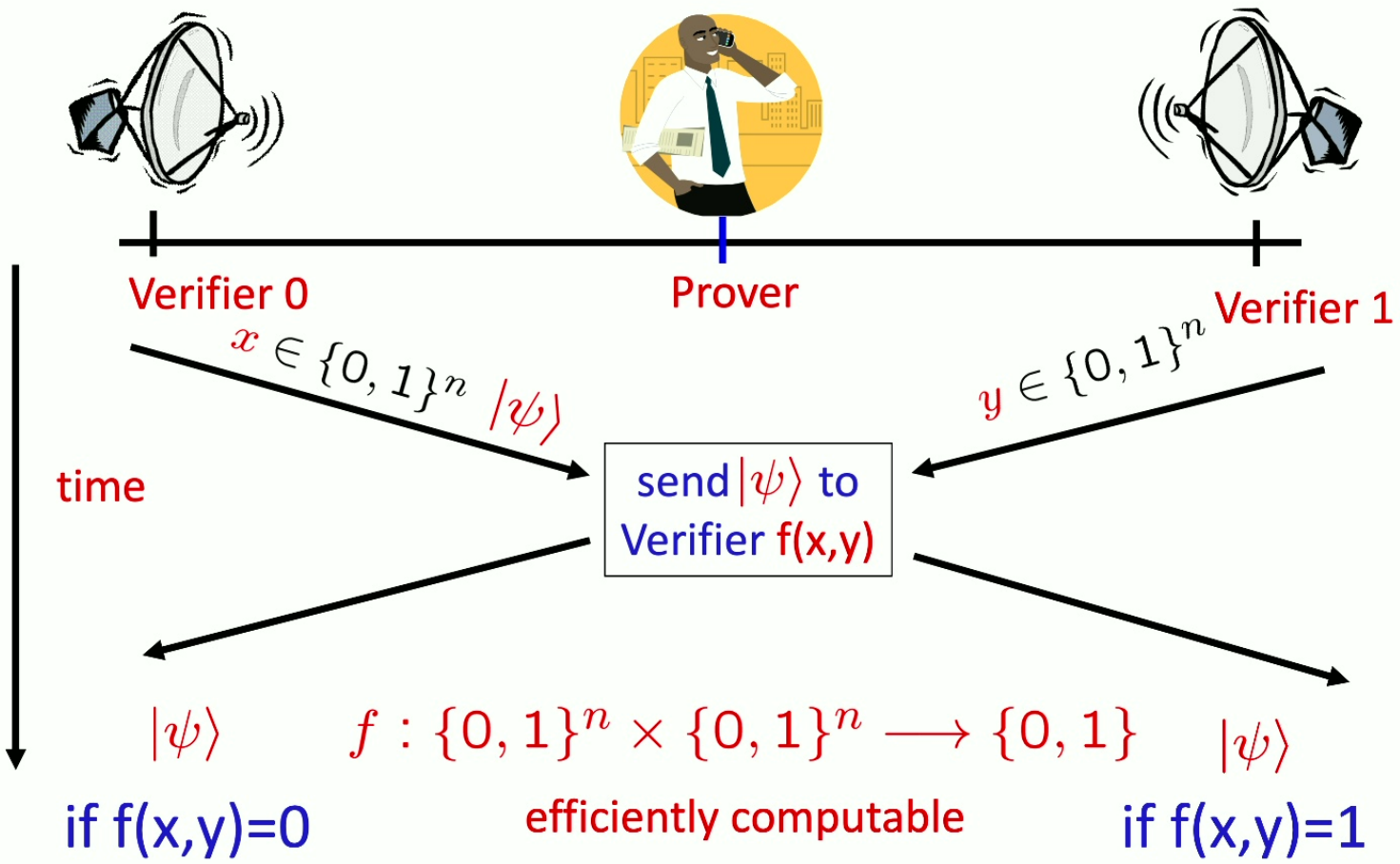
[Kent-Munro-Spiller 2010]

Single-Qubit Protocol: SQP_f (f-routing)

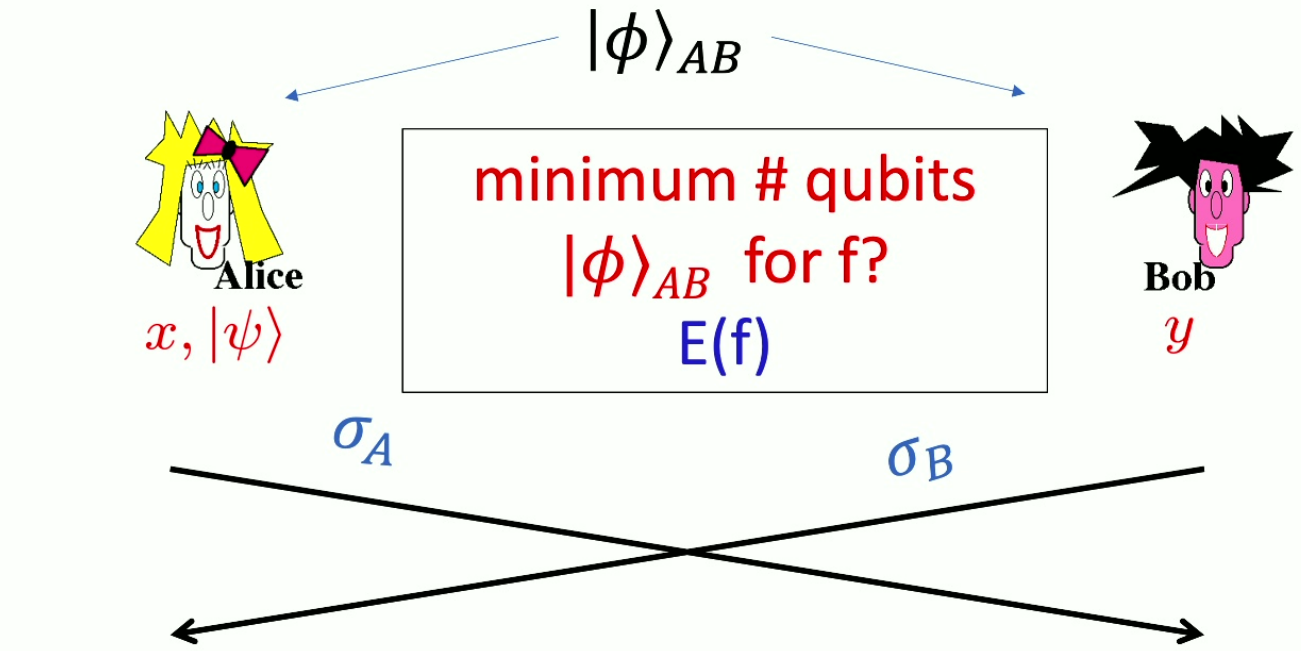


[Kent-Munro-Spiller 2010]

Single-Qubit Protocol: SQP_f (f-routing)



Attacking Game for f-routing



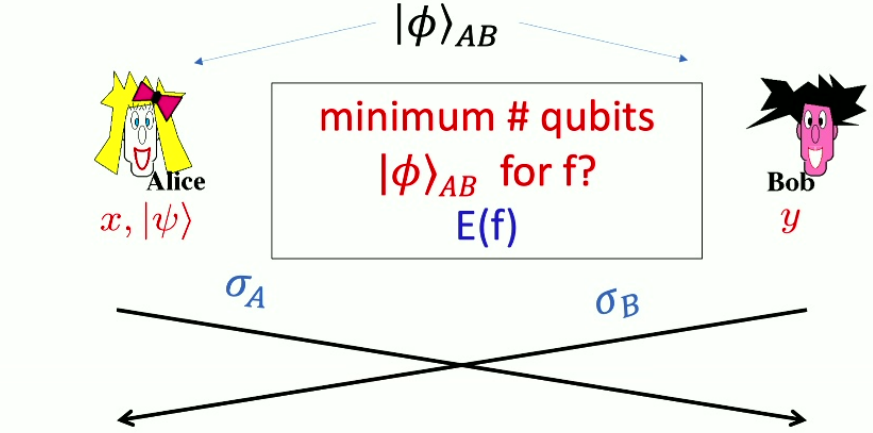
$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$

$|\psi\rangle$ if f(x,y)=0

$|\psi\rangle$ if f(x,y)=1

Computational Complexity Intuition for Attack

Attacking Game for f-routing



$|\psi\rangle$ $f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$ $|\psi\rangle$

if f(x,y)=0 if f(x,y)=1

Intuition

- Qubit has to be on the correct side *before* f(x,y) is known
- E(f) $\geq 2^{S(f)}$ [$S(f)$ = space to compute f]
- We were able to show that:
- E(f) $\leq 2^{S(f)}$, in particular poly-size attack for f in LOGSPACE
- QUESTION: ∃ f such that E(f) = exponential ??
- Best lower-bound: ∃ f: E(f) ≥ n

- QUESTION: ∃ f in P\LOGSPACE, with E(f) >> polynomial.
- Similar situation also manifest in other CS/Crypto problems
  - Private Simultaneous Messages (PSM)
  - Conditional Disclosure of Secrets (CDS)
  - Secret Sharing Protocols
  - Catalytic Space

QuSoft

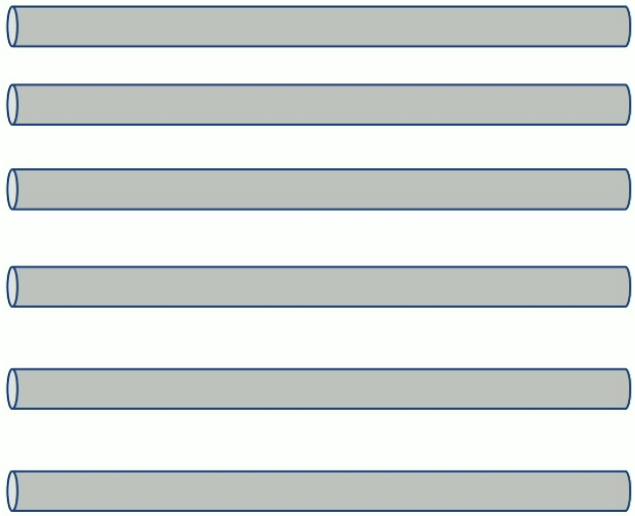
The Garden-Hose Model

$x \in \{0,1\}^n$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$y \in \{0,1\}^n$

share s pipes



The Garden-Hose Model

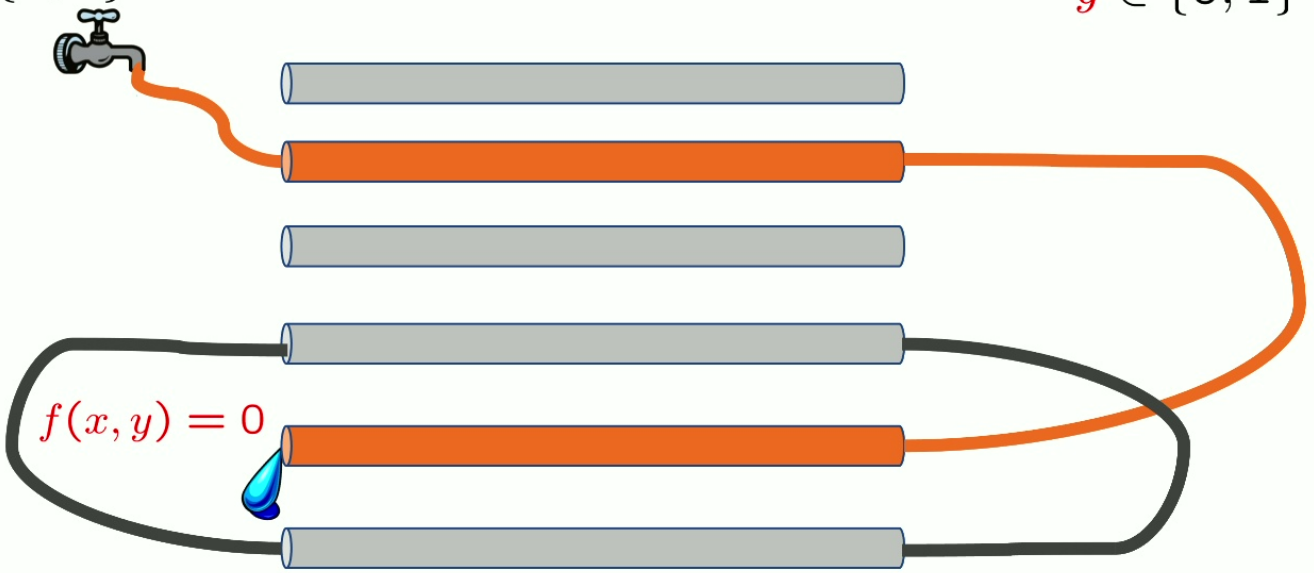
$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

Alice

$x \in \{0,1\}^n$

Bob

$y \in \{0,1\}^n$



- connect pipes with pieces of hose
- Alice connects the water tap

The Garden-Hose Model

Alice

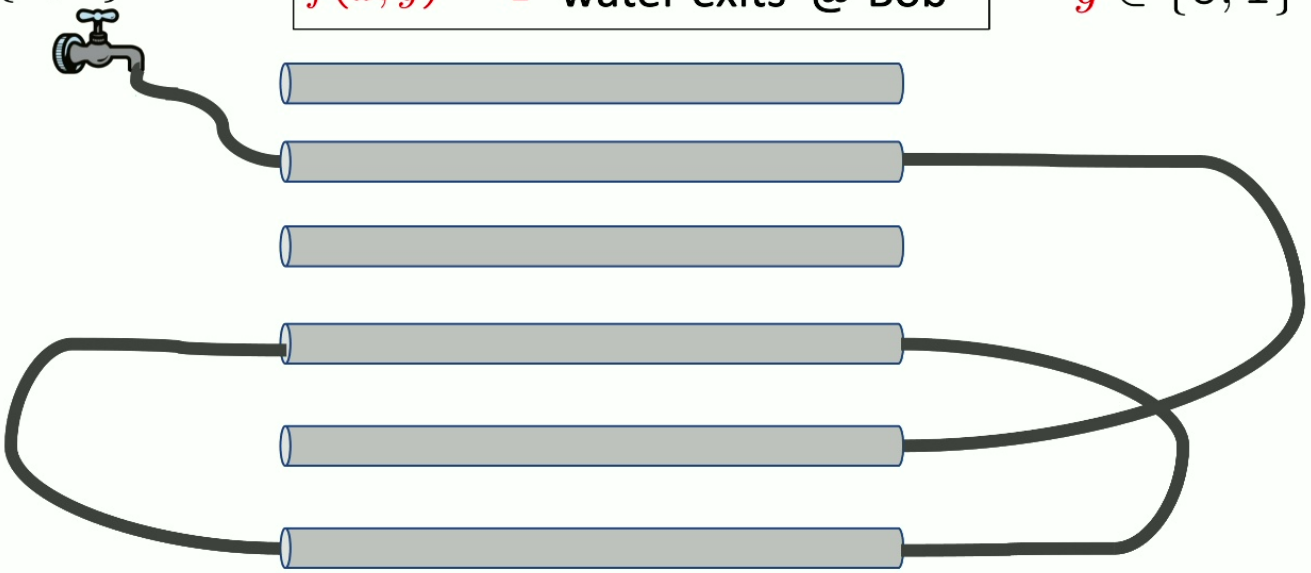
$x \in \{0,1\}^n$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$f(x,y) = 0$ water exits @ Alice
$f(x,y) = 1$ water exits @ Bob

Bob

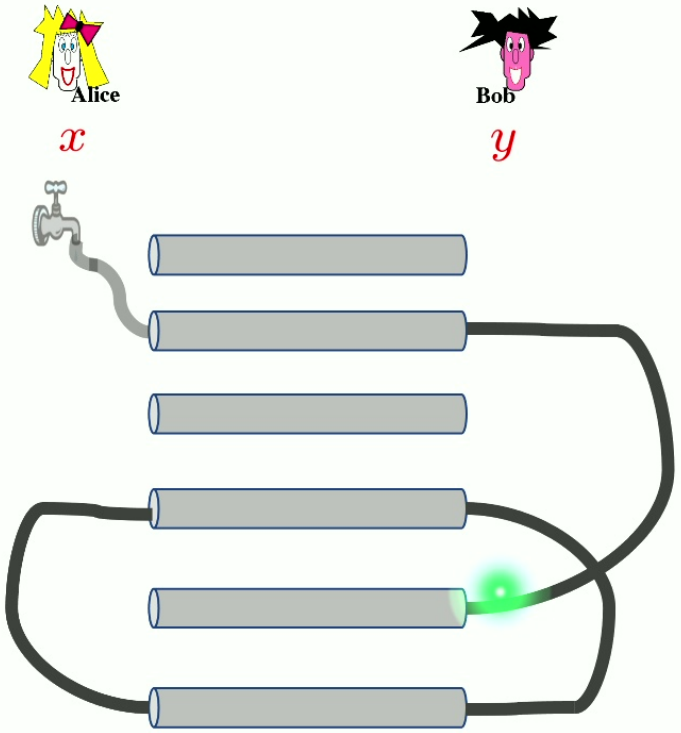
$y \in \{0,1\}^n$



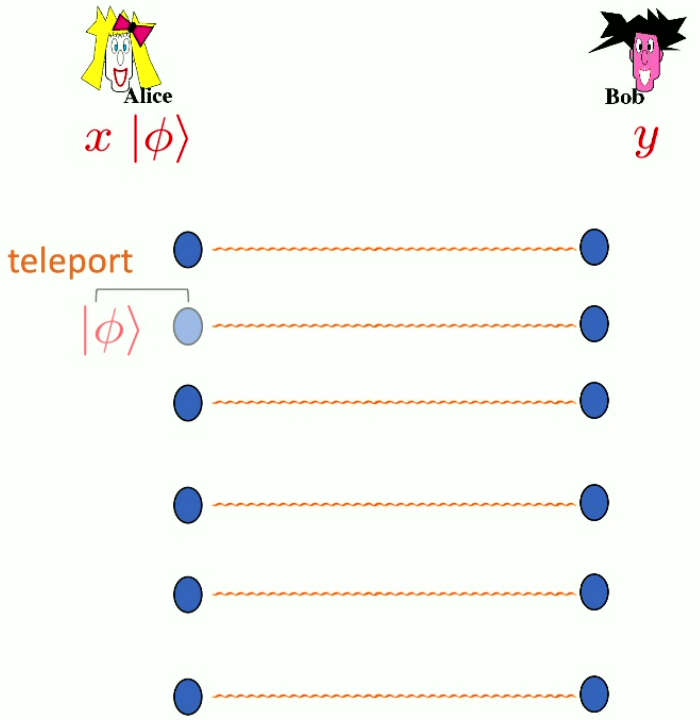
Garden-Hose complexity of f: GH(f)
minimum # of pipes needed to compute f

GH(f) ¸ E(SQP$_f$)

Garden-hose



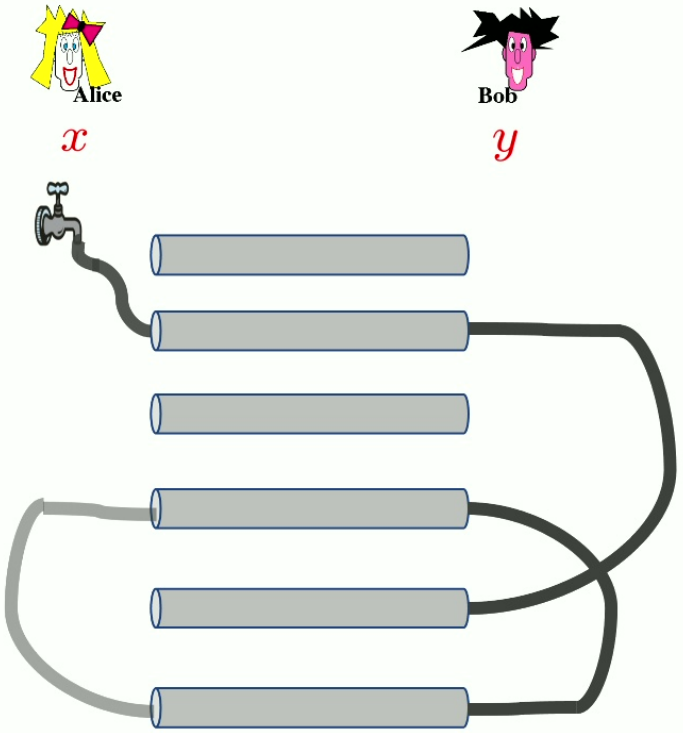
Attacking game



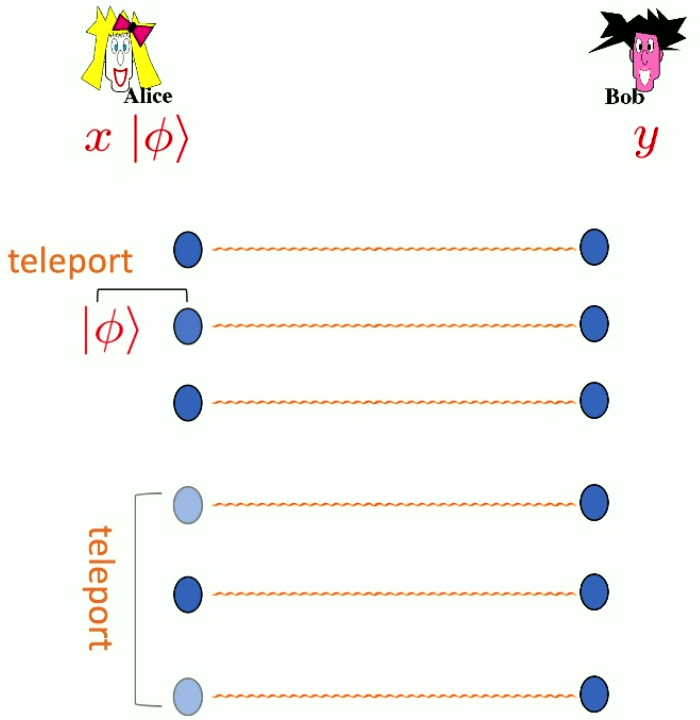
QuSoft

GH(f)¸E(SQP$_f$)

Garden-hose

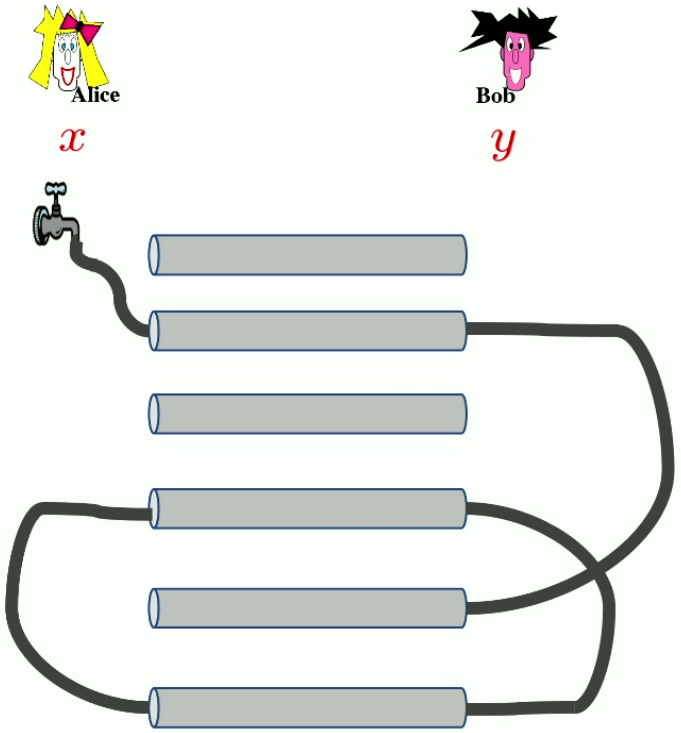


Attacking game



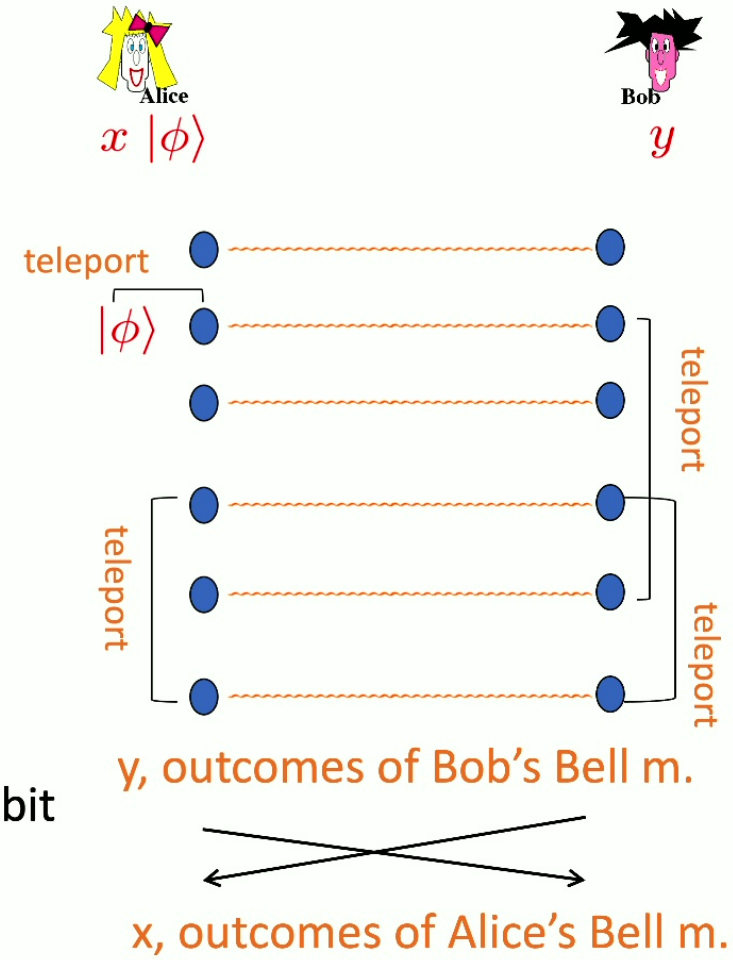
GH(f)¸E(SQP$_f$)

Garden-hose



- using x & y can follow the water/qubit

Attacking game

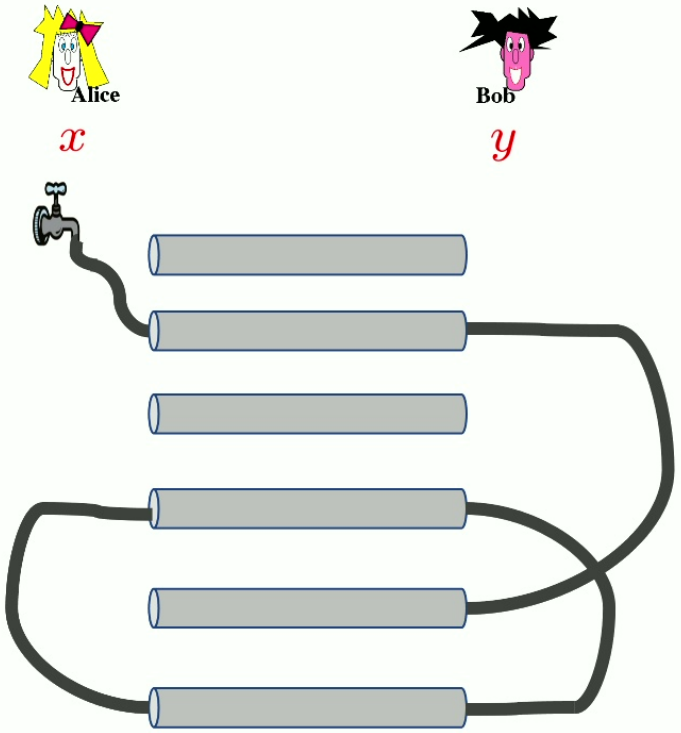


y, outcomes of Bob's Bell m.

x, outcomes of Alice's Bell m.

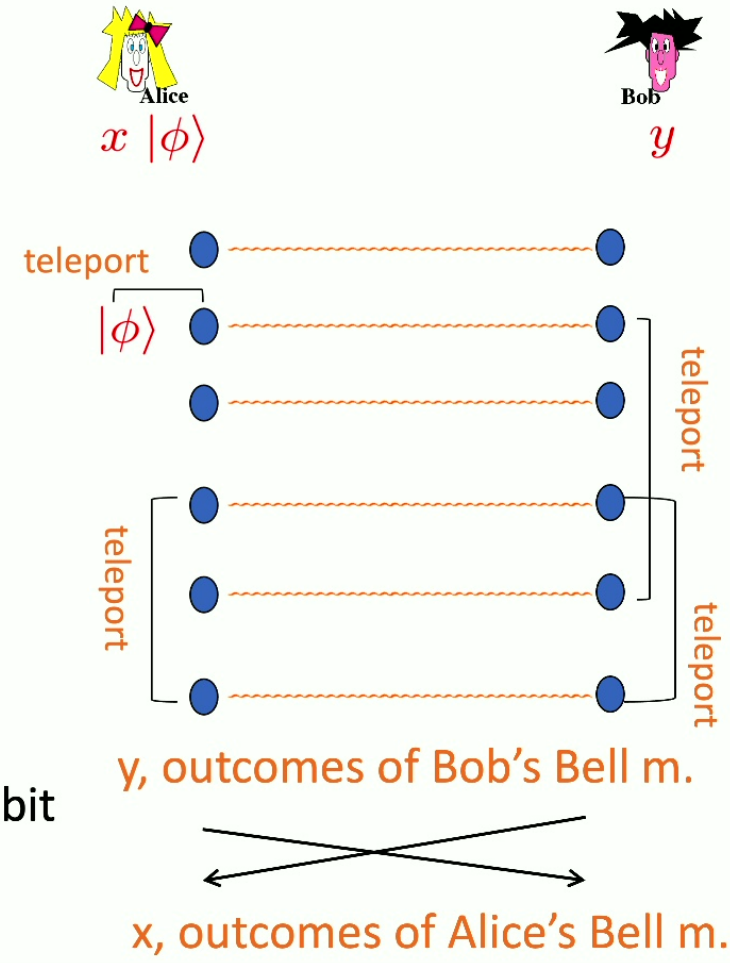
GH(f)¸E(SQP$_f$)

Garden-hose



- using x & y can follow the water/qubit
- correct water/qubit using all measurement outcomes

Attacking game



Relation with SQP_f

- $GH(f) \geq E(f)$
- The two models are not equivalent
  - exists f: $GH(f) = n$
    $E(F) \leq \log(n)$
- Quantum garden-hose model
  - give Alice & Bob also entanglement
  - are models now equivalent?
  - Probably not but we have no proof

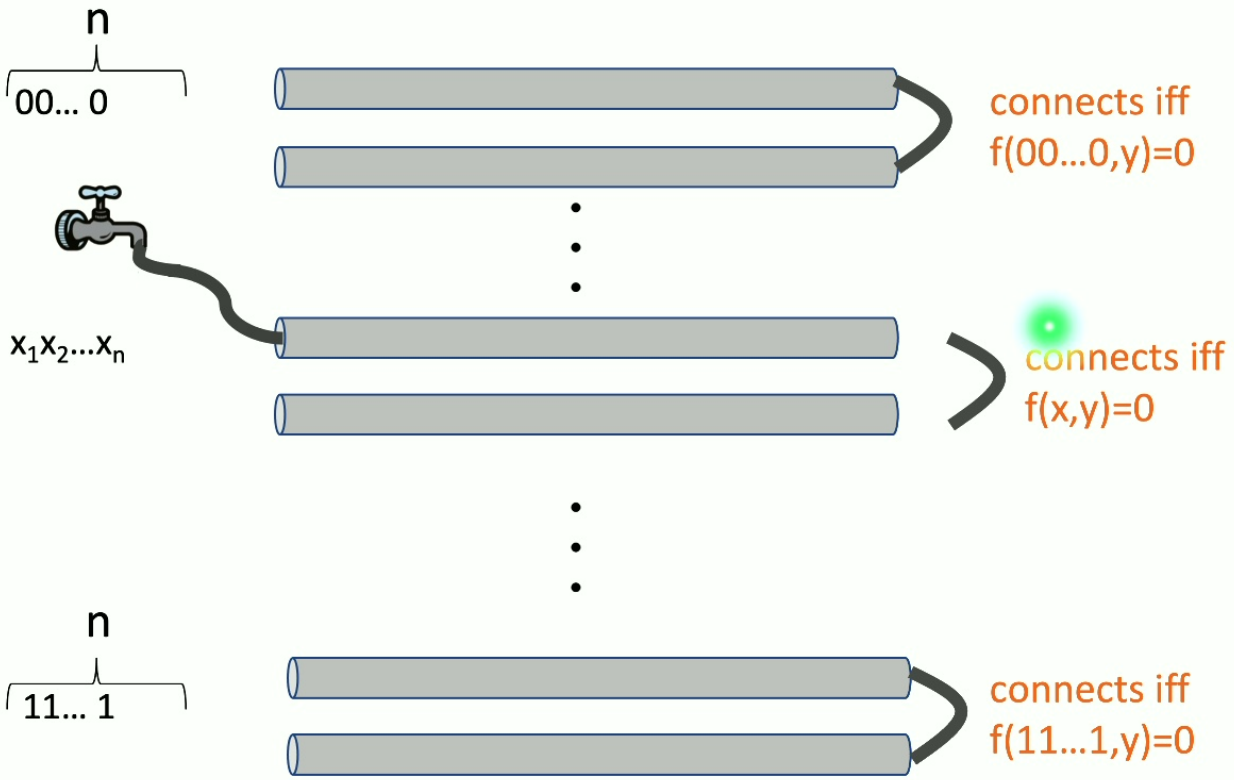
QuSoft

$x_1x_2...x_n$

Any f has GH(f) ≤ 2^{n+1}

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$y_1y_2...y_n$



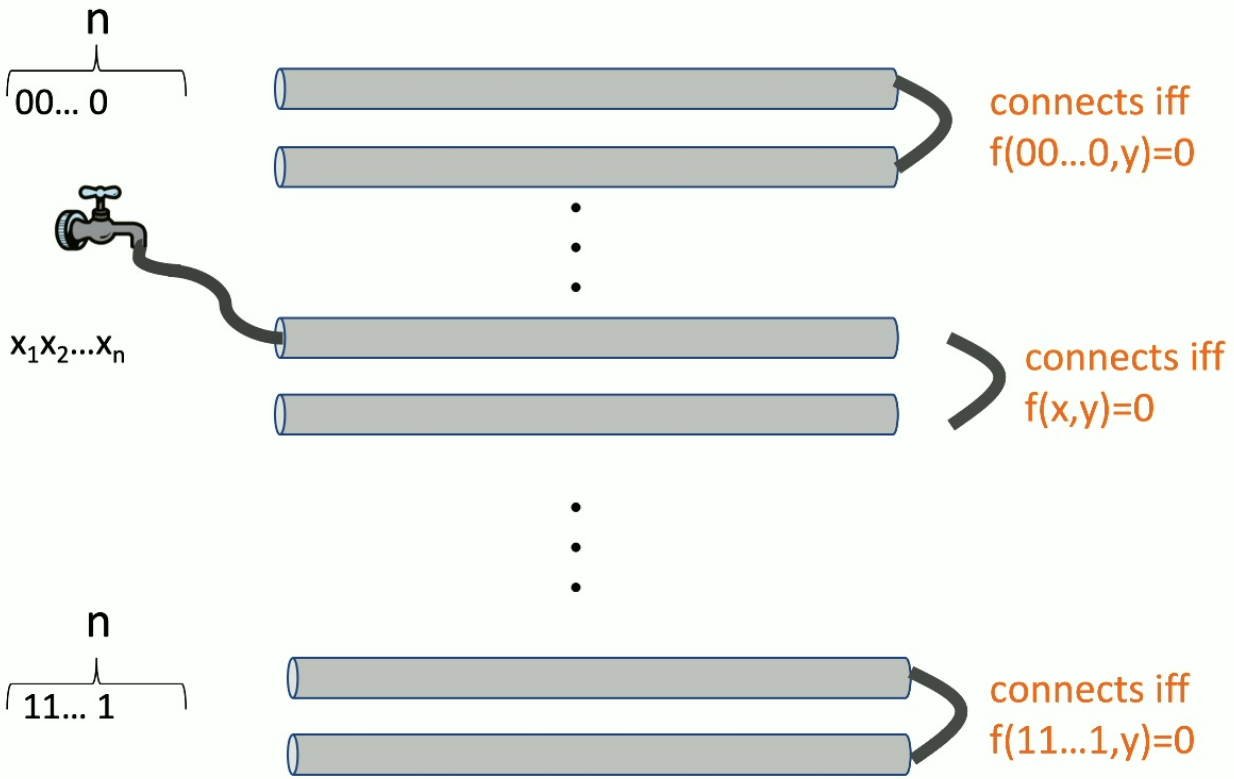
2^{n+1} pipes

$x_1x_2...x_n$

Any f has GH(f) ≤ 2^{n+1}

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$y_1y_2...y_n$



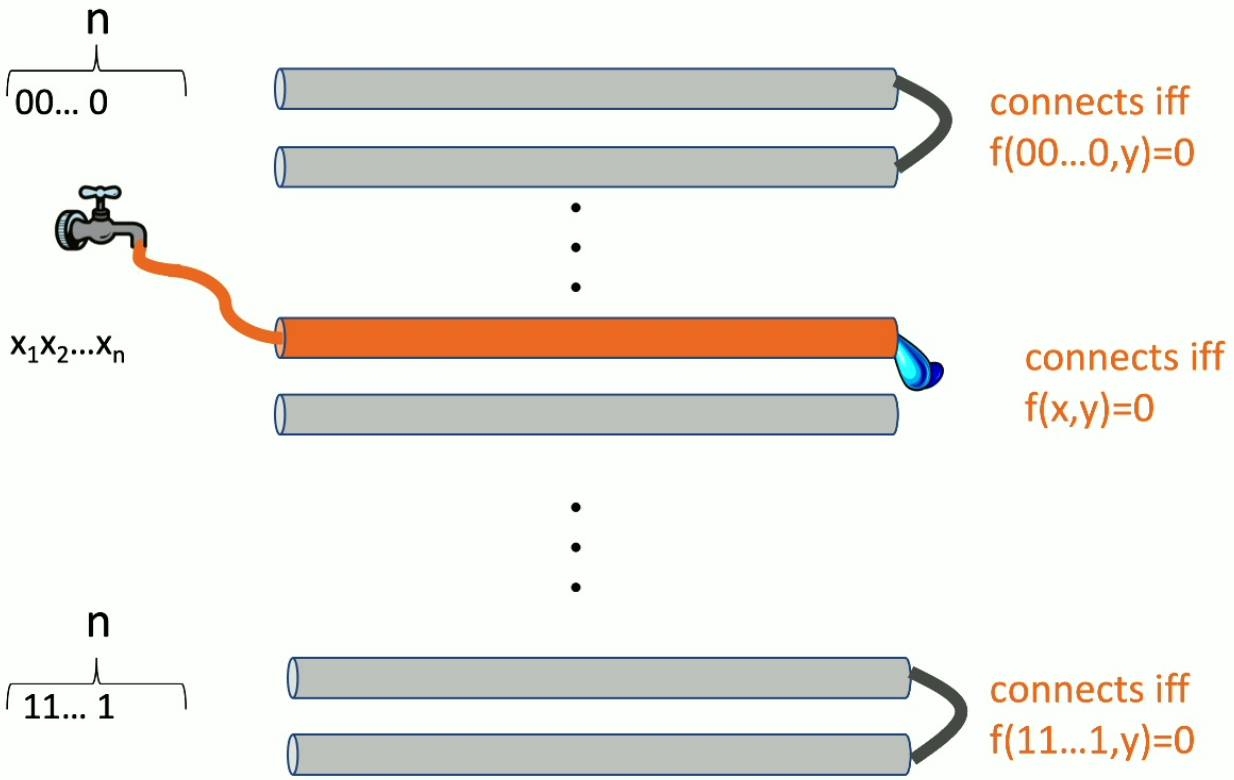
2^{n+1} pipes

$x_1x_2...x_n$

Any f has GH(f) ≤ 2^{n+1}

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$y_1y_2...y_n$



2^{n+1} pipes

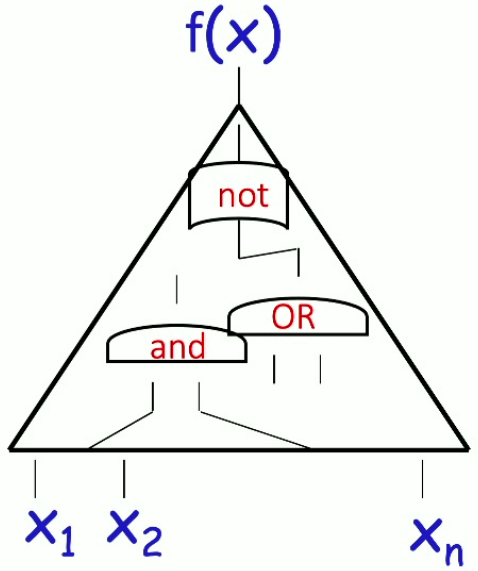
Garden-Hose complexity

- every f has GH(f) $\leq 2^{n+1}$
- f in logspace (L) then GH(f) is polynomial

QuSoft

NC^1

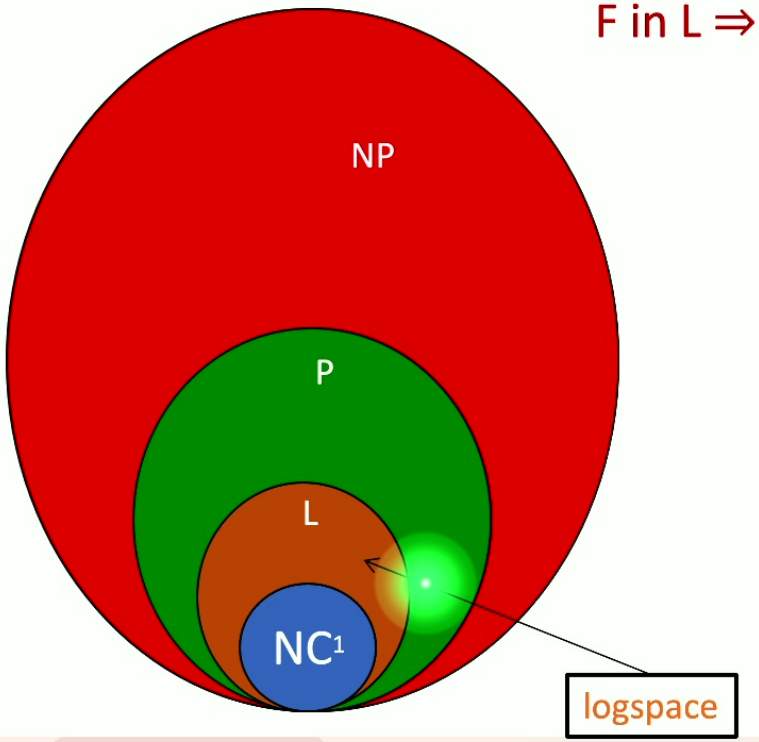
size is polynomial
depth is log(n)



$NP = NC^1$?

we will see
F in L ⇒ E(f)≤ polynomial

No proof that
$NP \neq NC^1$



QuSoft

Barrington's Theorem [1989]

NC^1	=	Branching Programs
• Polynomial size circuits • Log-depth		• Polynomial size • Permutations from S_5

QuSoft

Permutation Branching Programs of size k

input: $x_1 \ldots x_n$

list of instructions:

$$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_k, \sigma_k^0, \sigma_k^1)$$

$i_j \in [1 \ldots n]$

$\sigma_j^0, \sigma_j^1 \in S_5$

evaluate:

$$(i_j, \sigma_j^0, \sigma_j^1) \text{ to } \begin{cases} \sigma_j^0 & \text{if } x_{i_j} = 0 \\ \sigma_j^1 & \text{if } x_{i_j} = 1 \end{cases}$$

$$\sigma_1^{x_{i_1}} \circ \sigma_2^{x_{i_2}} \circ \ldots \circ \sigma_k^{x_{i_k}}$$

=

Identity

accept

=

fixed 5-cycle

reject

example:

$(2, \sigma_1^0, \sigma_1^1), (1, \sigma_2^0, \sigma_2^1), (2, \sigma_3^0, \sigma_3^1)$

input: x_1 x_2

= =

0 1

$\sigma_1^1 \circ \sigma_2^0 \circ \sigma_3^1$

Permutation Branching Programs of size k

input: $x_1 \ldots x_n$

list of instructions:

$$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_k, \sigma_k^0, \sigma_k^1)$$

$i_j \in [1 \ldots n]$

$\sigma_j^0, \sigma_j^1 \in S_5$

evaluate:

$$(i_j, \sigma_j^0, \sigma_j^1) \text{ to } \begin{cases} \sigma_j^0 & \text{if } x_{i_j} = 0 \\ \sigma_j^1 & \text{if } x_{i_j} = 1 \end{cases}$$

$$\sigma_1^{x_{i_1}} \circ \sigma_2^{x_{i_2}} \circ \ldots \circ \sigma_k^{x_{i_k}}$$

// Identity — accept

\\ fixed 5-cycle — reject

example:

$(2, \sigma_1^0, \sigma_1^1), (1, \sigma_2^0, \sigma_2^1), (2, \sigma_3^0, \sigma_3^1)$

input: $x_1 = 0$, $x_2 = 1$

$\sigma_1^1 \circ \sigma_2^0 \circ \sigma_3^1$

// Identity — accept

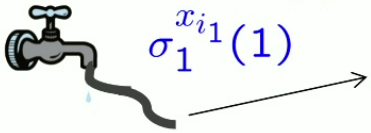
\\ fixed 5-cycle — reject

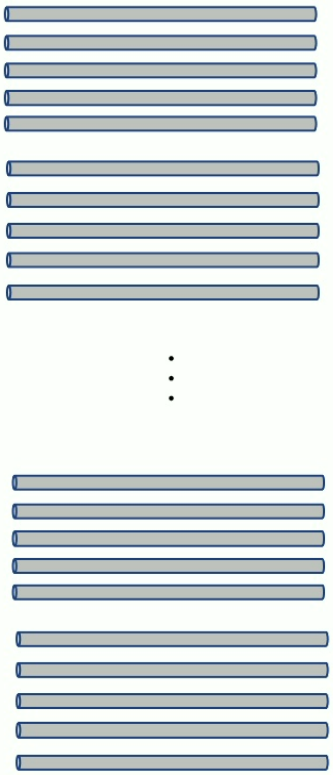
$f(x,y) \in NC^1 \Longrightarrow GH(f) \leq poly(n)$

$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_{p(n)}, \sigma_{p(n)}^0, \sigma_{p(n)}^1)$

WOLG alternates between x & y

connects to pipe $\sigma_1^{x_{i_1}}(1)$





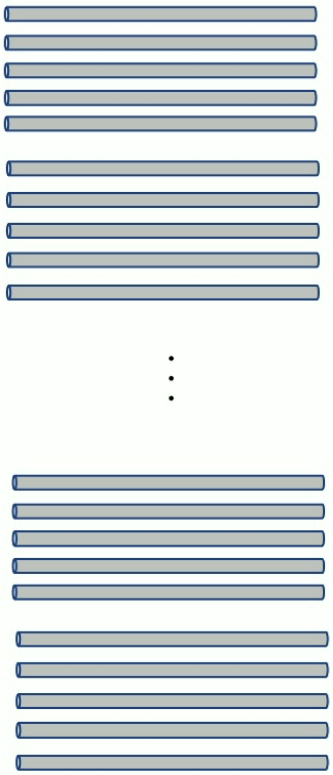
connects pipes according $\sigma_2^{y_{i_2}}$

5*p(n)-pipes

$f(x,y) \in NC^1 \Longrightarrow GH(f) \leq poly(n)$

$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_{p(n)}, \sigma_{p(n)}^0, \sigma_{p(n)}^1)$

WOLG alternates between x & y



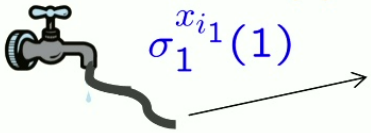
5*p(n)-pipes

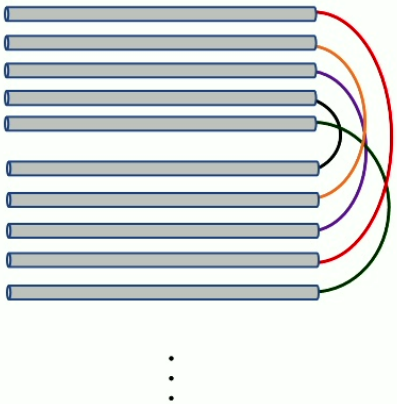
$f(x,y) \in NC^1 \Longrightarrow GH(f) \leq poly(n)$

$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_{p(n)}, \sigma_{p(n)}^0, \sigma_{p(n)}^1)$

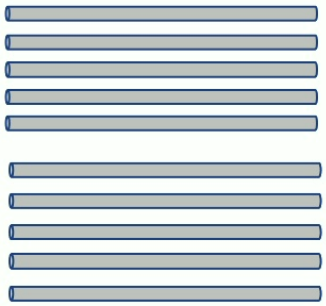
WOLG alternates between x & y

connects to pipe $\sigma_1^{x_{i_1}}(1)$





connects pipes according $\sigma_2^{y_{i_2}}$



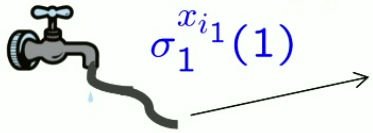
5*p(n)-pipes

$f(x,y) \in NC^1 \Longrightarrow GH(f) \leq poly(n)$

$(i_1, \sigma_1^0, \sigma_1^1), (i_2, \sigma_2^0, \sigma_2^1), \ldots, (i_{p(n)}, \sigma_{p(n)}^0, \sigma_{p(n)}^1)$

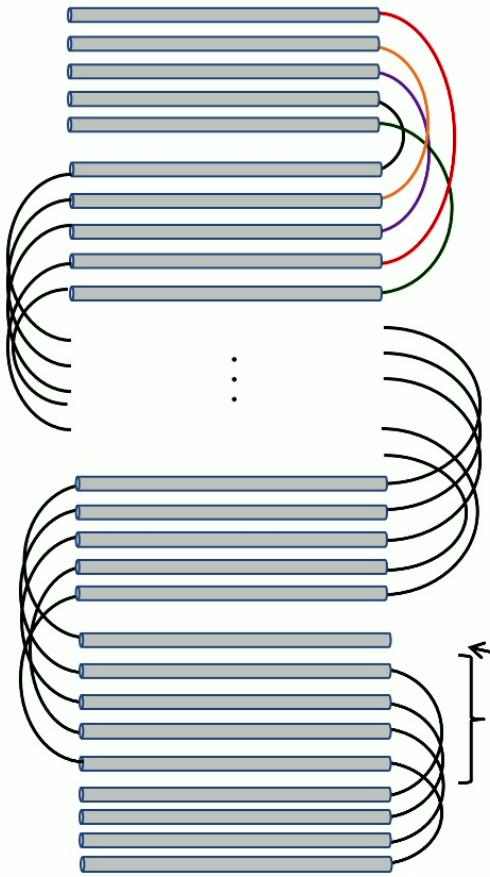
WOLG alternates between x & y

connects to pipe $\sigma_1^{x_{i_1}}(1)$



connects pipes according $\sigma_2^{y_{i_2}}$

connects pipes according $\sigma_3^{x_{i_3}}$



$$\sigma_1^{x_{i_1}} \circ \sigma_2^{y_{i_2}} \circ \ldots \circ \sigma_{p(n)}^{x_{i_{p(n)}}} = \sigma$$

connects pipes according $\sigma_{p(n)}^{x_{i_{p(n)}}}$

f(x,y)=1 ⇒ σ = identity

water comes out here

f(x,y)=0 ⇒ σ = 5-cycle

water comes out here

5*p(n)-pipes + 4

Garden-Hose complexity

- every f has GH(f) $\leq$ exponential
- f in NC^1 then GH(f) $\leq$ polynomial
- extend to Logspace
  - use S_n i.s.o. S_5
- exist f with GH(f) exponential (counting)
- g $\in$ {equality, IP, majority}, GH(g) $\geq$ n
  - techniques from communication complexity
- Note: f $\in P$ and E(f) $>$ polynomial $\Longrightarrow$ P$\neq$ L

QuSoft

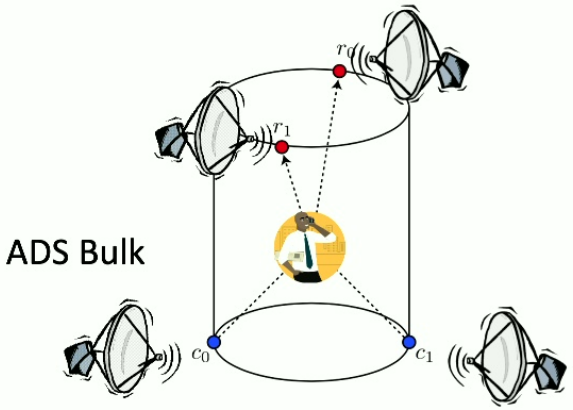
Garden-Hose complexity

- every f has GH(f) $\leq$ exponential
- f in NC^1 then GH(f) $\leq$ polynomial
- extend to Logspace
  - use S_n i.s.o. S_5
- exist f with GH(f) exponential (counting)
- g $\in$ {equality, IP, majority}, GH(g) $\geq$ n
  - techniques from communication complexity
- Note: f $\in P$ and E(f) $>$ polynomial $\Longrightarrow$ P$\neq$ L
- QUESTION does such an f exists?

QuSoft

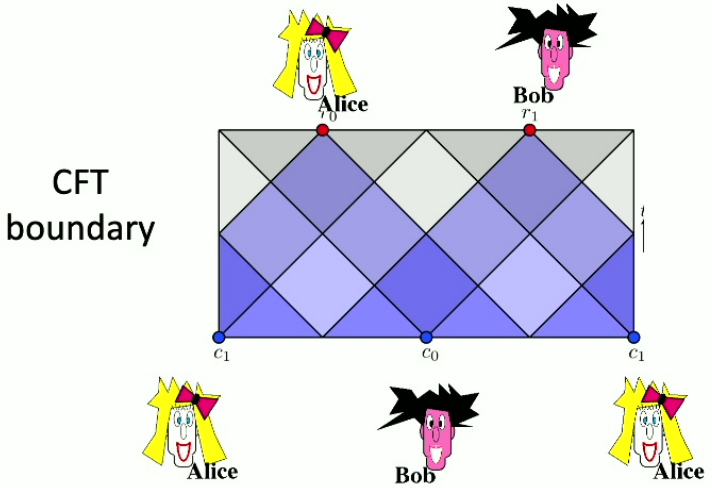
ADS/CFT

- Intriguing connection with ADS/CFT [May'21, Dolev-Cree'22]



Honest QPV protocol

correspondence

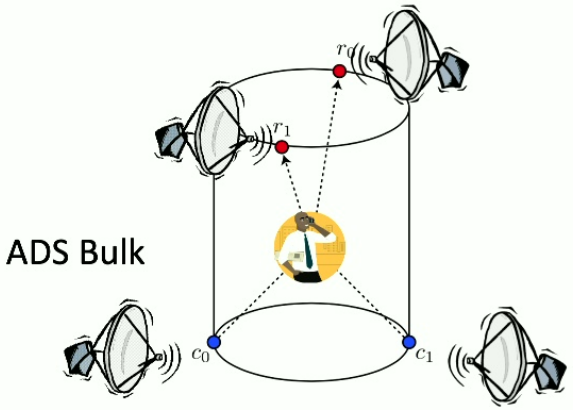


Attack on QPV protocol
(non-local computation)

- Correspondence –> linear upper bound on entanglement
- No construction is given
- Assumptions and unproven conjectures are needed
- No-Go theorem follows (or is in line with ADS/CFT)
- f $\in P \implies$ E(f) $\leq$ polynomial

ADS/CFT

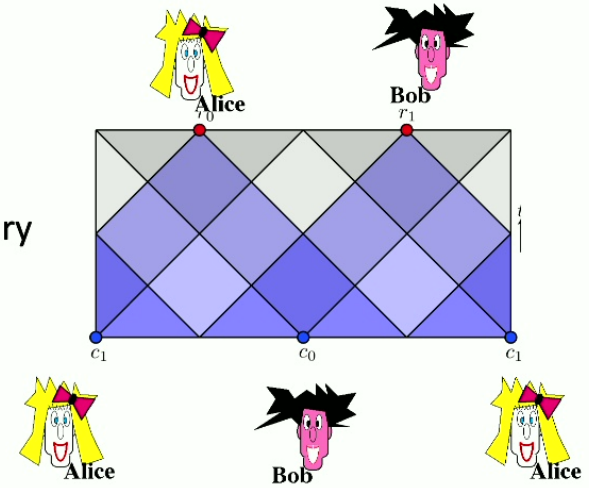
- Intriguing connection with ADS/CFT [May'21, Dolev-Cree'22]



Honest QPV protocol

correspondence

CFT boundary



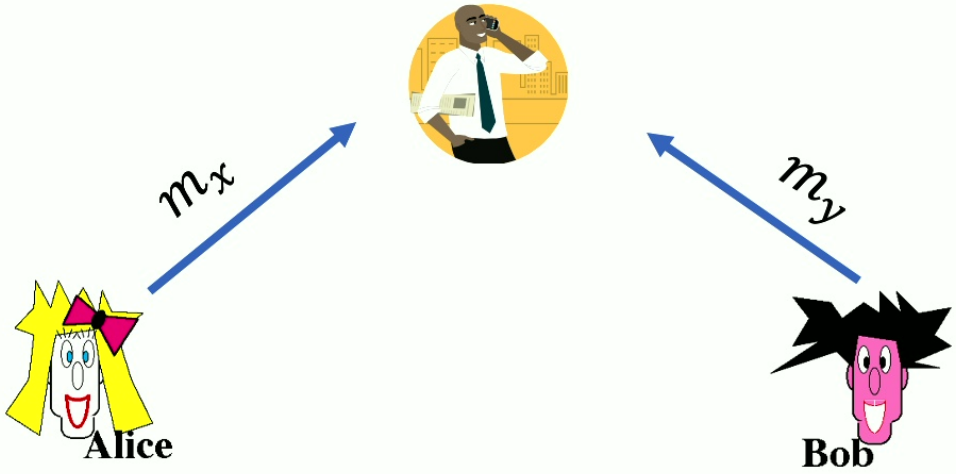
Attack on QPV protocol
(non-local computation)

- Correspondence –> linear upper bound on entanglement
- No construction is given
- Assumptions and unproven conjectures are needed
- No-Go theorem follows (or is in line with ADS/CFT)
- $f \in P \implies E(f) \leq$ polynomial

- What about the other barriers in CS?
- Are they connected to QPV?
- Does ADS/CFT have baring on them?

Conditional Disclosure of Secrets (CDS)

learns s iff $f(x,y) = 1$



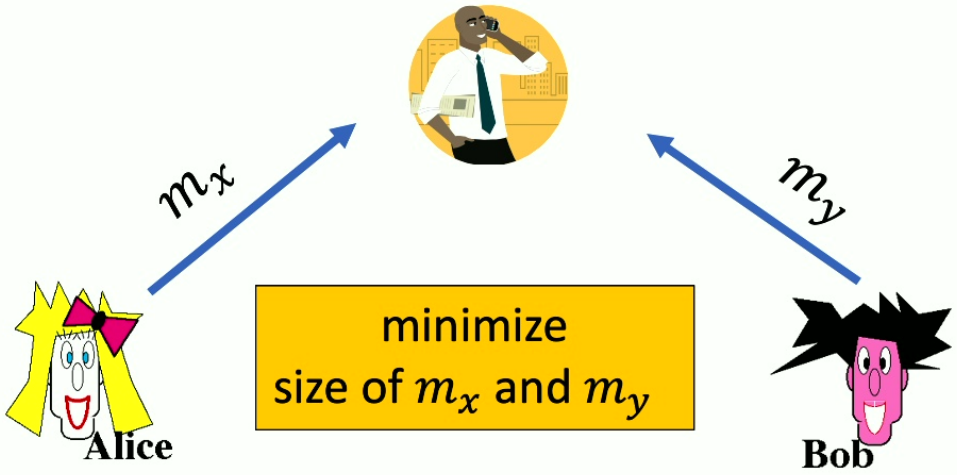
$x = x_1 \dots x_n$ $\qquad$ $y_1 \dots y_n$, $s \in \{0,1\}$

$r = r_1 \dots r_m$ $\qquad$ shared random bits $\qquad$ $r = r_1 \dots r_m$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

Conditional Disclosure of Secrets (CDS)

learns s iff $f(x,y) = 1$



$x = x_1 \dots x_n$ $\qquad$ $y_1 \dots y_n$, $s \in \{0,1\}$

$r = r_1 \dots r_m$ $\qquad$ shared random bits $\qquad$ $r = r_1 \dots r_m$

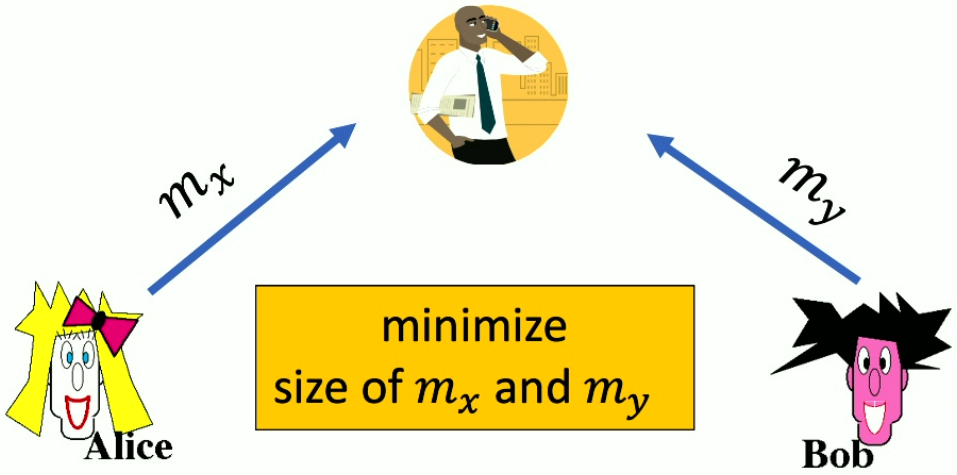
$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

Constructions:
- Any f exponential size CDS
- f in #L ⇒ poly-size CDS

Lower bounds
- Only linear lower bounds known
- Function not in P: poly-size CDS

Conditional Disclosure of Secrets (CDS)

learns s iff $f(x,y) = 1$



minimize size of m_x and m_y

$x = x_1 \dots x_n$ $\quad$ $y_1 \dots y_n$, $s \in \{0,1\}$

$r = r_1 \dots r_m$ $\quad$ shared random bits $\quad$ $r = r_1 \dots r_m$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

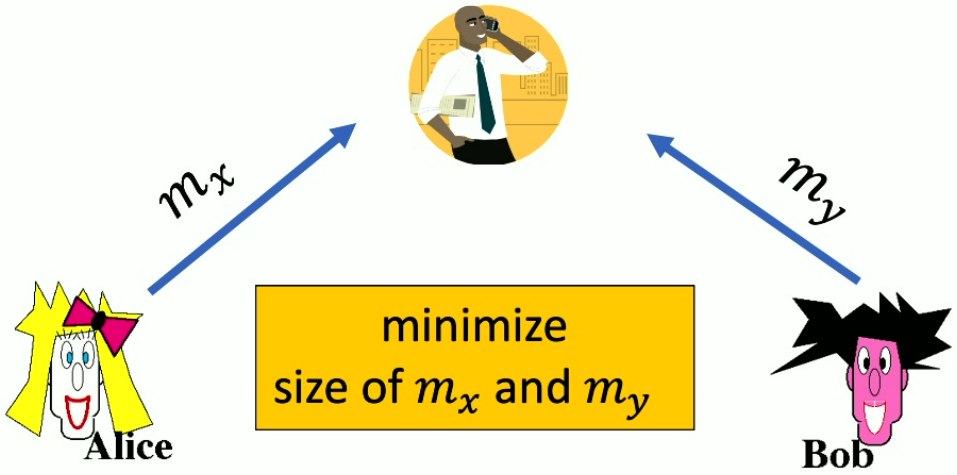
Constructions:
- Any f exponential size CDS
- f in #L ⇒ poly-size CDS

Lower bounds
- Only linear lower bounds known
- Function not in P: poly-size CDS

Quantum version of CDQS
- Classical inputs x & y
- Quantum shared state $|\phi\rangle_{AB}$
- Quantum messages $|m_x\rangle$ & $|m_y\rangle$
- Quantum secret: $|s\rangle$

Conditional Disclosure of Secrets (CDS)

learns s iff $f(x,y) = 1$



minimize size of m_x and m_y

$x = x_1 \dots x_n$ $\quad$ $y_1 \dots y_n$, $s \in \{0,1\}$

$r = r_1 \dots r_m$ $\quad$ shared random bits $\quad$ $r = r_1 \dots r_m$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

Constructions:
- Any f exponential size CDS
- f in #L ⇒ poly-size CDS

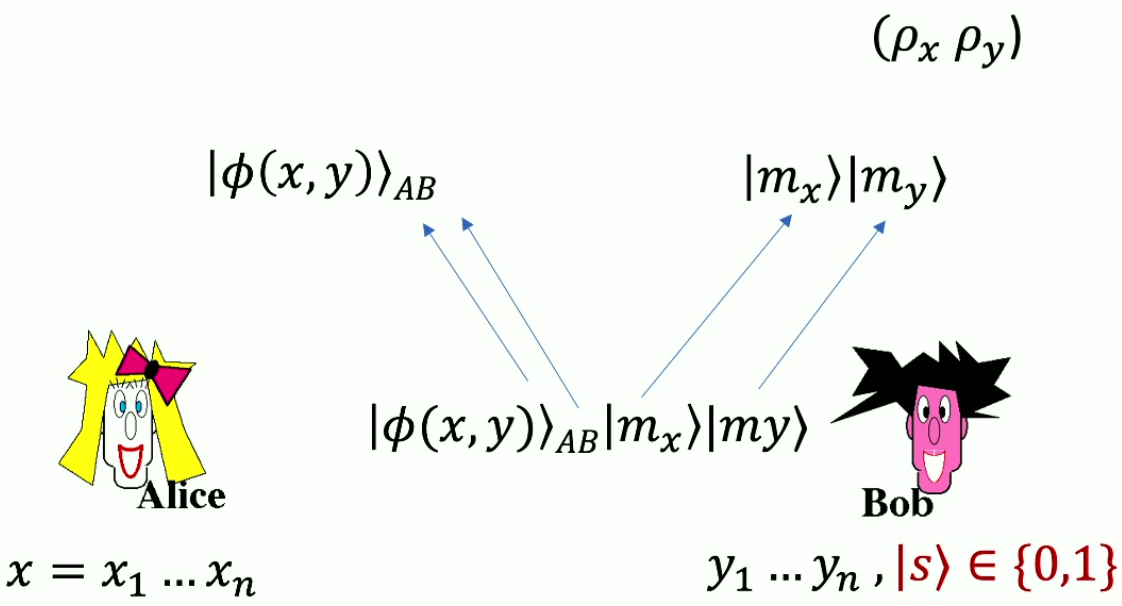
Lower bounds
- Only linear lower bounds known
- Function not in P: poly-size CDS

Quantum version of CDQS
- Classical inputs x & y
- Quantum shared state $|\phi\rangle_{AB}$
- Quantum messages $|m_x\rangle$ & $|m_y\rangle$
- Quantum secret: $|s\rangle$

CDS → CDQS ↔ f-routing

Conditional Disclosure of Secrets (CDQS)

learns $|s\rangle$ iff $f(x,y)=1$



$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

Proof CDQS → f-routing

If $f(x,y)=1$: Bob learns $|s\rangle$

- Follows from correctness QCDS

Purify the protocol

Bob:

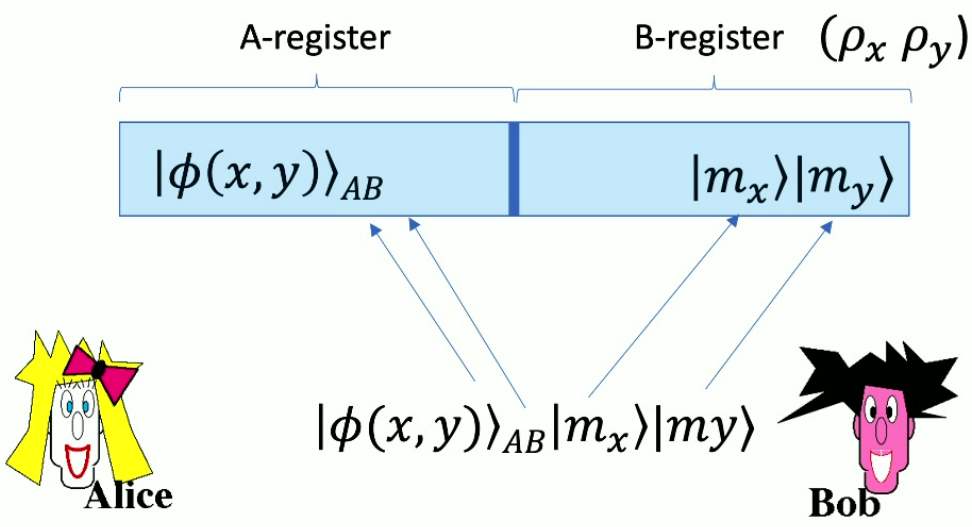
- Keeps $|m_y\rangle$register
- Send rest to Alice

Alice:

- Send $|m_x\rangle$ register to Bob
- Keeps rest

Conditional Disclosure of Secrets (CDQS)

learns $|s\rangle$ iff $f(x,y)=1$



$x = x_1 \dots x_n$

$y_1 \dots y_n$, $|s\rangle \in \{0,1\}$

$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$

Proof CDQS → f-routing

If $f(x,y)=1$: Bob learns $|s\rangle$

- Follows from correctness QCDS

If $f(x,y)=0$: Bob no info on $|s\rangle$

- Security of QCDS --> Alice extract $|s\rangle$

(THM: A reconstruct $|s\rangle$ from purified A register if no info on B register)

Purify the protocol

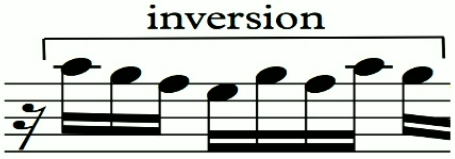
Bob:

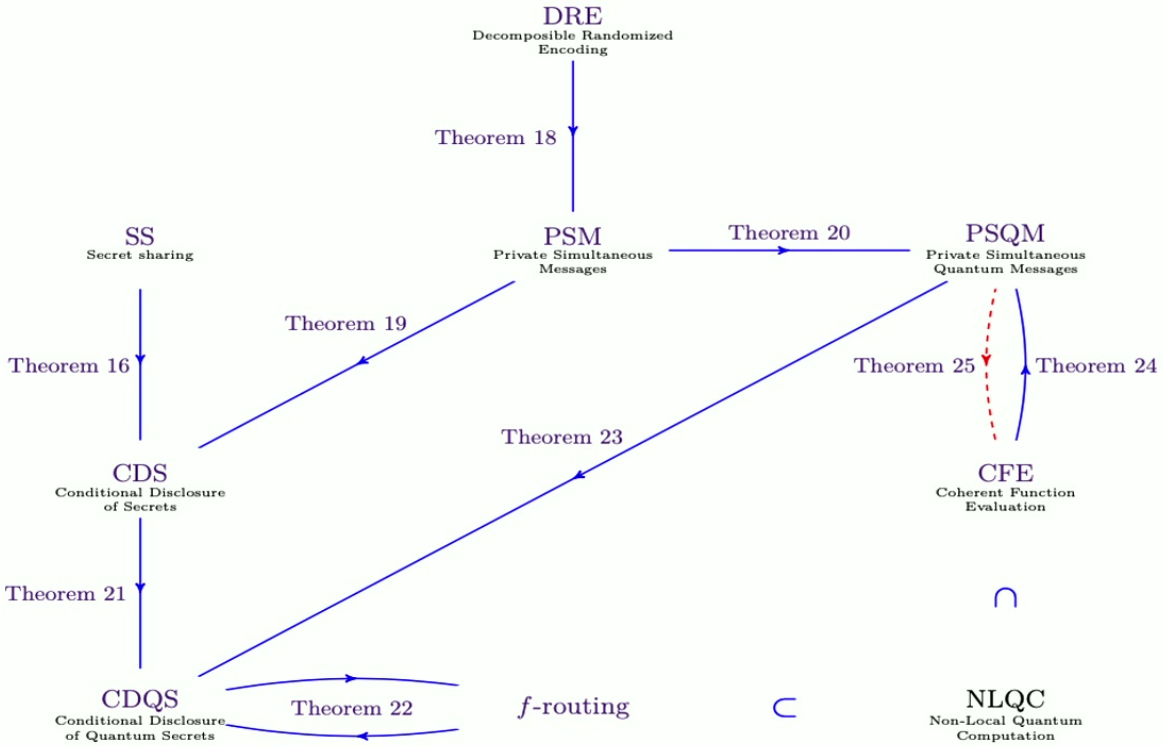
- Keeps $|m_y\rangle$register
- Send rest to Alice

Alice:

- Send $|m_x\rangle$ register to Bob
- Keeps rest

More Connections





- Protocols for Q Position Verification

Inversion 1

- Attacks: communication game

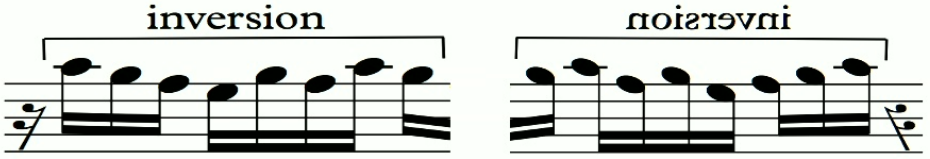
Inversion 2

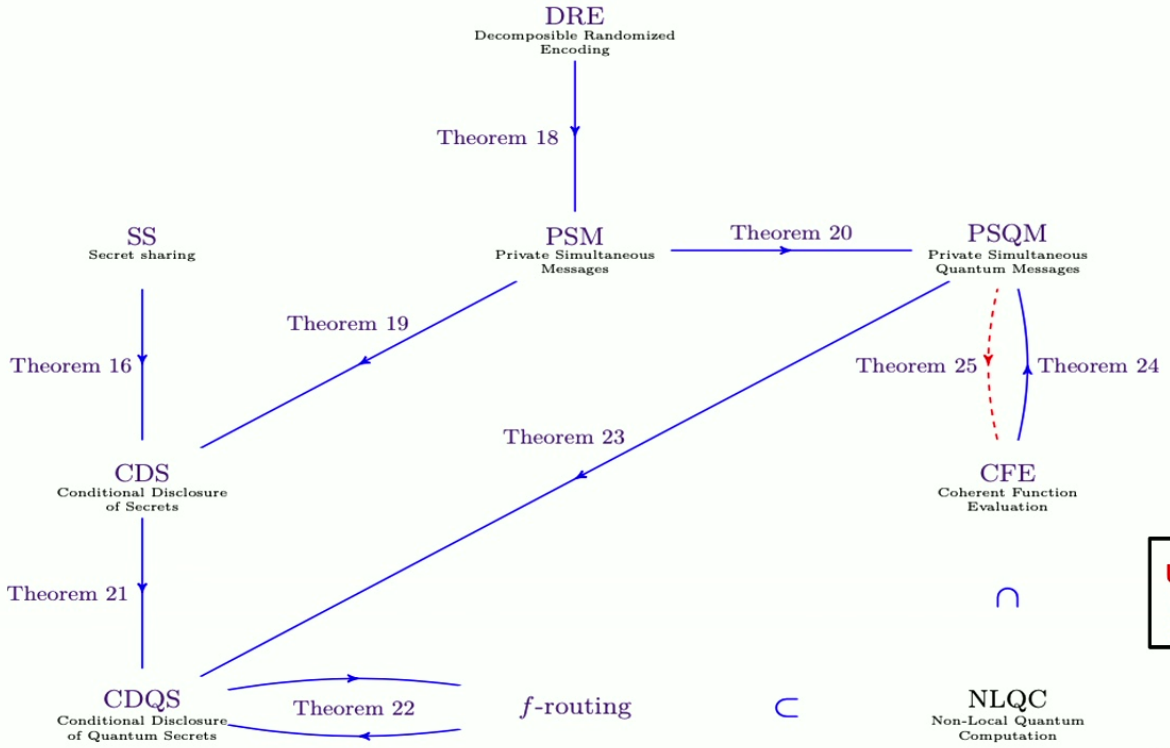
- Secure cryptographic protocols yield quantum attacks

[Allerstorfer-Buhrman-May-Speelman-Verduyn Lunel'23]

QuSoft

More Connections





- Protocols for Q Position Verification

Inversion 1

- Attacks: communication game

Inversion 2

- Secure cryptographic protocols yield quantum attacks

upper and lower bounds in complexity theory:
good upper bounds yield strong lower bounds

[Allerstorfer-Buhrman-May-Speelman-Verduyn Lunel'23]

QuSoft

Some Consequences

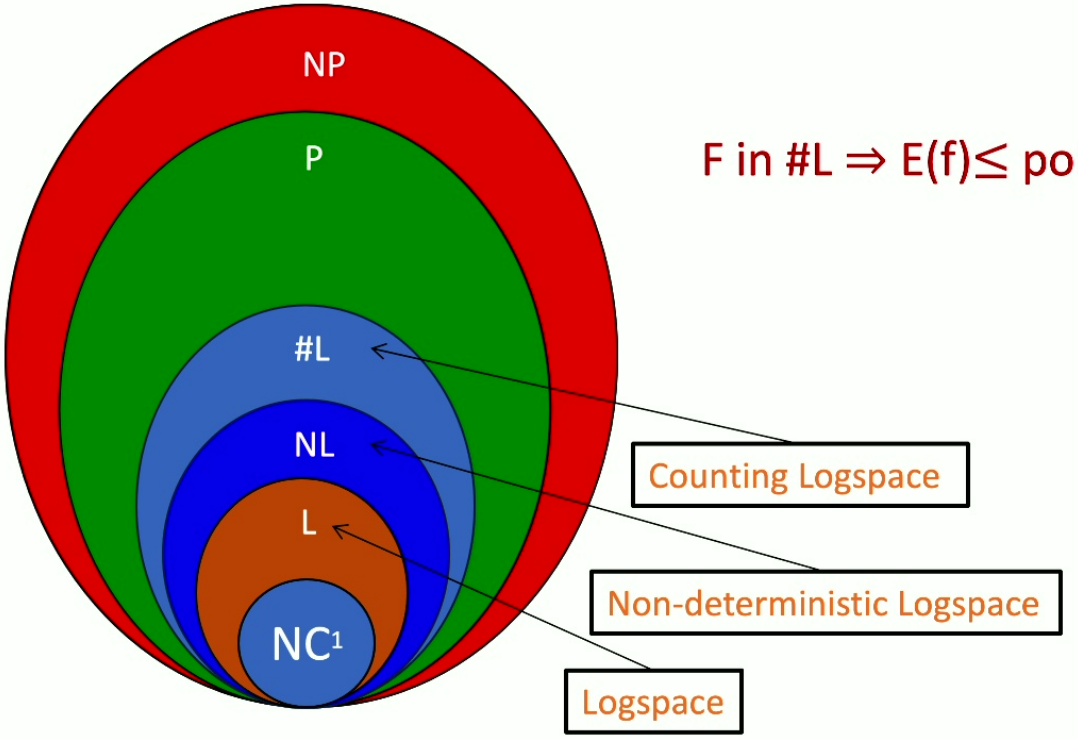
- For arbitrary f : $\mathrm{E}(\mathrm{f}) \leq 2^{n/2}$ (never need more entanglement)
- For Quadratic Residuosity (QR) exists a PSM protocol with poly communication → $E(QR) \leq p(n)$

  QR: input a , m decide if exists $b : a \equiv b^2 \bmod m$

  m is a prime: it is in P (but believed to not be in NC)

  m is composite: not known to be in P (but it is in BQP)
- f ∈ $\#L$ ⇒ E(f) ≤ $p(n)$
- Still not known whether for f ∈ P: E(f) ≤ $p(n)$ (as ADS/CFT might suggest)

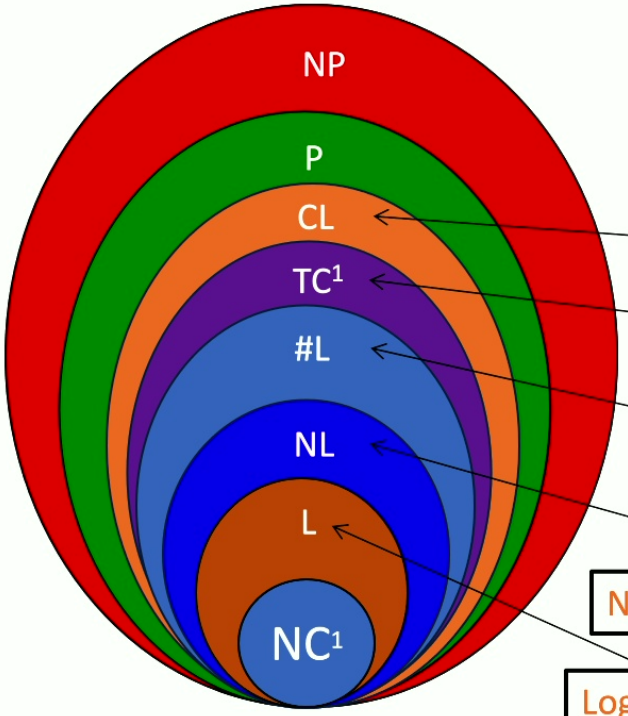
$NP = NC^1$?



F in #L ⇒ E(f)≤ polynomial

QuSoft

$NP = NC^1$?



F in #L ⇒ E(f)≤ polynomial

Catalytic Logspace

Log depth CKT with Threshold gates

Counting Logspace

Non-deterministic Logspace

Logspace

QuSoft

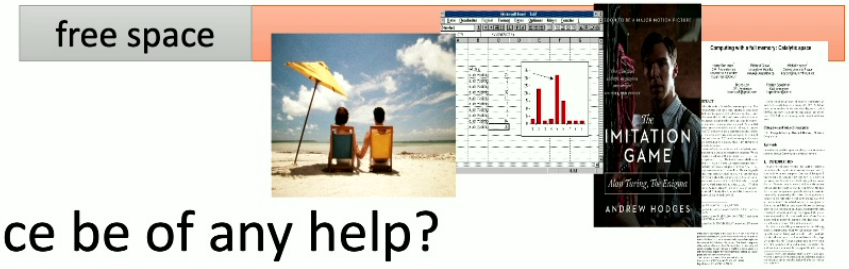
Catalytic Logspace

[Buhrman-Cleve-Coucky-Loff-Speelman,14]

Can full memory be of any use?

- Consider the following scenario:
  - You want to perform a computation, but do not have enough free space.
  - On the other hand, you **do** have a hard drive full of pictures/data/movies/etc.

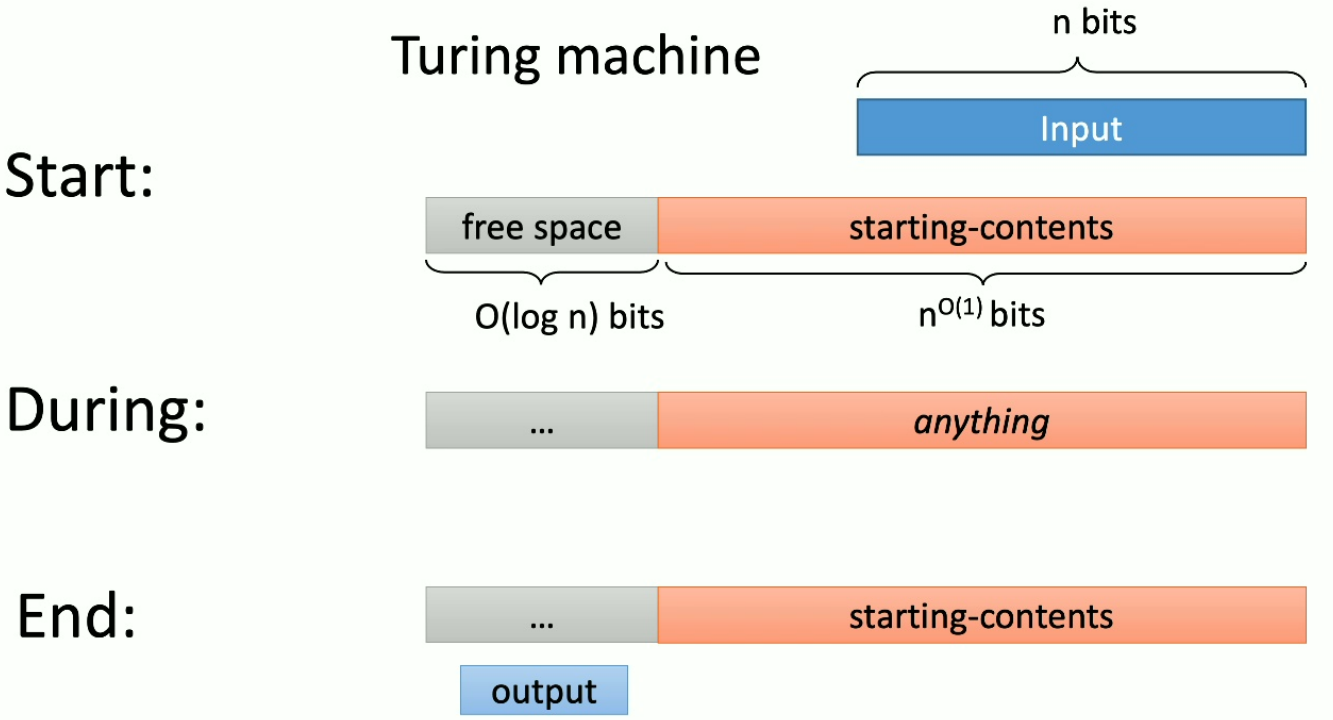
  (It's not currently in use, but you do want to keep the contents)



- Can the extra space be of any help?

Computational model

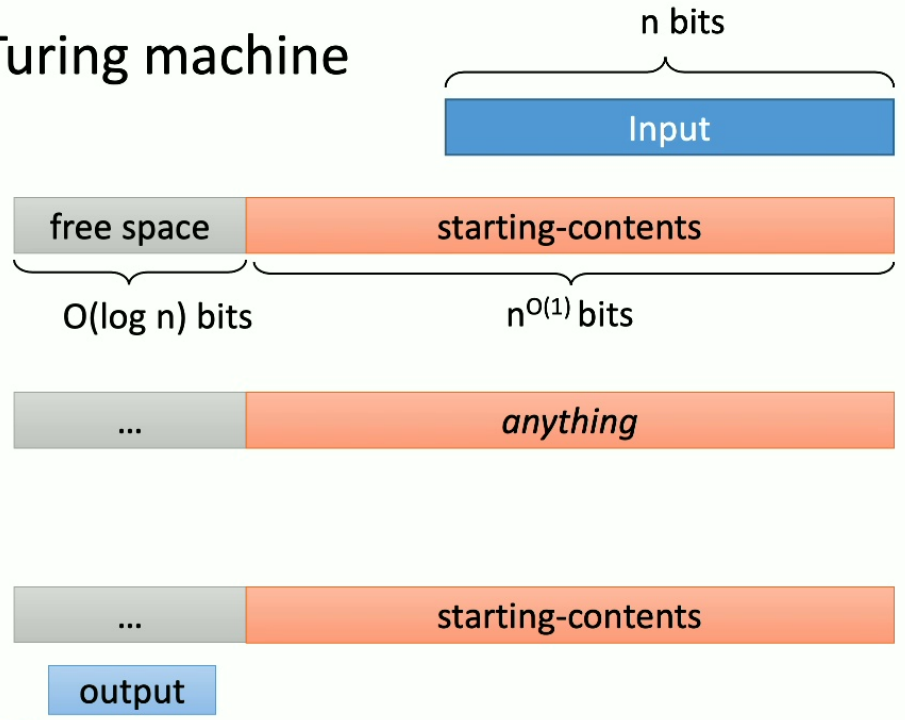
Turing machine



(has to work for *all* starting-contents!)

Computational model

Turing machine



Catalytic Space: CL

- O(log n) clean space
- $n^{O(1)}$ catalytic space

(has to work for *all* starting-contents!)

Compressing tape?

How about:

1) compress the extra/catalytic tape
2) use extra space for computation
3) copy answer into clean space
4) un-compress extra/catalytic tape

Won't work if catalytic tape is incompressible

Reversible Computation

How about:

1) make computation reversible

Reversible Computation

How about:

1) make computation reversible
2) use extra tape as normal space
3) copy answer when done
4) reverse computation until beginning

Won't work since reversible computation requires clean starting space

Is CL more powerful than Logspace?

X Y — we want to swap them

t_x t_y — easy if you have a 3^d one: Z

1) Z:= X 2) X:= Y 3) Y:= Z

Can you do it *without* extra register?

Yes!!

1) X:= Y - X \\ $t_y - t_x$

Is CL more powerful than Logspace?

X Y — we want to swap them

t_x t_y — easy if you have a 3^d one: Z

1) Z:= X 2) X:= Y 3) Y:= Z

Can you do it *without* extra register?

Yes!!

1) X:= Y - X \\ $t_y - t_x$

2) Y:= Y - X \\ $t_y - (t_y - t_x) = t_x$

3) X:= Y + X \\ $t_x + (t_y - t_x) = t_y$

Transparent Programs

filled registers: input: $f : \mathcal{R}^n \to \mathcal{R}$ Ring

$R_0\ R_1 \ldots R_m \qquad X = X_1 \ldots X_n$

$t_0\ t_1\ t_m \in \mathcal{R}$

Instructions: $R_i := R_i +/- (R_j)R_k$

$R_i := R_i +/- (R_j)X_k$

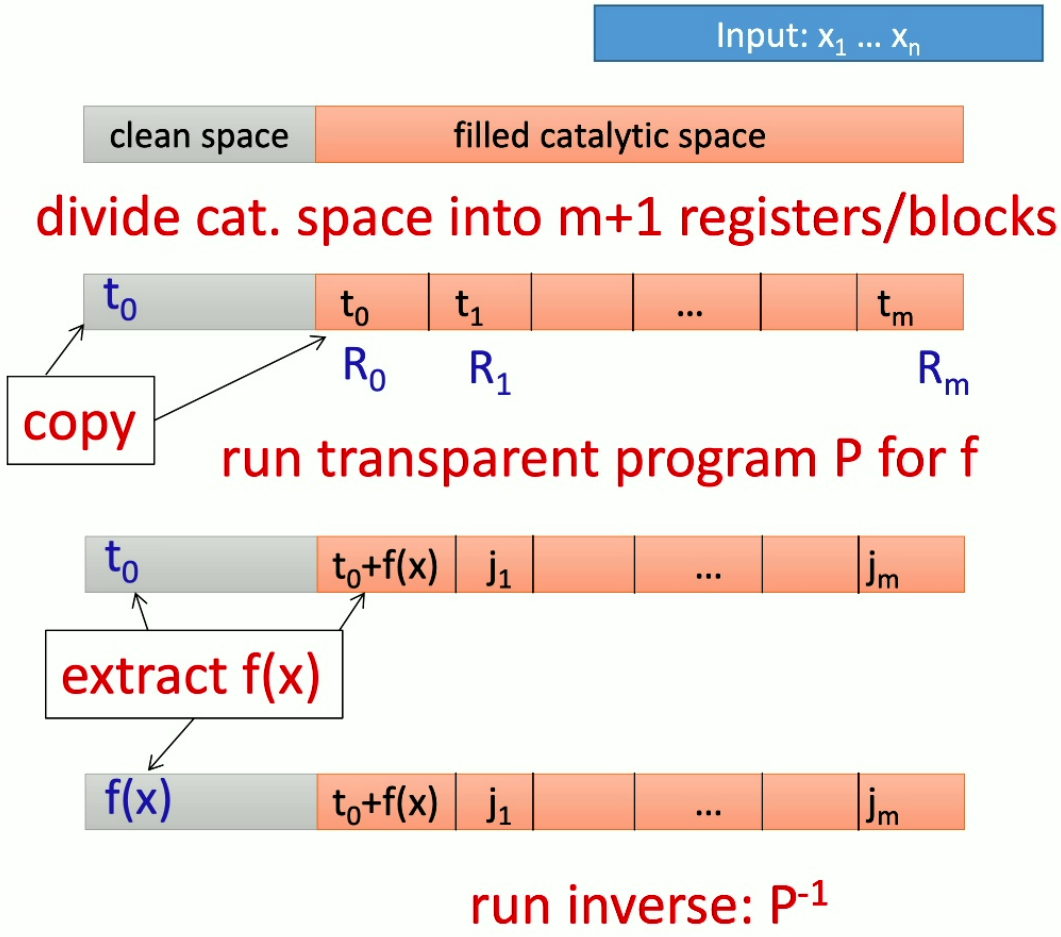
Goal: $R_0 := t_0 + f(X)$ for any initial setting of $R_0 \ldots R_m$

Note: programs are reversible:

$R_i := R_i + R_jR_k$

From Transparent Program to Catalytic Computation

use clean space
for execution
of program P
(n^c instructions)



Transparent Programs

- We show that TC^1 has Transparant Programs of poly size.
- Extend trick reminiscent of Barrington due to Ben-or-Cleve
- Use appropriate Ring & more tricks
- Catalytic Space has been used in other settings due to its has unexpected power. It helped solve a conjecture of Cook (by his son).

Catalytic Computation & QPV

- Catalytic Logspace goes beyond the known complexity classes C for which we know f $\in C \Rightarrow \mathrm{E}(\mathrm{f}) \leq$ polynomial
- Catalytic & Transparent computation have the same feel as CDS

Open Problems

- Quantum GH-compl. equivalent to E(f)?
- Good lower bounds on E(f)
  - Exist f with E(f) exponential?
- Exist $f \in P$ such that $E(f) \geq$ polynomial?
- Does $f \in CL \Rightarrow E(f) \leq$ polynomial?
- Parallel repetition, like SDP & non-locality
- Implementation: noise & precision
- Other position-based primitives?