Power and limitation of distributed quantum proofs

Harumichi Nishimura (Nagoya University)
Joint work with Atsuya Hasegawa and Srijita Kundu

Shenzhen-Nagoya Workshop on Quantum Science 2024

September 19

This talk

- 2022: Power of distributed quantum Merlin-Arthur proofs
- 2023: More distributed quantum Merlin-Arthur protocols: improvement and extension
- 2024: Power and limitation of distributed quantum proofs

<u>Keywords:</u>

- Quantum (computation)
- Distributed (network)
- Proof verification (or Merlin-Arthur proof system)

Proof verification

- P vs NP
  - P:=problems that can be computed efficiently (in poly-time)
  - NP:=problems that can be verified efficiently with the help of proofs
- Yes-No problem $A = (A_{yes}, A_{no}) \in$ NP $\Leftrightarrow \exists V$: poly-time algorithm
  - (completeness) $x \in A_{yes} \rightarrow \exists w\ [V(x, w) = 1\ (yes)]$
    - w is called a **certificate** (**proof**, witness)
  - (soundness) $x \in A_{no} \rightarrow \forall w\ [V(x, w) = 0\ (no)]$

<u>Ex: Factoring</u>

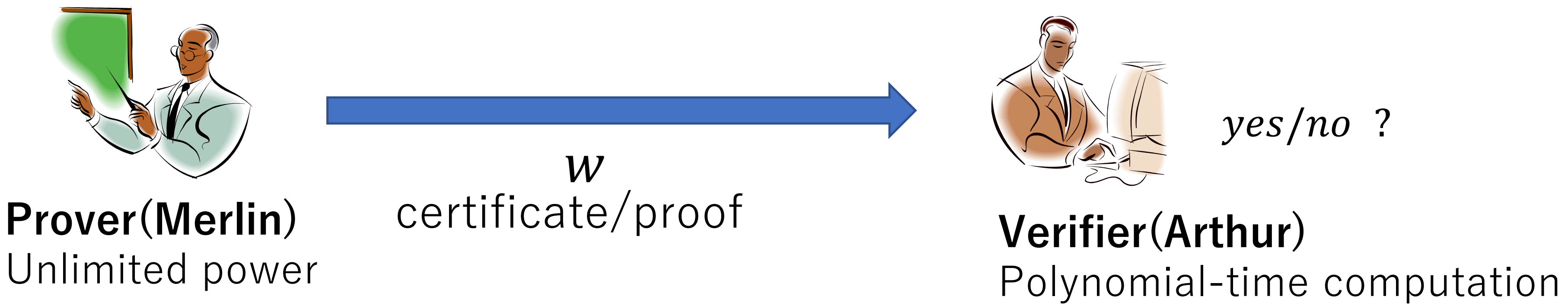
Input: positive integers N & k

Output: Yes⇔N has a non-trivial divisor smaller than k

Certificate: Any non-trivial divisor smaller than k

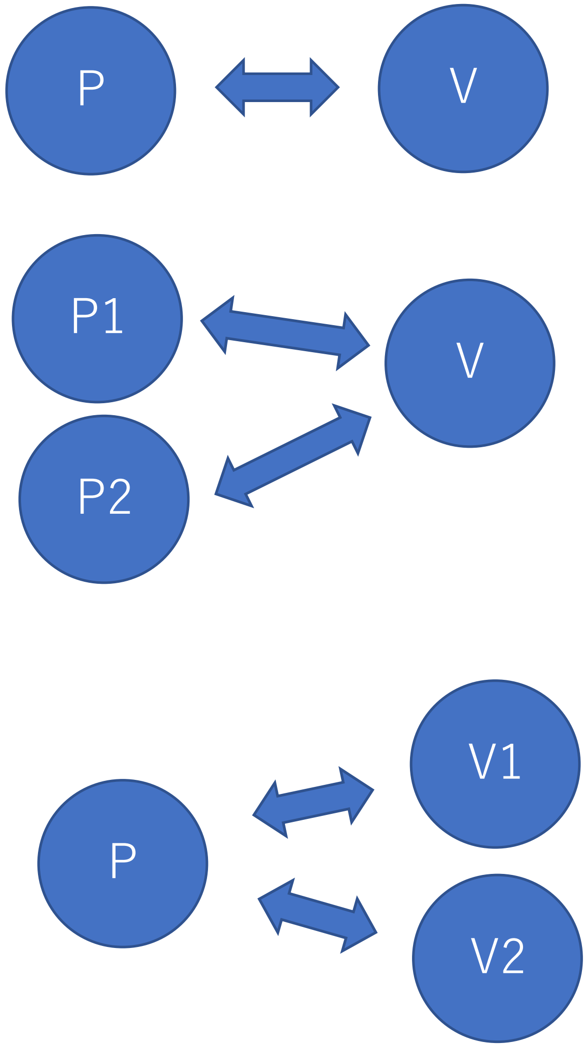
NP as communication systems

- Yes-No problem $A = \left(A_{yes}, A_{no}\right) \in$ NP $\Leftrightarrow \exists V$: poly-time algorithm
  - (completeness) $x \in A_{yes} \to \exists y\ [V(x, w) = 1\ (yes)]$
  - (soundness) $x \in A_{no} \to \forall y\ [V(x, w) = 0\ (no)]$
- Prover (Merlin): computationally unlimited
  - Sends w
- Verifier (Arthur): computationally limited (poly-time)
  - Receives w and verifies whether $V(x, w) = 1$
- MA:=Randomized version of NP; poly-time⇒randomized poly-time



Extensions of NP

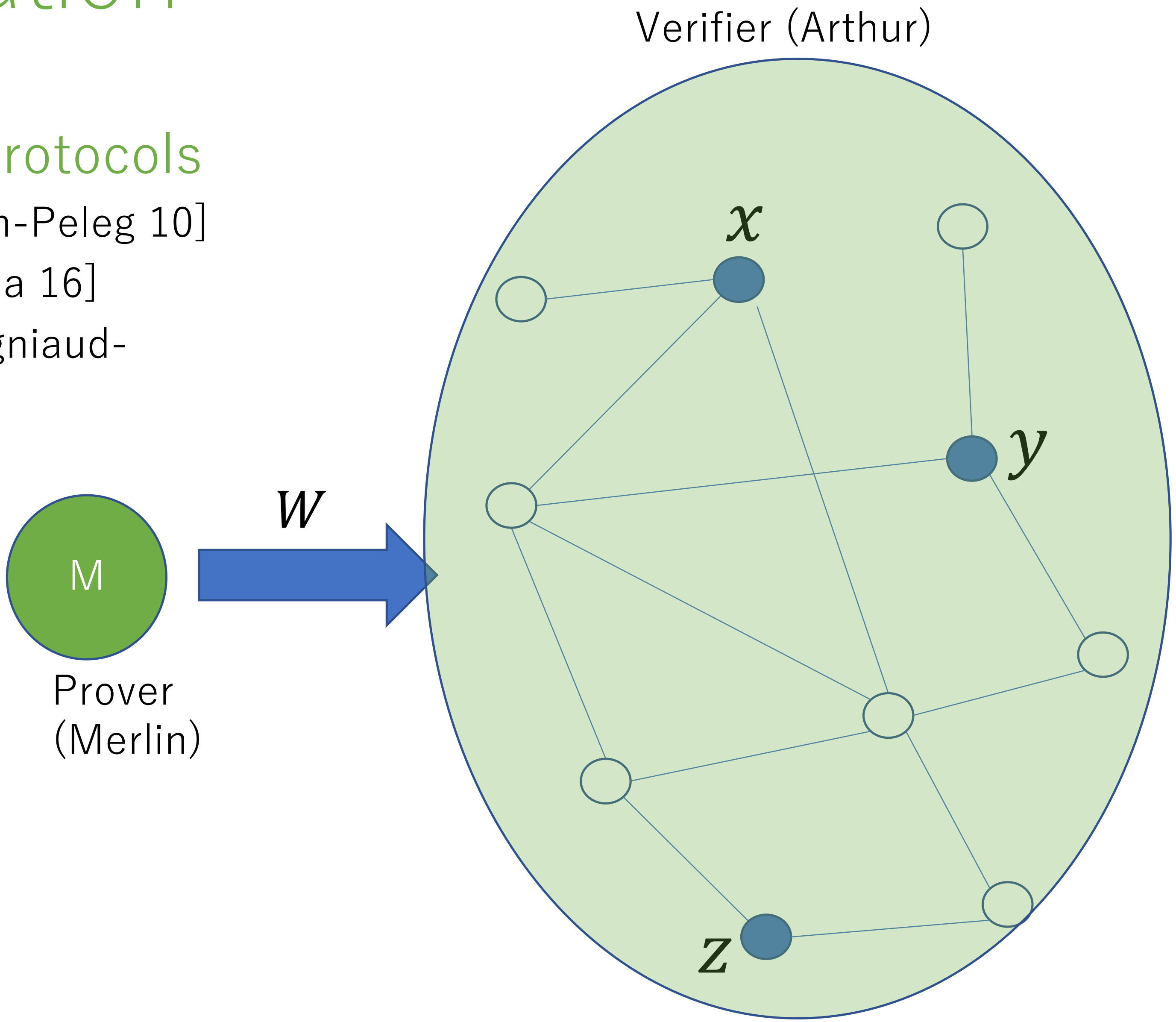
- Interactive proof
  - Prover and verifier can interact (two-way communication)
- Multi-prover interactive proof
  - Multiple provers can interact with verifier
  - Provers cannot communicate with each other
- Multi-verifier (interactive) proof
  - Verifier consisting of multiple parties can interact with prover
  - Parties can communicate with each other but the communication is expensive
  - Target in this talk



Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman-Kutten-Peleg 10]
  - Locally checkable proof [Göös-Suomela 16]
  - Nondeterministic local decision [Fraigniaud-Korman-Peleg 13]

  etc
- Input
  - Graph (structure of the network)
  - Strings for nodes (terminals)

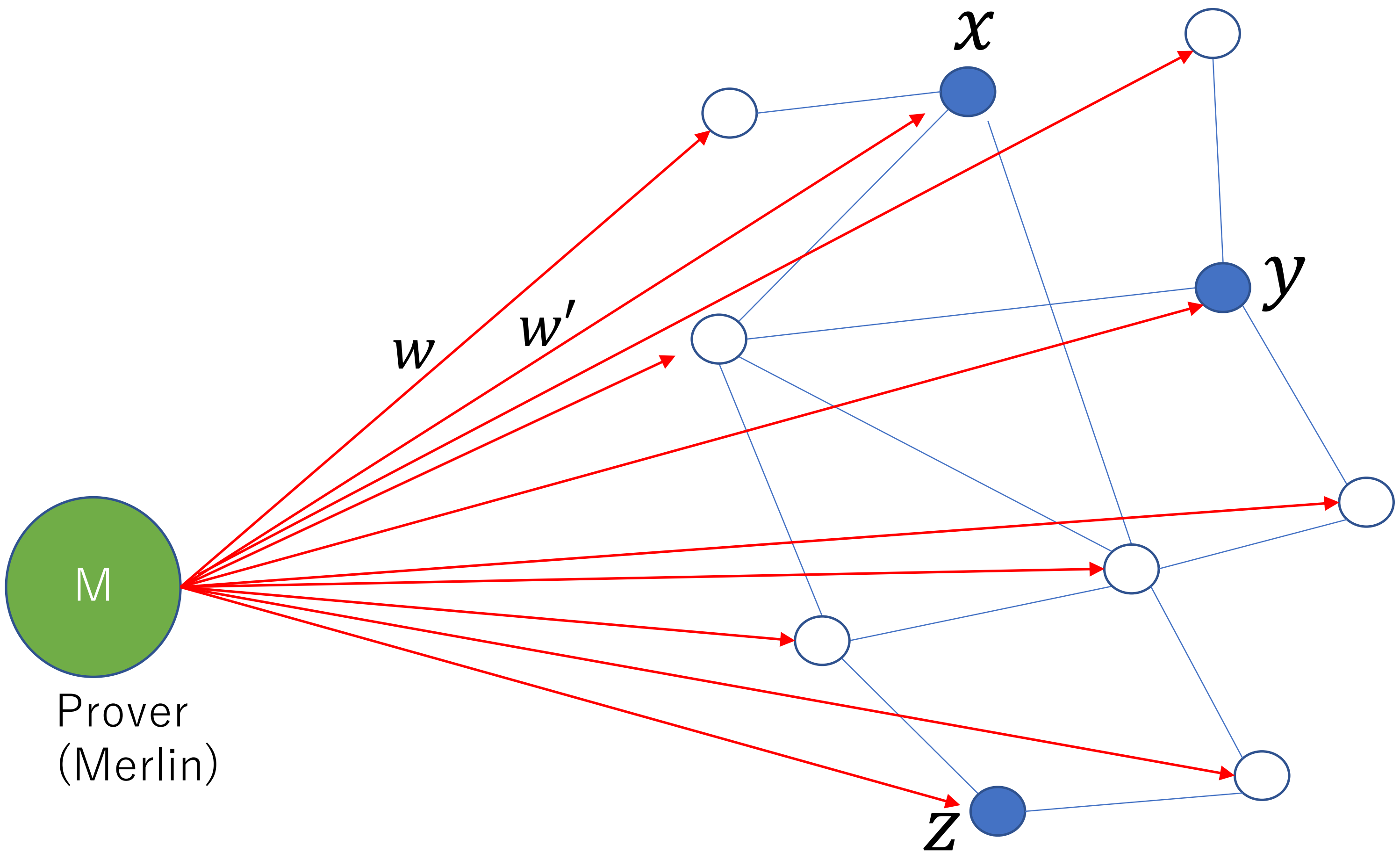


terminals (nodes who have data)

Distributed Merlin-Arthur (dMA) protocol

Two phases:

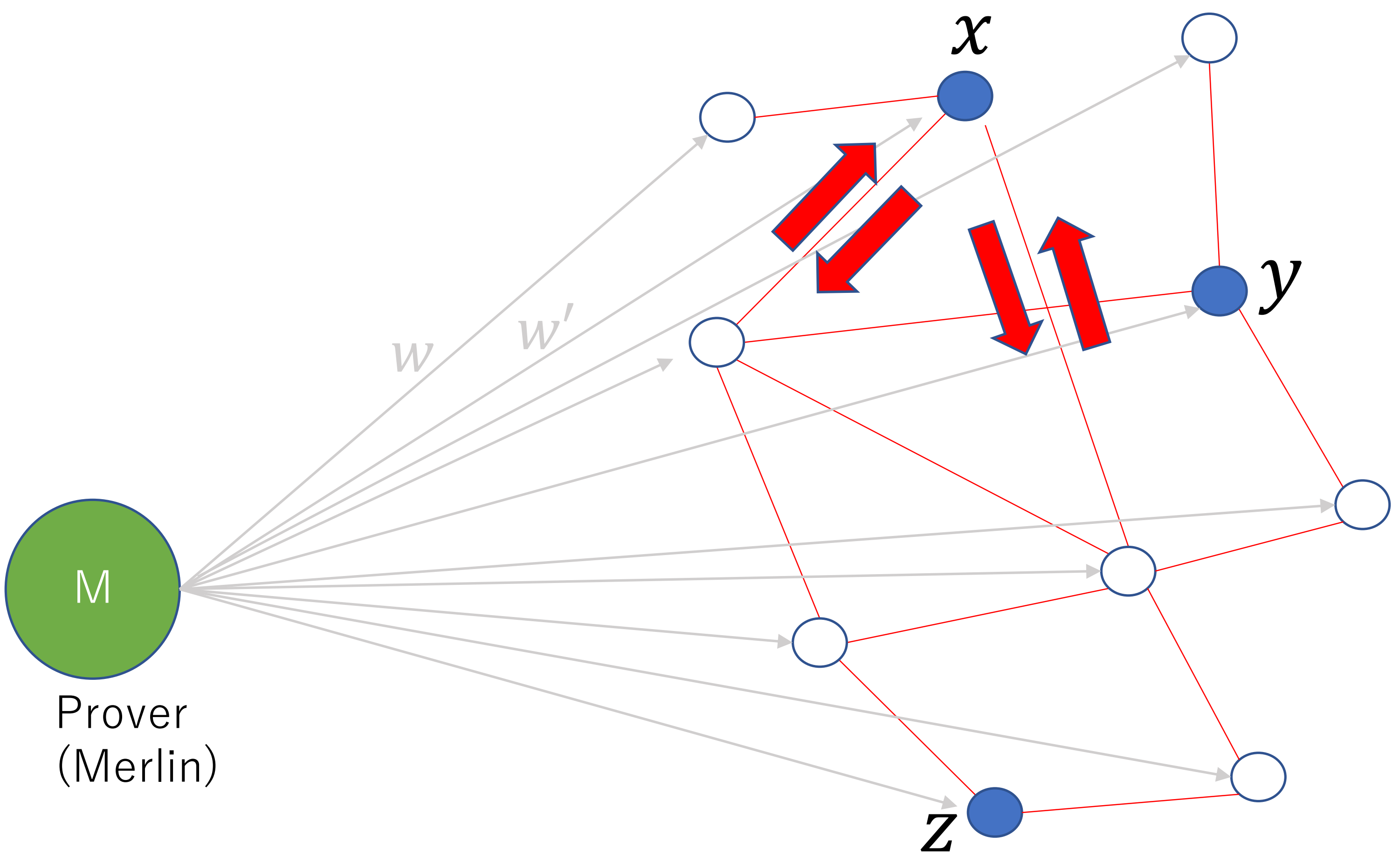
1. (Prover phase) Prover sends certificates to each node



Distributed Merlin-Arthur (dMA) protocol

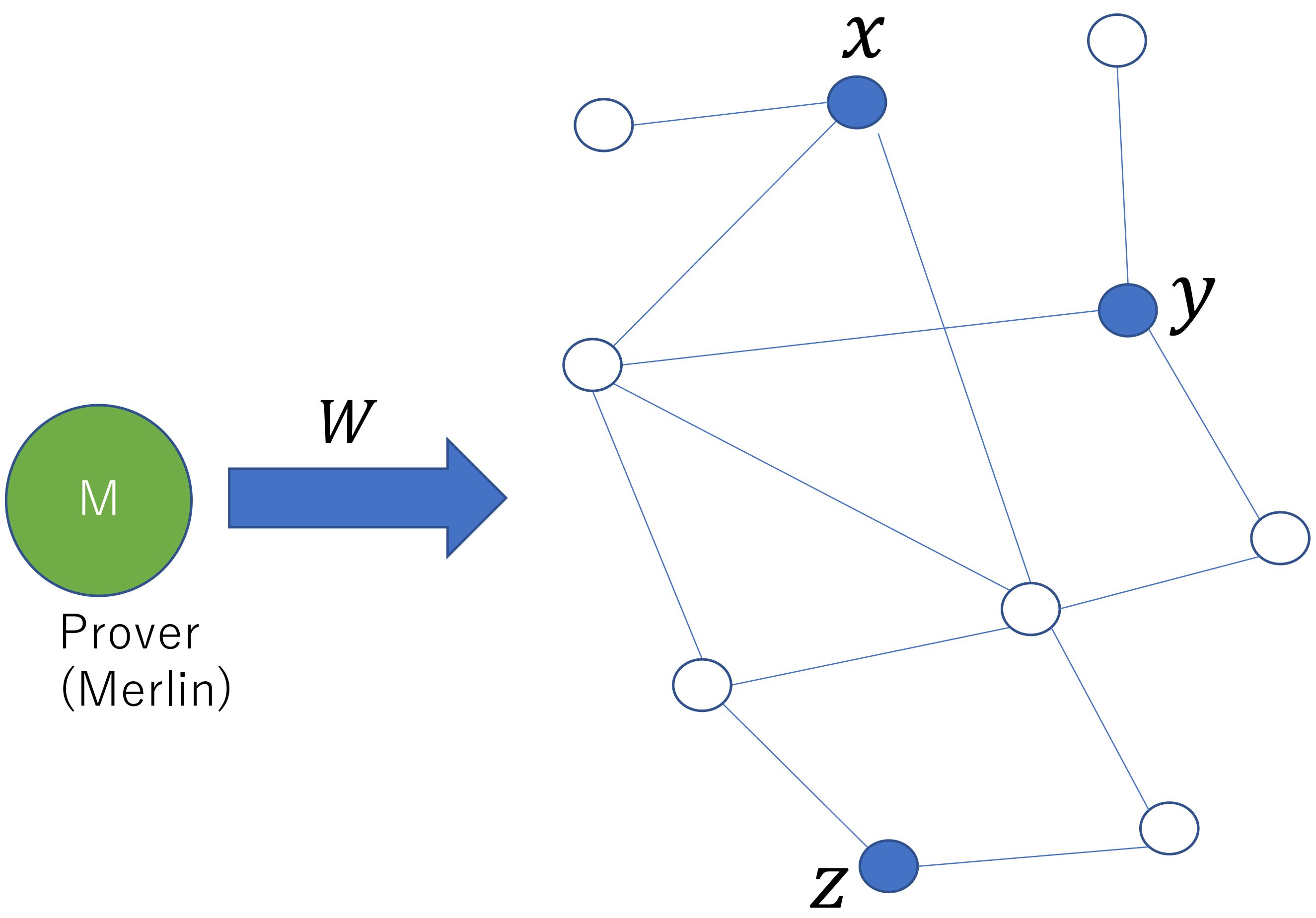
Two phases:

1. (Prover phase) Prover sends certificates to each node
2. (Verification phase) Each node exchanges messages with the neighbors



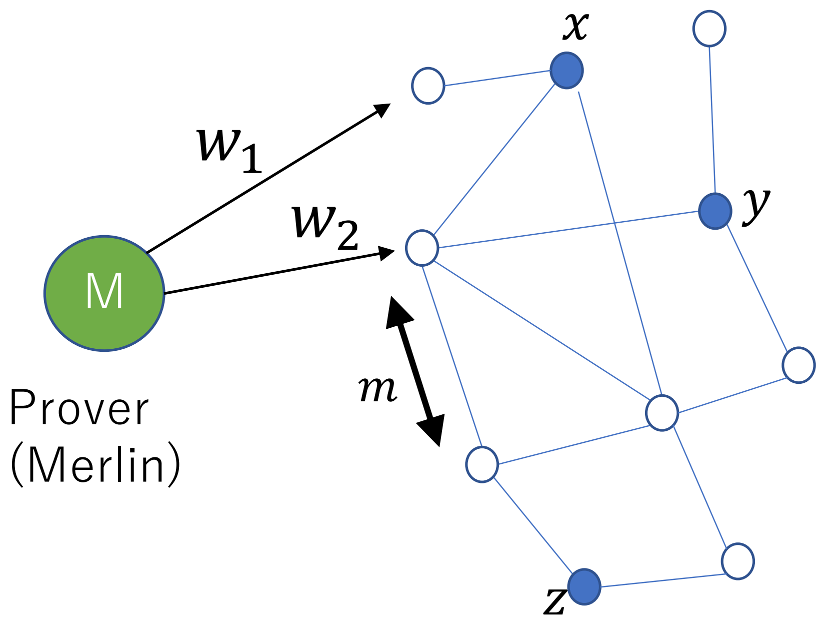
Properties of dMA

Properties:
(YES case: Completeness)
$\exists w$[all nodes accept] (w.h.p.)
(NO case: Soundness)
$\forall w$[some node rejects] (w.h.p.)



Complexity of dMA

- Efficiency of NP
  - Time (polynomial-time)
- Efficiency of dMA
  - **Communication**
    - Unlimited prover knows all information (network & terminals' inputs)
    - Verifier knows only local information
  - Prover phase: **proof** (or certificate)
  - Verification phase: **messages among neighbors**
  - **Local proof (message) size**:=maximum of the number of bits of proofs (messages) sent to nodes (sent between neighbors)
  - **Total proof (message) size**:=sum of the number of bits of proofs (messages) sent to nodes (sent between neighbors)

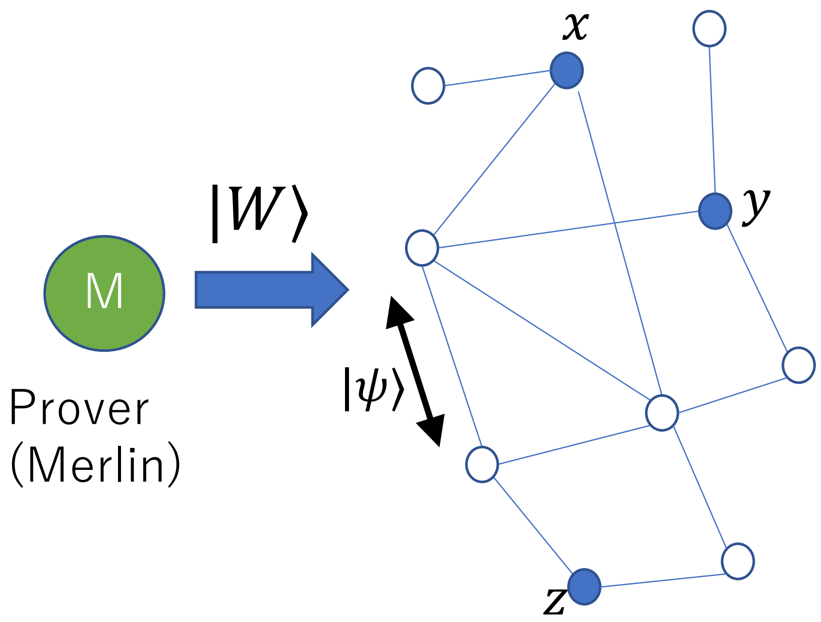


Distributed Quantum Merlin-Arthur (dQMA)

[FLNP21]

- Distributed Quantum Merlin-Arthur (dQMA) protocols on the network
  - Quantum certificates from the prover
  - Quantum messages among nodes

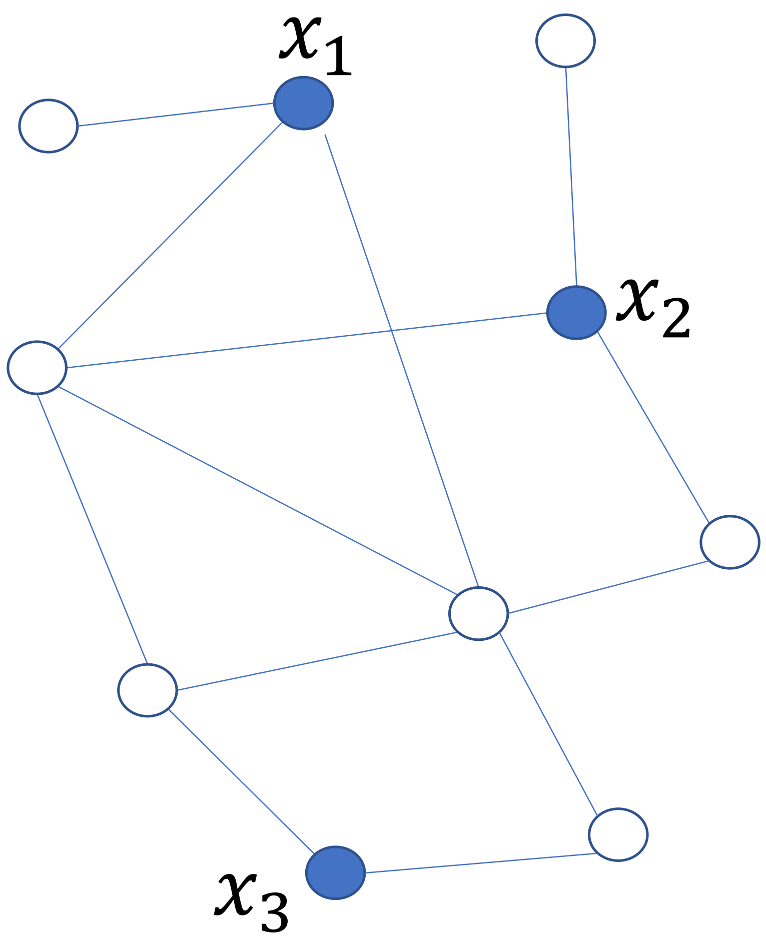
Q. Which problems are efficient for dQMA protocols?



[FLNP21] P. Fraigniaud, F. Le Gall, HN, A. Paz, Proc. ITCS21, arXiv:2002.10018

EQ: Equality of Data

- Replicated data on a network
- Are all data identical?
- $\mathrm{EQ}(x_1, \cdots, x_t) = 1 \Leftrightarrow x_1 = \cdots = x_t$
  - jth terminal has $x_j \in \{0,1\}^n$

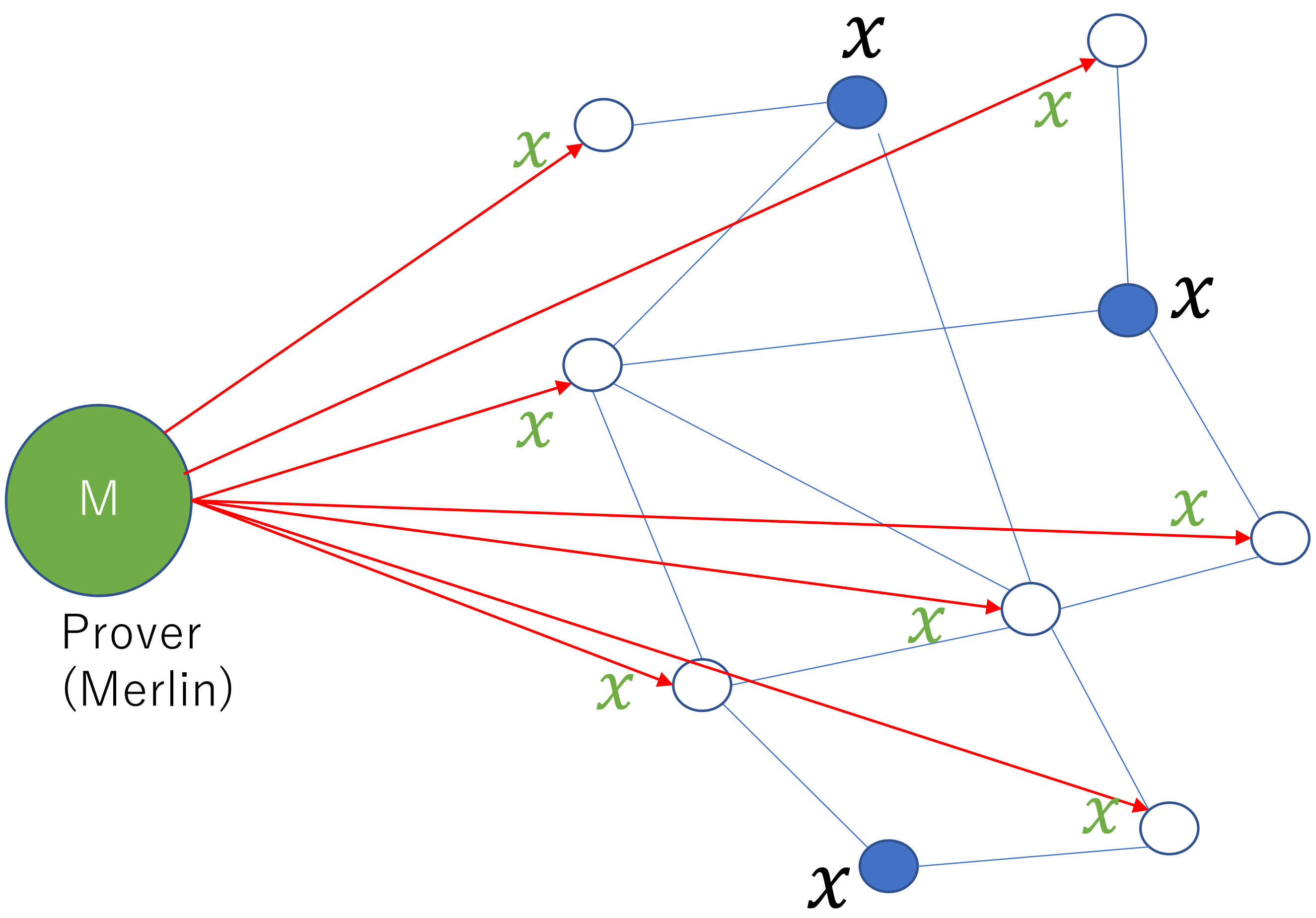


terminals (nodes who have data)

dMA Protocol for EQ

Trivial protocol:
(P) Prover M sends x to intermediate nodes when all data are x
(V) Each node checks if it is same as the neighbor's ones

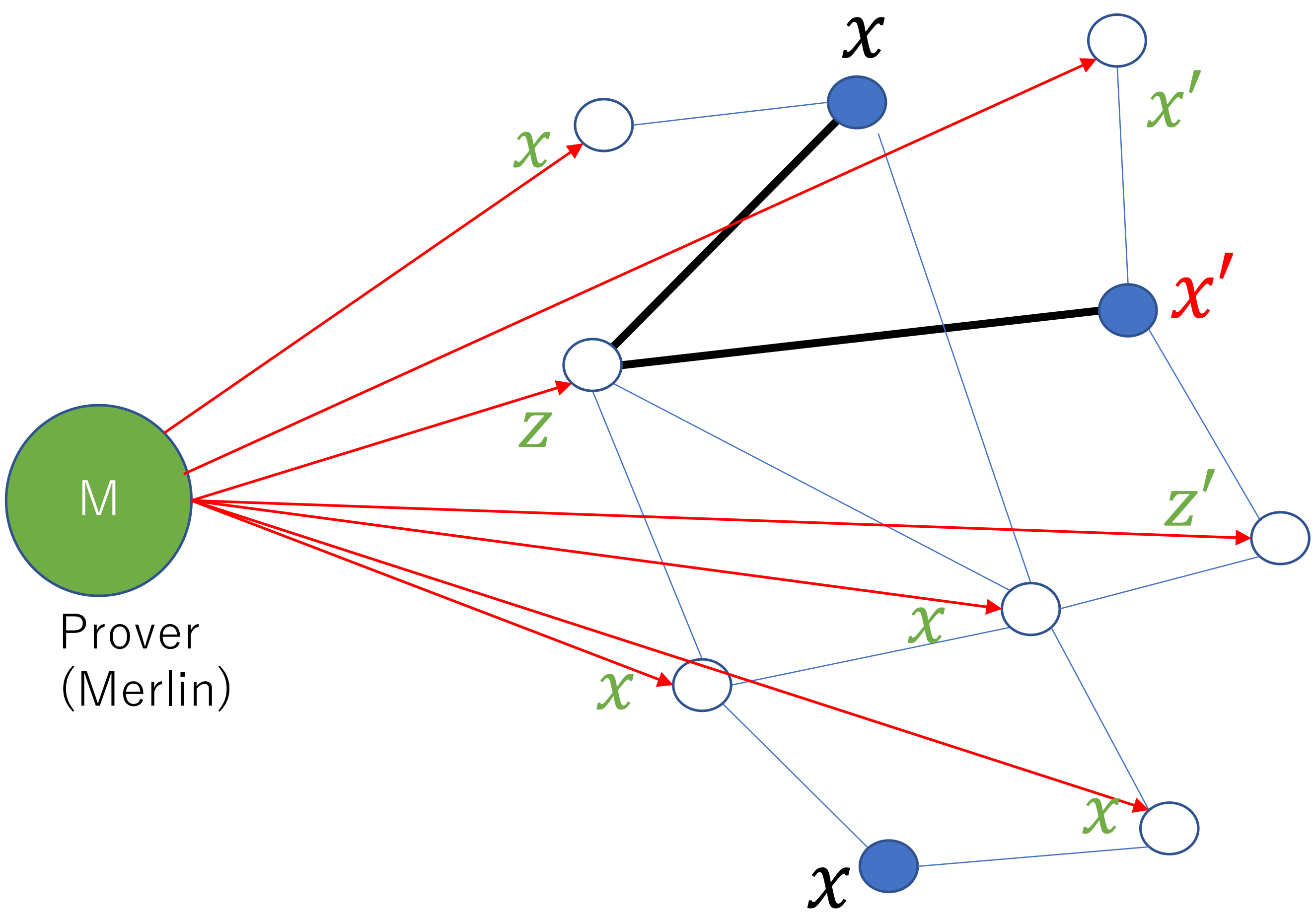
(YES case: Completeness)
$\exists W$[all nodes accept]



dMA Protocol for EQ

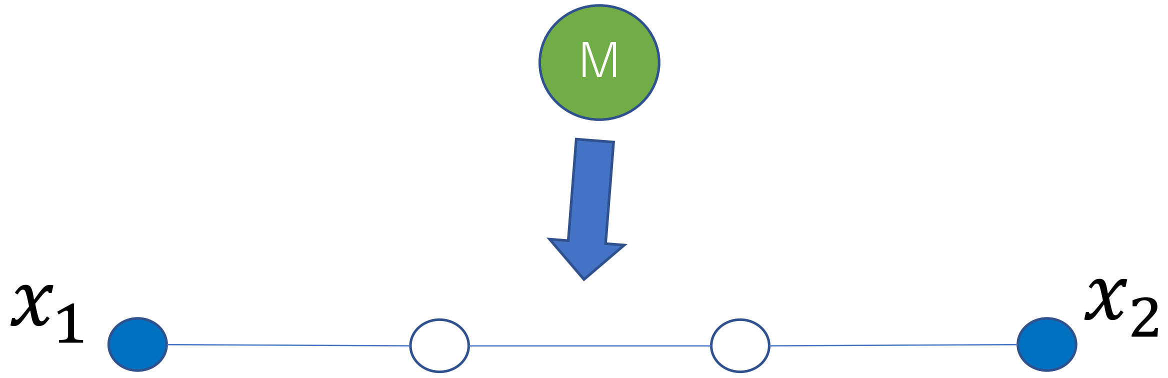
Trivial protocol:
(P) Prover M sends x to intermediate nodes when all data are x
(V) Each node checks if it is same as the neighbor's ones

(NO case: Soundness)
$\forall w$[some node rejects]



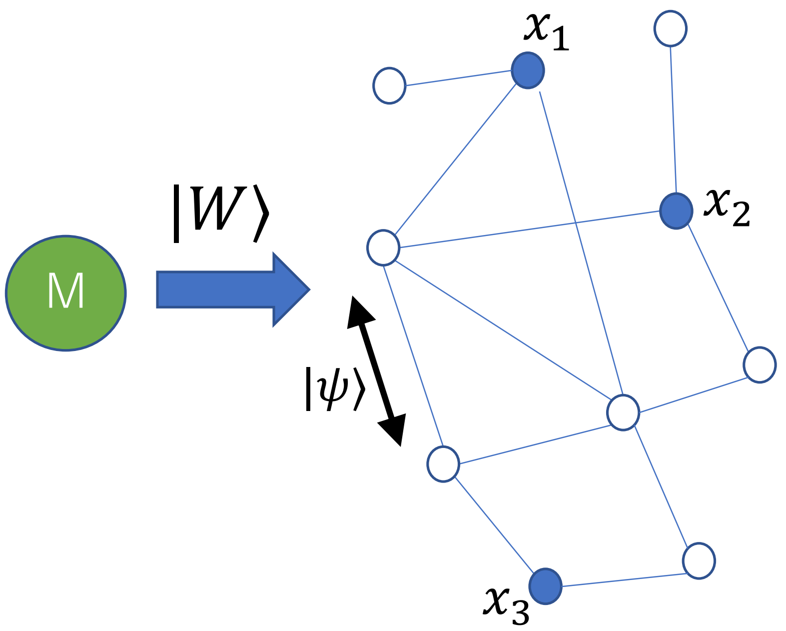
Results for EQ [FLNP21]

- Distributed Quantum Merlin-Arthur (dQMA) protocols on the network
  - Quantum certificates from the prover
  - Quantum messages among nodes
- Classical lower bound for EQ
  - Any dMA protocol requires local proof size $\Omega(n)$ (i.e., $\Omega(n)$-bit certificates to some node) when the error probability is reasonably small (say, 1/4)



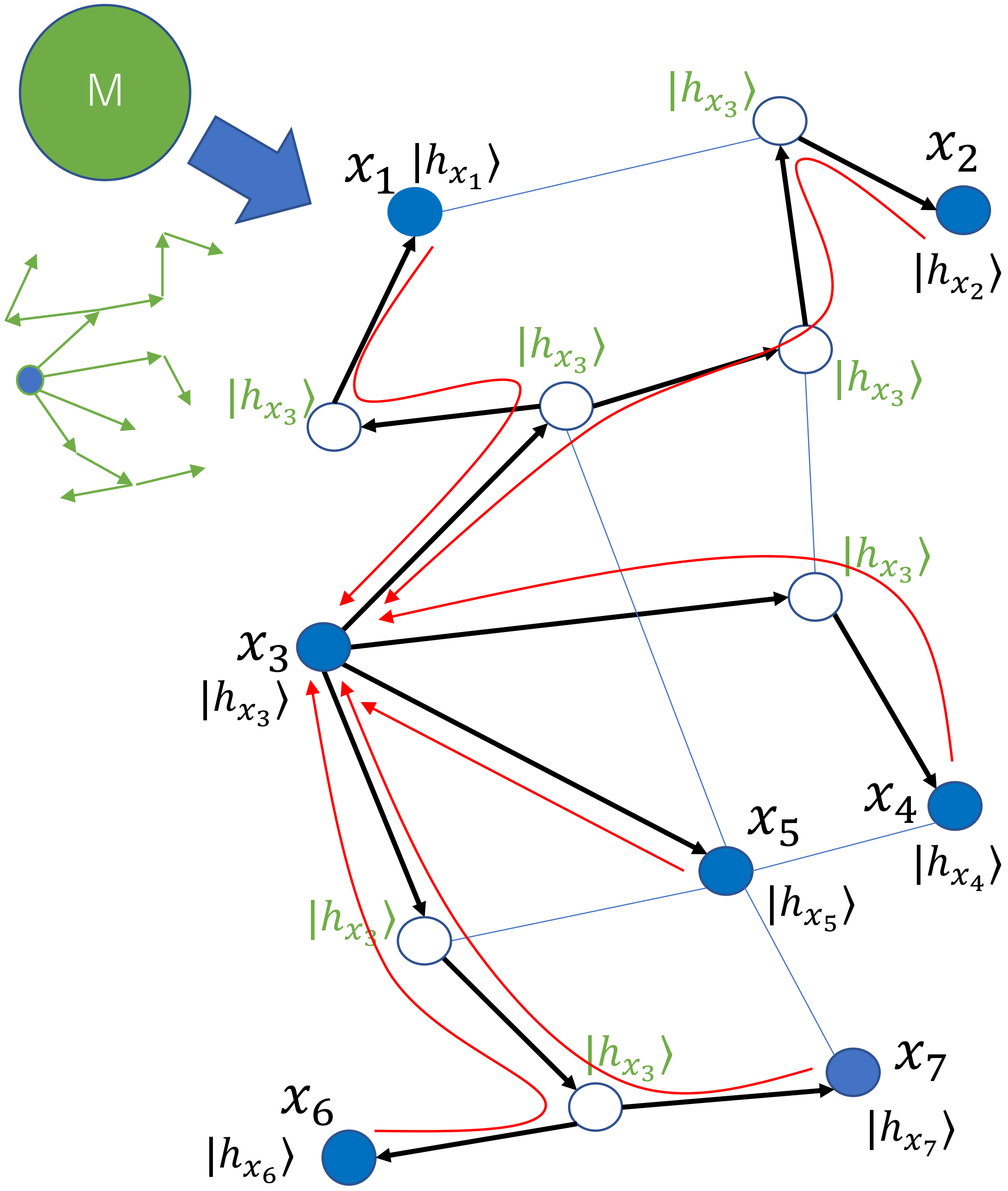
Results for EQ [FLNP21]

- Distributed Quantum Merlin-Arthur (dQMA) protocols on the network
  - Quantum certificates from the prover
  - Quantum messages among nodes
- Classical lower bound for EQ
  - Any dMA protocol requires local proof size $\Omega(n)$ when the error probability is reasonably small (say, 1/4)
- Quantum upper bound for EQ
  - ∃ dQMA protocol for EQ with local proof size & message size $O(tr^2 \log n)$
    - t:= number of the terminals (= nodes who have data)
    - r := diameter of the network
    - **t and r are typically much smaller than n**



Results for EQ [FLNP21]

- Quantum upper bound for EQ
  - ∃ dQMA protocol for EQ with local proof size & message size $O(tr^2 \log n)$
    - t:= number of the terminals (= nodes who have data)
    - r ≔ diameter of the network
    - **t and r are typically much smaller than n**
  - Proof strategy
    - Prover sends quantum fingerprint of the data to intermediate nodes
    - Verifier does quantum fingerprint check (by SWAP test) in the line network (sound for entangled proofs)
    - Verifier checks a spanning tree sent from the prover [Korman-Kutten-Peleg 10]



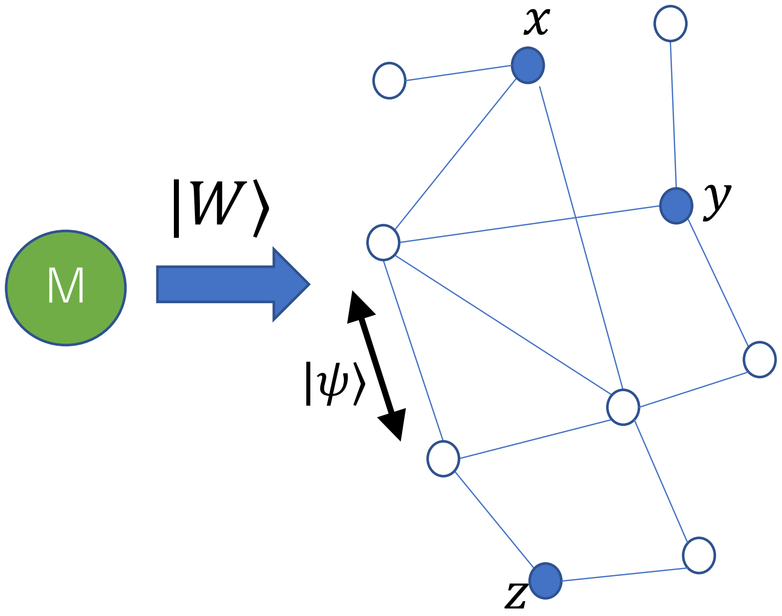
Follow-up work

- Distributed quantum interactive proofs [LMN23-1]
  - Verifier (network) can interact with prover (Merlin)
- Distributed quantum state synthesis [LMN23-2]
  - Yes-No problems ⇒ generation of quantum states
  - Application: dQMA proof systems for Set-Equality

[LMN23-1] F. Le Gall, M. Miyamoto, HN, Proc. STACS23, arXiv: 2210.01390
[LMN23-2] F. Le Gall, M. Miyamoto, HN, Proc. MFCS23, arXiv: 2210.01389

Questions

- More problems
  - EQ
  - Set Equality
  - ???
- Quantum lower bound
  - Proof size
  - Message size



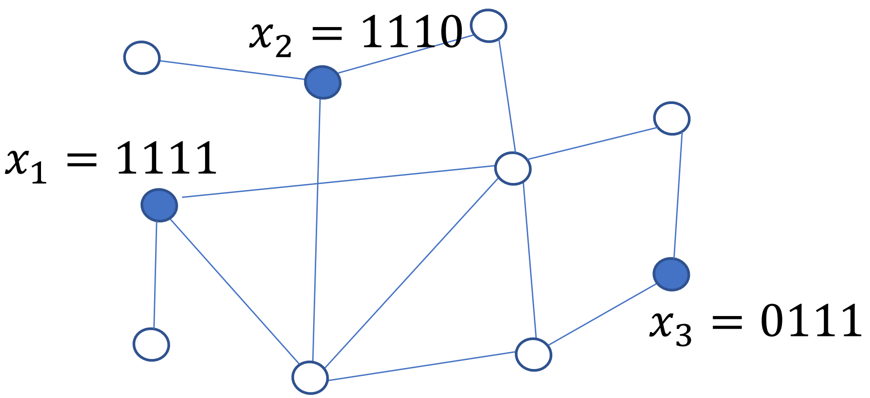
Our results [HKN24]

- More problems can be verified in dQMA proof systems
  - Hamming distance
  - Ranking verification
- First quantum lower bounds
  - Proof size + message size

[HKN24] A. Hasegawa, S. Kundu, HN, Proc. PODC24, arXiv:2403.14108

$HAM_1(x_1, x_2, x_3) = 0$
$HAM_2(x_1, x_2, x_3) = 1$

Hamming distance



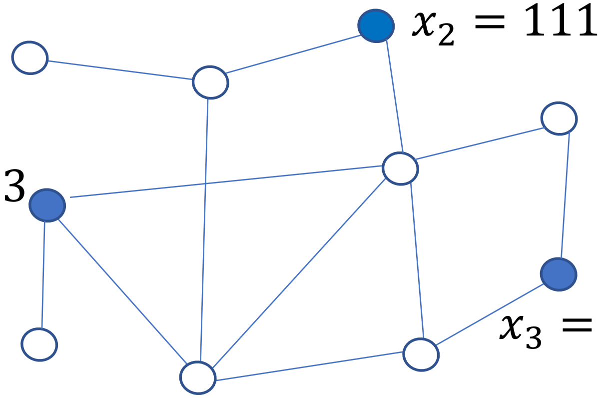
- Natural extension of EQ
- $\mathrm{EQ}(x_1, \cdots, x_t) = 1 \Leftrightarrow x_1 = \cdots = x_t$
- $HAM_d(x_1, \cdots, x_t) = 1 \Leftrightarrow \forall i, j[HD(x_i, x_j) \leq d]$
  - $HD(x, y)$:=Hamming distance between x and y

[FLNP21] Efficient dQMA protocol <u>in the line network</u> for constant d

[Theorem] There is a dQMA protocol for HAM_d for constant d such that local proof (message) size is $\tilde{O}(t^2 r^2 (\log n)^2)$ <u>in general networks</u>

- t:= number of the terminals (= nodes who have data)
- r := diameter of the network

Ranking verification



- Ranking: Generalization of maximum
  - $Rank_t^j(x_1, x_2, \cdots, x_t) :=$ j-th largest value in the list $x_1, x_2, \cdots, x_t$
  - $x_j \in \{0,1\}^n \cong \{0,1,\cdots,2^n - 1\}$: n-bit integer
- Ranking verification
  - $RV_t^{i,j}(x_1, x_2, \cdots, x_t) := 1 \Leftrightarrow x_i$ is the j-th largest value in the list
  - $RV_t^{i,1}(x_1, x_2, \cdots, x_t) = 1 \Leftrightarrow x_i$ is the largest value in the list

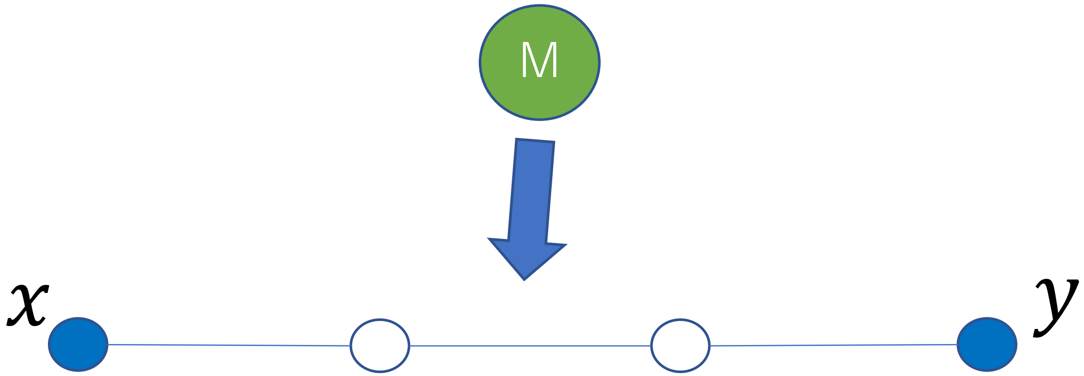
[Theorem] There is a dQMA protocol for $RV_t^{i,j}$ such that local proof (message) size is $O(tr^2 \log n)$ in a general network

Quantum lower bound

- We show lower bounds on the total proof & message size in the line network (where the both end nodes are the terminals)

[Theorem] The total proof & message size of any dQMA protocol for EQ is $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ where $\varepsilon > 0$ is any small constant (for any length r of the line network)

- $\Omega((\log n)^{\frac{1}{2}-\varepsilon})$ when the length of the line is a constant
- $O(r^3 \log n)$ [FLNP21]: Upper bound on total proof & message size



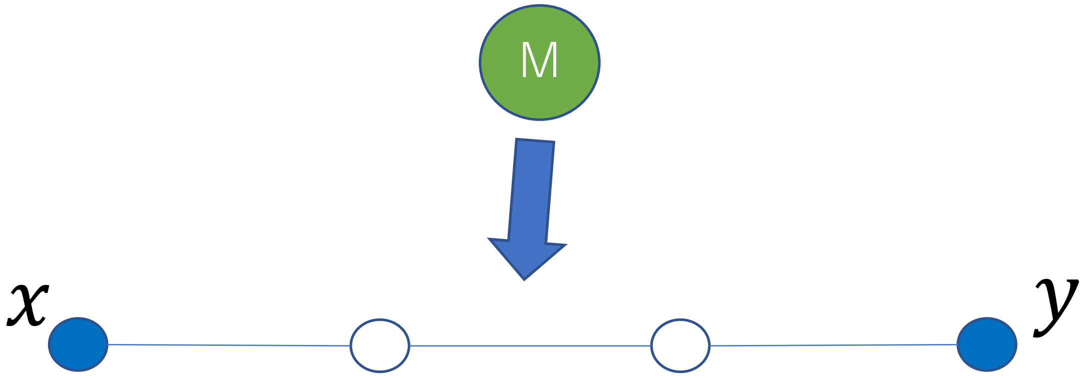
Quantum lower bound

- We show lower bounds on the total proof & message size in the line network (where the both end nodes are the terminals)

[Theorem] The total proof & message size of any dQMA protocol for EQ is $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ where $\varepsilon > 0$ is any small constant (for any length of the line network)

[Theorem] The total proof & message size of any dQMA protocol for DISJ is $\Omega(n^{1/3})$

[Theorem] The total proof & message size of any dQMA protocol for IP is $\Omega(n^{1/2})$



Our results [HKN24]

- More problems can be verified in dQMA proof systems
  - Hamming distance
  - Ranking verification
- First quantum lower bounds
  - Proof size + message size (EQ, DISJ, IP)
- Improvement over [FLNP21]
  - Local proof (message) size for EQ: $O(tr^2 \log n) \Rightarrow O(r^2 \log n)$
    - t:= number of the terminals (= nodes who have data)
    - r ≔ diameter of the network
  - Permutation test & rigidity
- Quantum advantage for EQ on the line network even if the length is large compared to input length of EQ
  - Total proof size: classical $\Omega(rn)$; quantum $\tilde{O}(rn^{2/3})$
    - r:= length of the line (=diameter of the line)

[HKN24] A. Hasegawa, S. Kundu, HN, Proc. PODC24, arXiv:2403.14108

Proof ideas

- Ranking verification
- Lower bound for EQ

Ranking verification

- Ranking verification
  - $RV_t^{i,j}(x_1, x_2, \cdots, x_t) \coloneqq 1 \Leftrightarrow x_i$ is the j-th largest value in the list
  - $RV_t^{i,1}(x_1, x_2, \cdots, x_t) = 1 \Leftrightarrow x_i$ is the largest value in the list

[Theorem] There is a dQMA protocol for $RV_t^{i,j}$ such that local proof (message) size is $O(tr^2 \log n)$

- Proof strategy:
  1. Creates a dQMA protocol for the **Greater-Than (GT) function** in the line network
  - $GT(x, y) = \begin{cases} 1 & (x > y) \\ 0 & (x \leq y) \end{cases}$
  - Reduces GT to EQ
    - $GT(x, y) = 1 \Leftrightarrow \exists j\, [x_j = 1 \,\&\, y_j = 0 \,\&\, x_1 \cdots x_{j-1} = y_1 \cdots y_{j-1}]$

      Ex: $x = 101011,\ y = 101001$

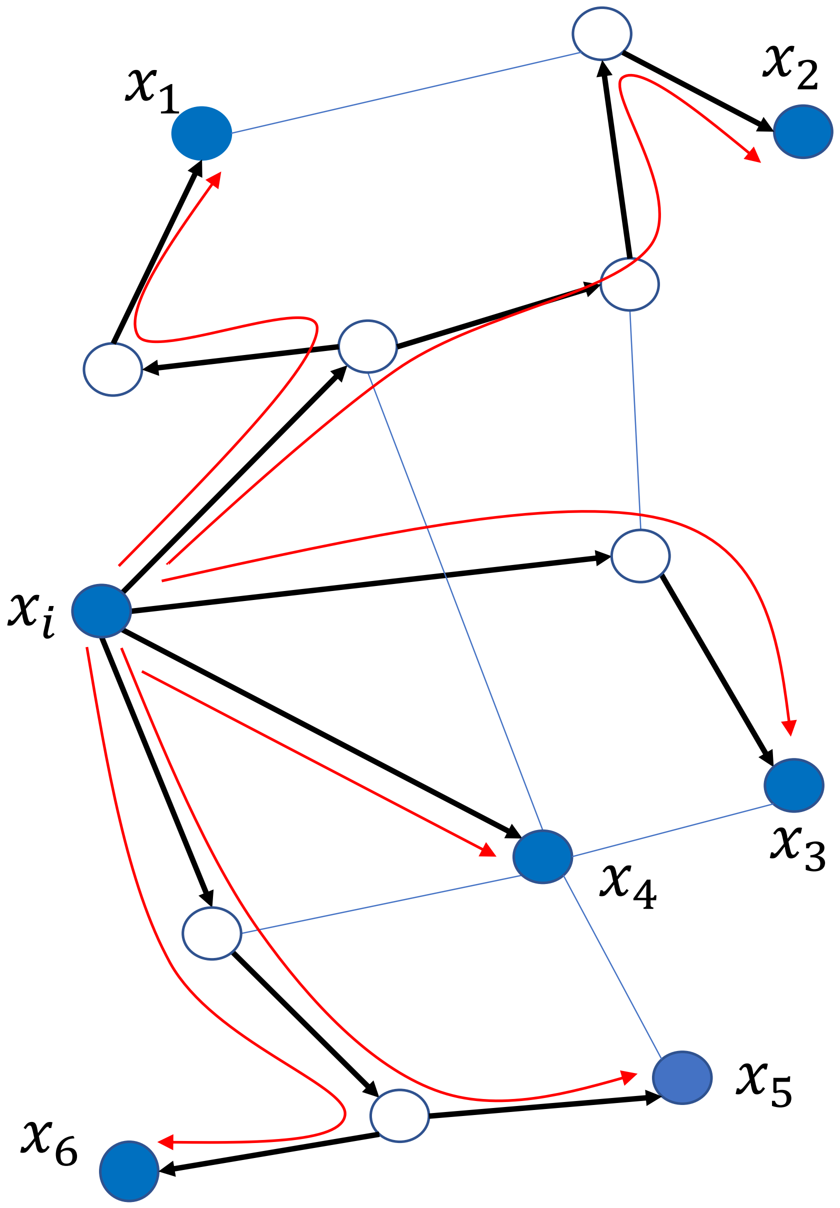
      $GT(x, y) = 1$ since $x_5 = 1 \,\&\, y_5 = 0 \,\&\, x_1 x_2 x_3 x_4 = y_1 y_2 y_3 y_4$

Ranking verification

- Ranking verification
  - $RV_t^{i,j}(x_1, x_2, \cdots, x_t) \coloneqq 1 \Leftrightarrow x_i$ is the j-th largest value in the list
  - $RV_t^{i,1}(x_1, x_2, \cdots, x_t) = 1 \Leftrightarrow x_i$ is the largest value in the list

[Theorem] There is a dQMA protocol for $RV_t^{i,j}$ such that local proof (message) size is $O(tr^2 \log n)$

- Proof strategy:
  1. Creates dQMA protocol for the Greater-Than (GT) function in the line network
  2. **Run the dQMA protocol for GT between node i and each of the other terminals**

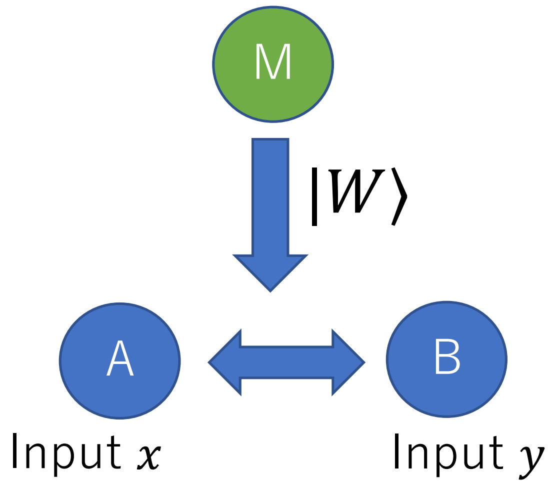


Proof ideas

- Ranking verification
- Lower bound for EQ

Proof sketch for EQ lower bound

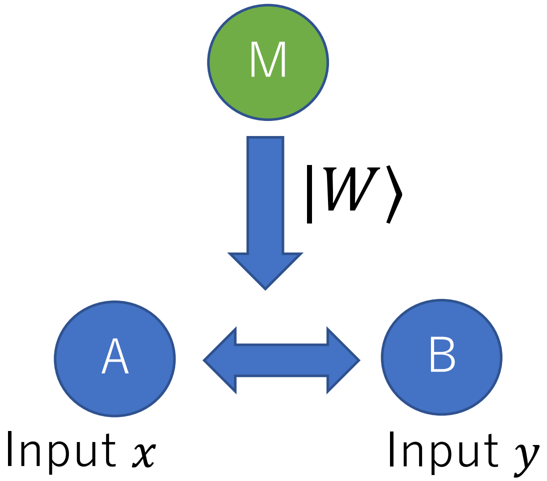
- [Theorem] The total proof & message size of any dQMA protocol for EQ is $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ where $\varepsilon > 0$ is any small constant
- Reduction to 2-party communication complexity
  - QMA communication complexity [Raz-Shpilka 04]
    - Special case that the network is the line with 2 nodes
    - $QMAcc(f)$:=total proof & message size for verifying $f(x,y) = 1$

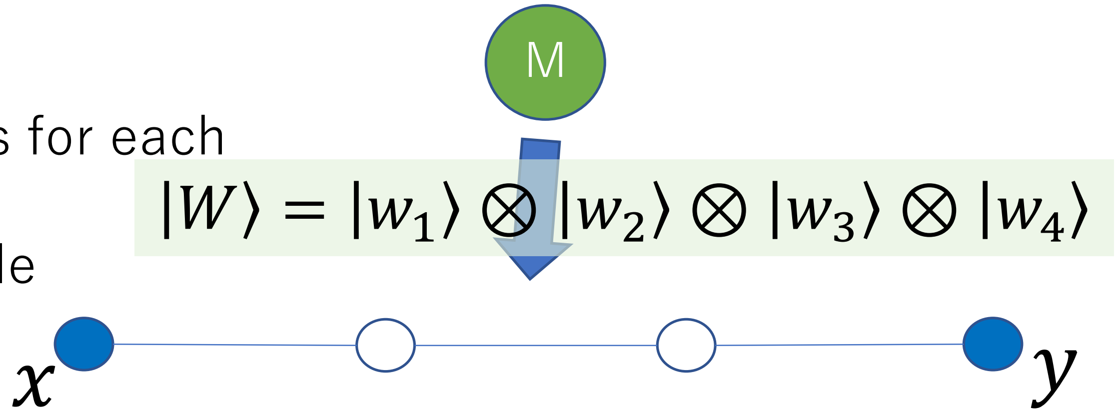


[Raz-Shapilka 04] R. Raz, A. Shapilka, Proc. CCC04

Proof sketch for EQ lower bound

- [Theorem] The total proof & message size of any dQMA protocol for EQ is $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ where $\varepsilon > 0$ is any small constant
- Reduction to 2-party communication complexity
  - QMA communication complexity [Raz-Shpilka 04]
    - Special case that the network is the line with 2 nodes
    - $QMAcc(f)$:=total proof & message size for verifying $f(x,y) = 1$
- Separable dQMA protocol
  - Quantum proof must be a product of states for each party
  - Protocols in [FLNP21,HKN24] are separable



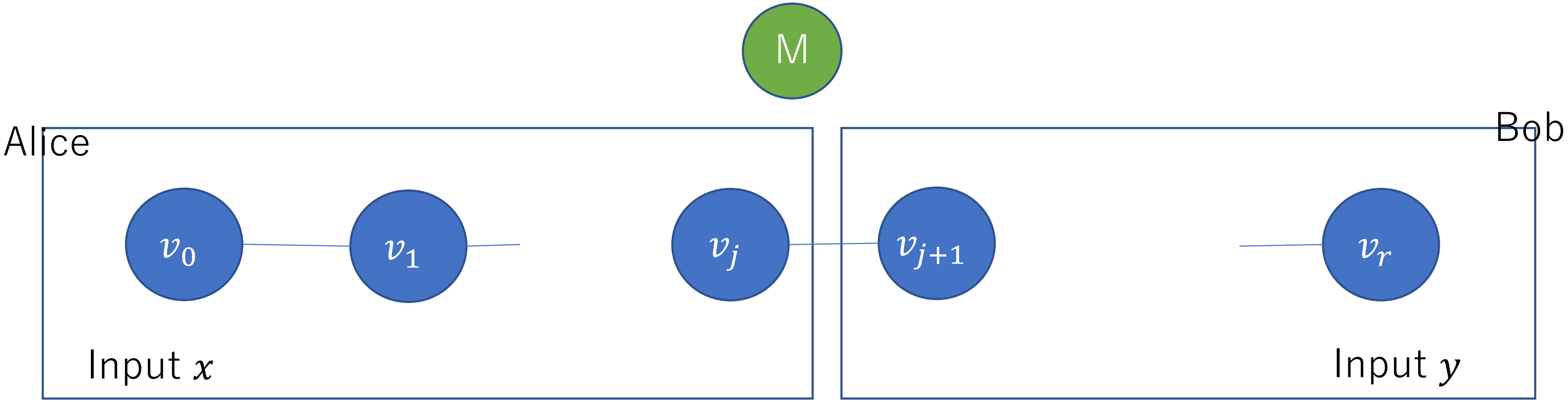


Proof sketch for EQ lower bound

[Lemma1 (dQMA ⇒ separable dQMA)]

If any function $f\colon\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a dQMA protocol with total proof + min message size C in the line of length r, then there is a separable dQMA protocol for f with total proof size $O(r^3C^2)$

- Reduces to a 2-party QMA communication complexity (CC) protocol

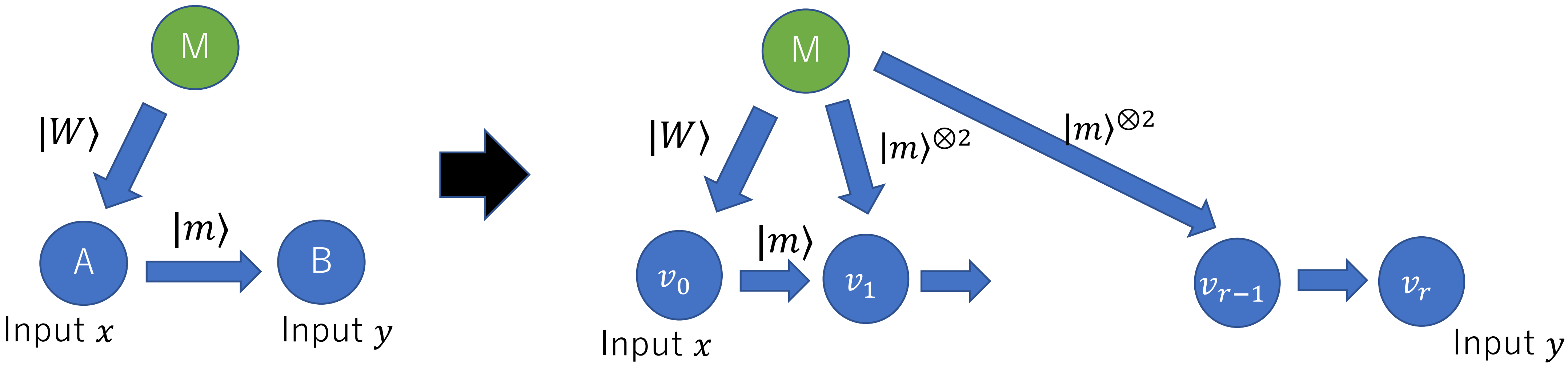


Proof sketch for EQ lower bound

[Lemma1 (dQMA⇒separable dQMA)]

If any function $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a dQMA protocol with total proof + min message size C in the line of length r, then there is a separable dQMA protocol for f with total proof size $O(r^3C^2)$

- Reduces to a 2-party QMA communication complexity (CC) protocol
- Creates a separable dQMA protocol (based on [FLNP21]) for the CC protocol



Proof sketch for EQ lower bound

- Gives a lower bound on separable dQMA protocols for EQ
  - Total proof size $\Omega(r \log n)$
  - Classical LB for EQ [FLNP21] + Size lower bound of quantum fingerprints
- Lemma1 implies
  - Total proof & min message size $\Omega((\log n)^{\frac{1}{2}-\varepsilon}/r^{1+\delta})$ for any constant $\varepsilon, \delta > 0$ on (entangled) dQMA protocols for EQ

[Lemma1 (dQMA⇒separable dQMA)]
If any function $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a dQMA protocol with total proof + min message size C on the line of length r, then there is a separable dQMA protocol for f with total proof size $O(r^3 C^2)$

Proof sketch for EQ lower bound

- Gives a lower bound on separable dQMA protocols for EQ
  - Total proof size $\Omega(r \log n)$
  - Classical LB for EQ [FLNP21] + Size lower bound of quantum fingerprints
- Lemma1 implies
  - Total proof & min message size $\Omega((\log n)^{\frac{1}{2}-\varepsilon}/r^{1+\delta})$ for any constant $\varepsilon, \delta > 0$ on (entangled) dQMA protocols for EQ
- Gives another lower bound on dQMA protocols for EQ
  - $\Omega(r)$

$\Rightarrow$

[Theorem] The total proof & min message size of any dQMA protocol for EQ is $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ where $\varepsilon > 0$ is any small constant

Summary & Future work

- Our results [HKN24]
  - More problems can be verified in dQMA proof systems
    - Hamming distance & Ranking verification
  - First quantum lower bound
    - Total proof size + message size: $\Omega((\log n)^{\frac{1}{4}-\varepsilon})$ (for EQ in the line network)
  - Improvement over [FLNP21]
    - Total proof size for EQ: $O(tr^3 \log n) \Rightarrow O(r^3 \log n)$
  - Quantum advantage for EQ on the line network even if the length is large compared to input length of EQ: classical $\Omega(rn)$ vs quantum $\tilde{O}(rn^{\frac{2}{3}})$
- Future work
  - Lower bounds on proof size (only)
  - Quantum advantage for natural problems when the network size is large

[HKN24] A. Hasegawa, S. Kundu, HN, Proc. PODC24, arXiv:2403.14108