

Quantum Random Access Coding and Its Applications

Harumichi Nishimura (Kyoto U.)

TQC2006, Feb. 22

Overview

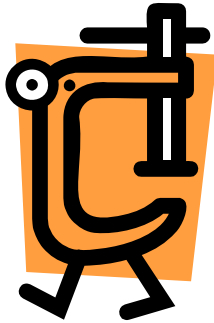
1. Quantum random access coding (QRAC)
 - QRAC for a few bits
 - Asymptotic bound
 - More bound of QRAC
2. Applications to advised computation
3. QRAC on the network

Quantum Random Access Coding

[Ambainis-Nayak-Ta-shma-Vazirani. 99]

(m,n,p) -QRAC

Sender



x

m bits



$|\Psi(x)\rangle$

n qubits



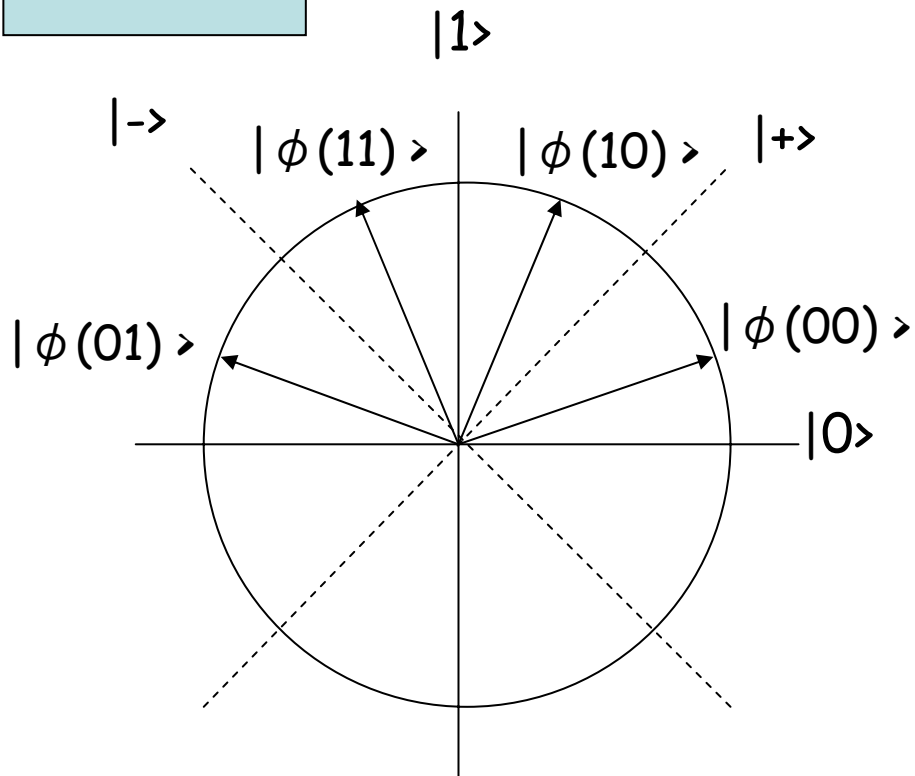
Receiver

$i \in \{1, 2, \dots, m\}$

Goal: For any given i ,
output the i -th bit of x
with prob. $p > 1/2$

(2,1,0.85)-QRAC

Encoding



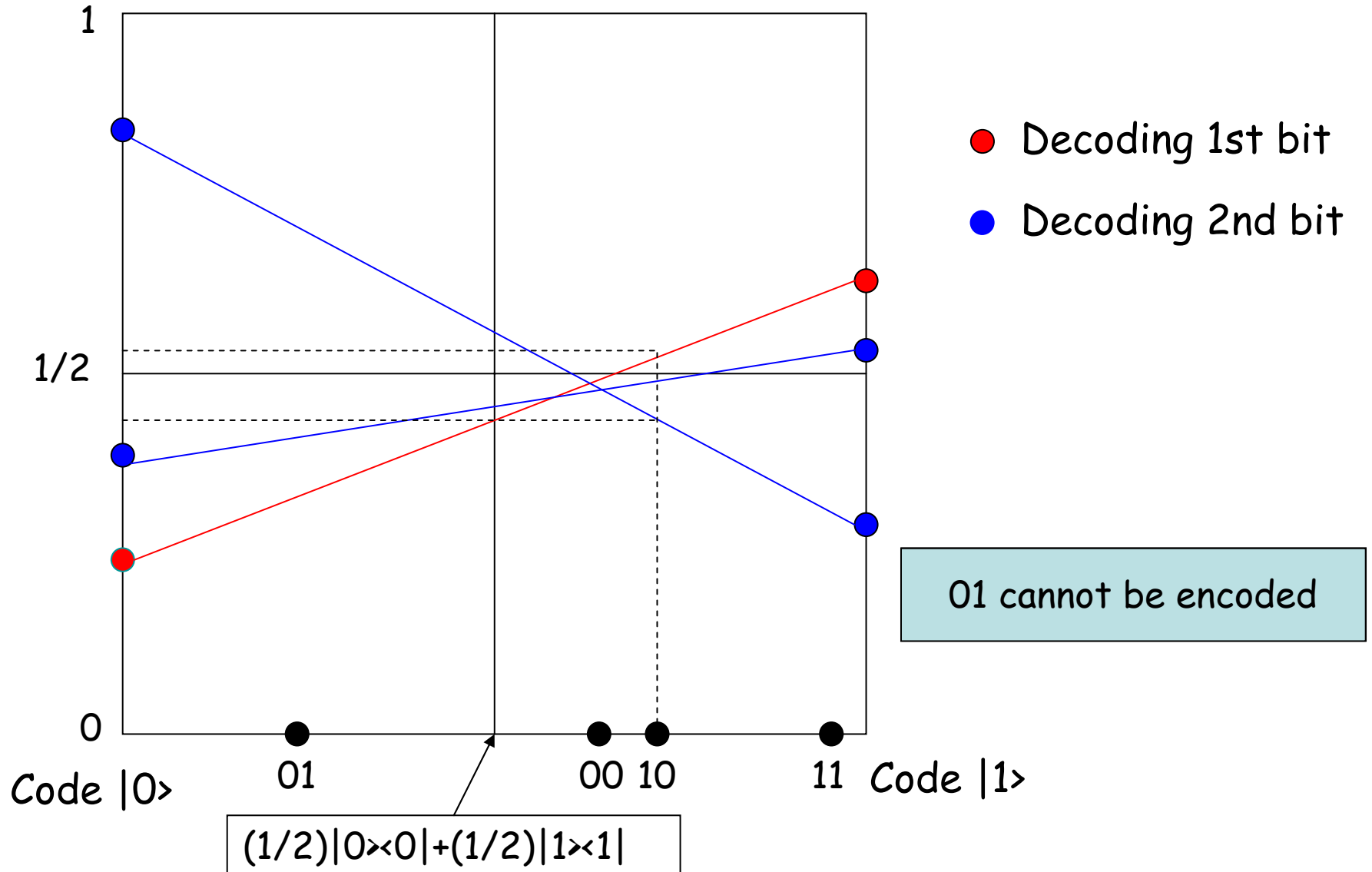
Decoding

To obtain 1st bit,
use the basis $\{|0\rangle, |1\rangle\}$.

For 2nd bit,
use the basis $\{|+\rangle, |-\rangle\}$

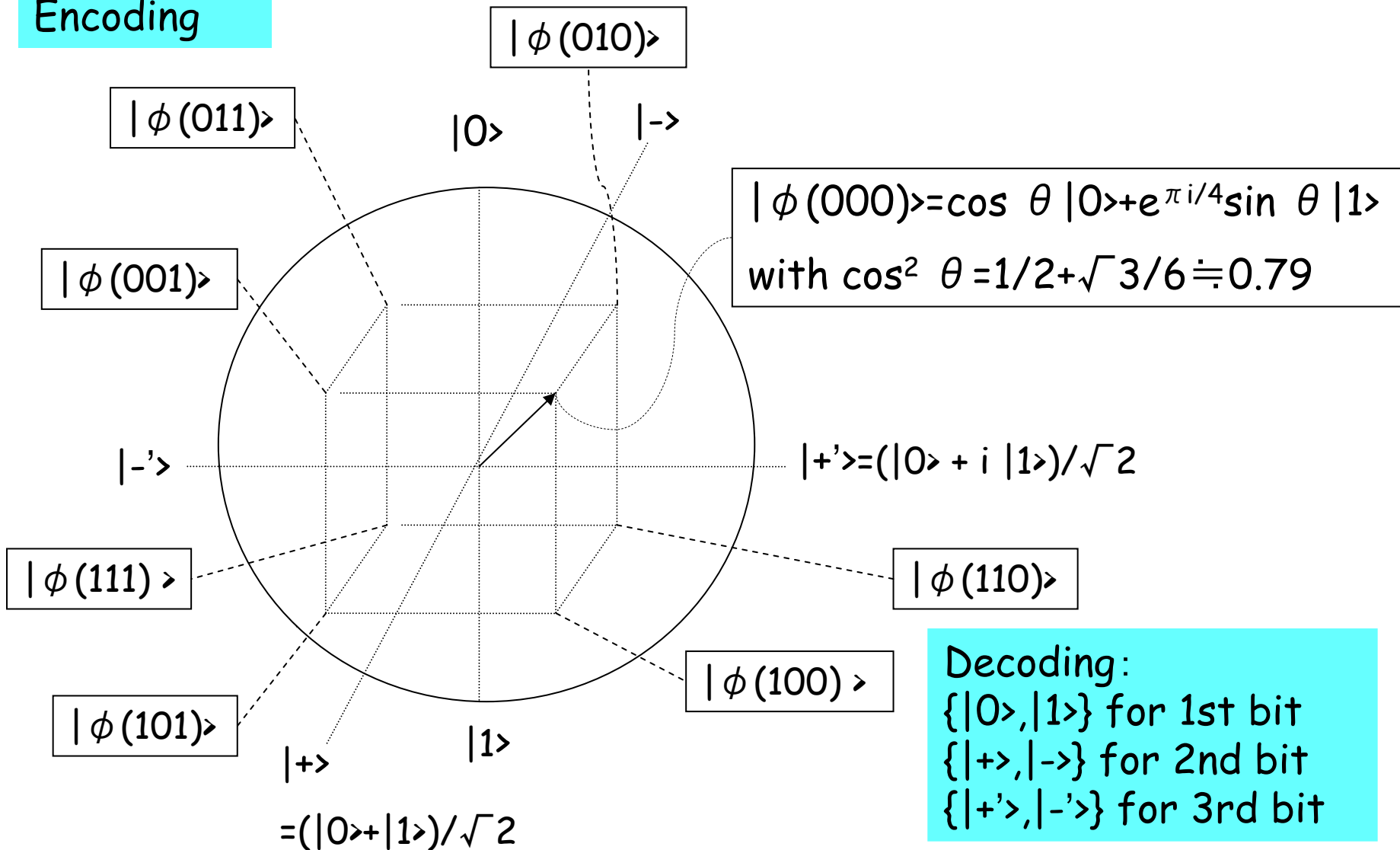
$(2,1,>1/2)$ -RAC is Classically Impossible

Prob[Out=1]



(3,1,0.79)-QRAC

Encoding



Asymptotic Bound

- **Upper bound** [Ambainis et al. 99]
 - (m,n,p) -QRAC exists such that
$$n \leq (1 - H(p))m + O(\log m)$$
 - In fact, the coding is classical
 - Using "covering code"
- **Lower bound** [Nayak 99]
 - $n \geq (1 - H(p))m$
 - Proved by the use of quantum information theory
 - Many applications in computational complexity!

More Bound of QRAC

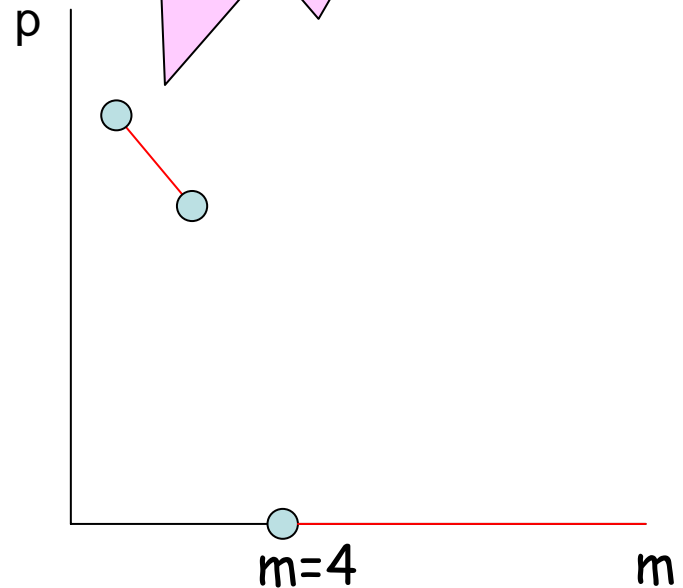
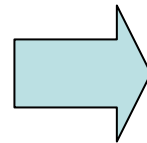
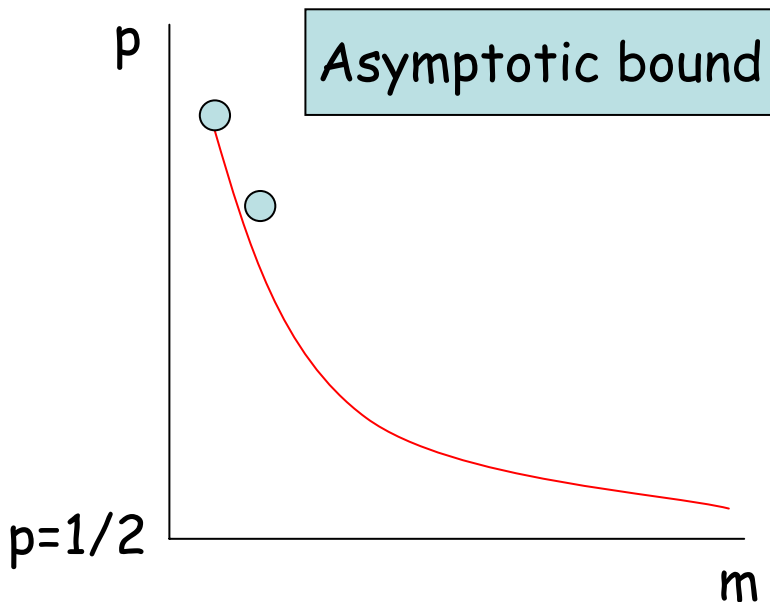
• Does an $(m, 1, p > 1/2)$ -QRAC exist?

- $(2, 1, 0.85)$ -QRAC

- $(3, 1, 0.79)$ -QRAC

- $(4, 1, p)$ -QRAC, $(5, 1, p)$ -QRAC?

**$(4, 1, p)$ -QRAC
is impossible
[Hayashi-Iwama
-N-Raymond
-Yamashita06]**



Contents

1. Quantum random access coding (QRAC)
 - QRAC for a few bits
 - Asymptotic bound
 - More bound of QRAC
2. Applications to advised computation
3. QRAC on the network

Applications of QRAC Lower Bound

- Limit of quantum finite automata
[Ambainis et al. 99, Nayak 99]
- Communication complexity
[Klauck 00, Buhrman-de Wolf 01, Gavinsky-Kempe-Regev-de Wolf. 06]
- **Advised computation**
[N-Yamakami 04, Aaronson 05]
- Locally decodable code and private information retrieval
[Kerenidis-de Wolf 03, Wehner-de Wolf 05]

Advised Computation

Input X (length n)



Advice Y_n



Polynomial-time
Computer (P-machine)

Adviser:
Unlimited power

He does not know her input
 x while knows its length n

$P/poly$:= Class of sets recognized by P-machines with polynomial advice

Advised Quantum Computation

Input X (length n)



Adviser:
Unlimited power

Advice Y
(length $f(n)$)



Quantum
Advice $|\Phi\rangle$
(length $f(n)$)



Polynomial-time
Quantum Computer
(BQP-machine)

BQP/ $f(n)$:= Class of sets recognized by BQP-machines with advice of length $f(n)$

BQP/ $Qf(n)$:= Class of sets recognized by BQP-machines with quantum advice of length $f(n)$

Why Quantum Advice?

She sends messages securely using a quantum one-way function F



$F(X)$



Eve cannot find the message X

However, if Eve has some quantum information (say, by previous communication history), it can be **quantum advice for Eve!**

Limitation of Quantum Advice

- $BQP/\log \subseteq BQP/Q\log \subseteq BQP/poly \subseteq BQP/Qpoly$
- $BQP/\log \neq BQP/Q\log$
 - By using fingerprint
- For any positive function f , $P/f(n)$ is not included in $BQP/Q(0.08f(n))$ [N-Yamakami 04]
 - By using the lower bound of QRAC
- Thus,
 - $P/linear \not\subseteq BQP/Q\log$.
 - $P/poly \not\subseteq BQP/Qlinear$, and hence
 - $BQP/Q\log \neq BQP/poly$.

$P/f(n) \not\subseteq BQP/Q(0.08f(n))$

Recognized by P-machine + advice of length $f(n)$

Consider all the subsets L_n of $\{x \in \{0,1\}^n \mid x \leq s^{f(n)}\}$,
which have cardinality at most $f(n)$.

Adviser

$|\Phi_n\rangle$: length m



$\text{Prob}[M_n(x, |\Phi_n\rangle) = L_n(x)] \geq 2/3$
for all $x \leq s^{f(n)}$ (= the $f(n)$ -th string
of $\{0,1\}^n$ in the lexicographic order).

BQP-machine
 M_n

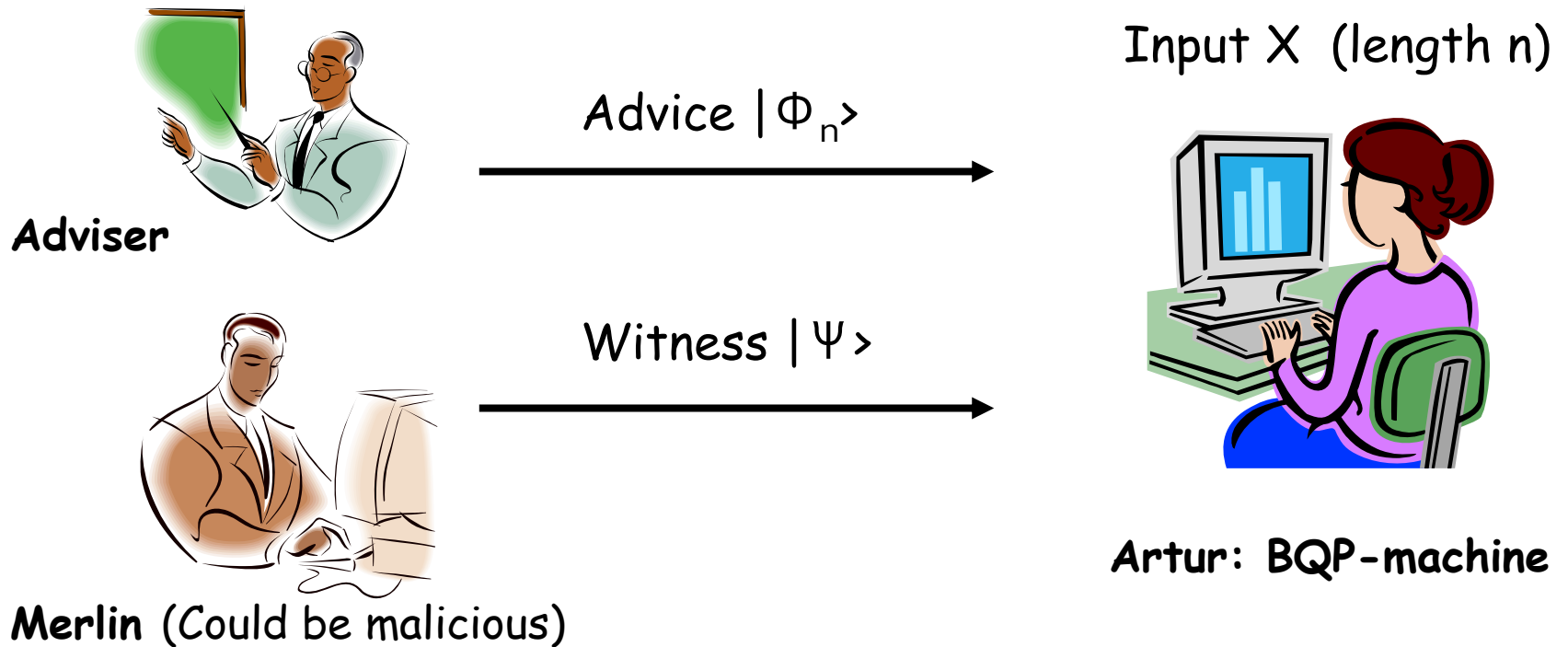


The input x given to M_n is random for Adviser.

Thus, $g(n) = |\Phi_n\rangle$ is $(f(n), m, 2/3)$ -QRAC, and hence
some subset not recognized by M_n + quantum advice
of length $(1 - H(1/3))f(n)$ exists

QMA + Advice

- $L \in \text{QMA}/\text{Qpoly} \Leftrightarrow \exists \text{ptime QC } M, \text{ advice } \{|\Phi_n\rangle\}$
If $x \in L$, then $\exists |\Psi\rangle \text{Prob}[M(x, |\Psi\rangle, |\Phi_n\rangle) = \text{"YES"}] > 2/3$
If $x \notin L$, then $\forall |\Psi\rangle \text{Prob}[M(x, |\Psi\rangle, |\Phi_n\rangle) = \text{"YES"}] < 1/3$



Limit of QMA + Advice

Input L (length $N=2^n$)



Adviser

Advice (length a)



Witness (length w)



Merlin

Input X (length n)



Artur: BQP-machine

This setting can be considered as $(N, a, 1/3)$ -QRAC with witness of length w

- (De-Merlization) If $\exists (N, a, 1/3)$ -QRAC with witness of length w , then $\exists (N, O(a \cdot w \log^2 w), 1/3)$ -QRAC. [Aaronson 05]
- $\text{QMA}/\text{Qpoly} \subseteq \text{PSPACE}/\text{poly}$

Contents

1. Quantum random access coding (QRAC)
 - QRAC for a few bits
 - Asymptotic bound
 - More bound of QRAC
2. Applications to advised computation
3. QRAC on the network

Network Coding

- Network coding [Ahlsvede-Cai-Li-Yeung. 2000]
 - Information theory + Transportation problem
 - Google "Network coding"

Information theory

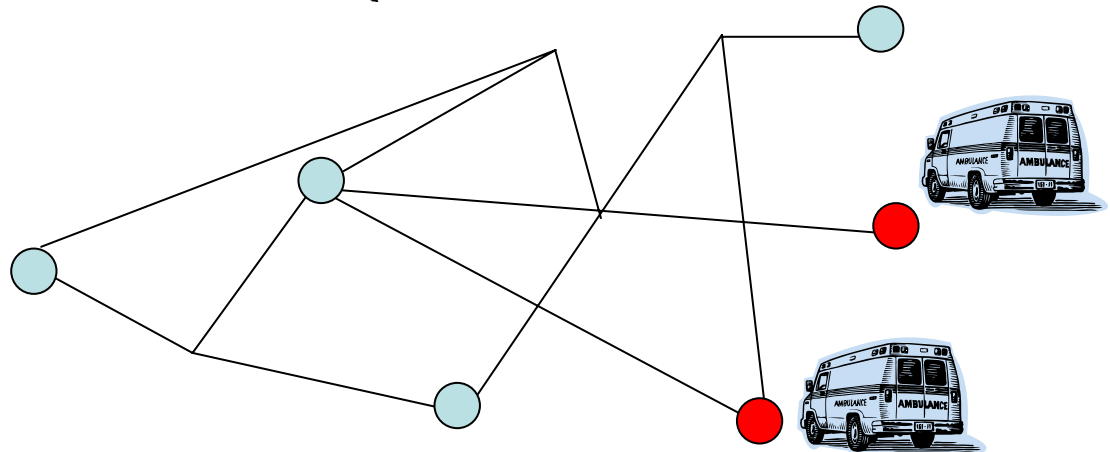
- One-to-one
- Noisy channel



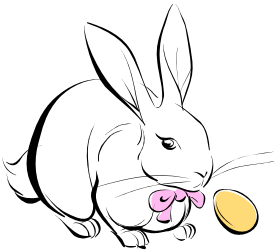
Data Compression
Error Correction
Security

Transportation problem

- Complicated network
- No coding



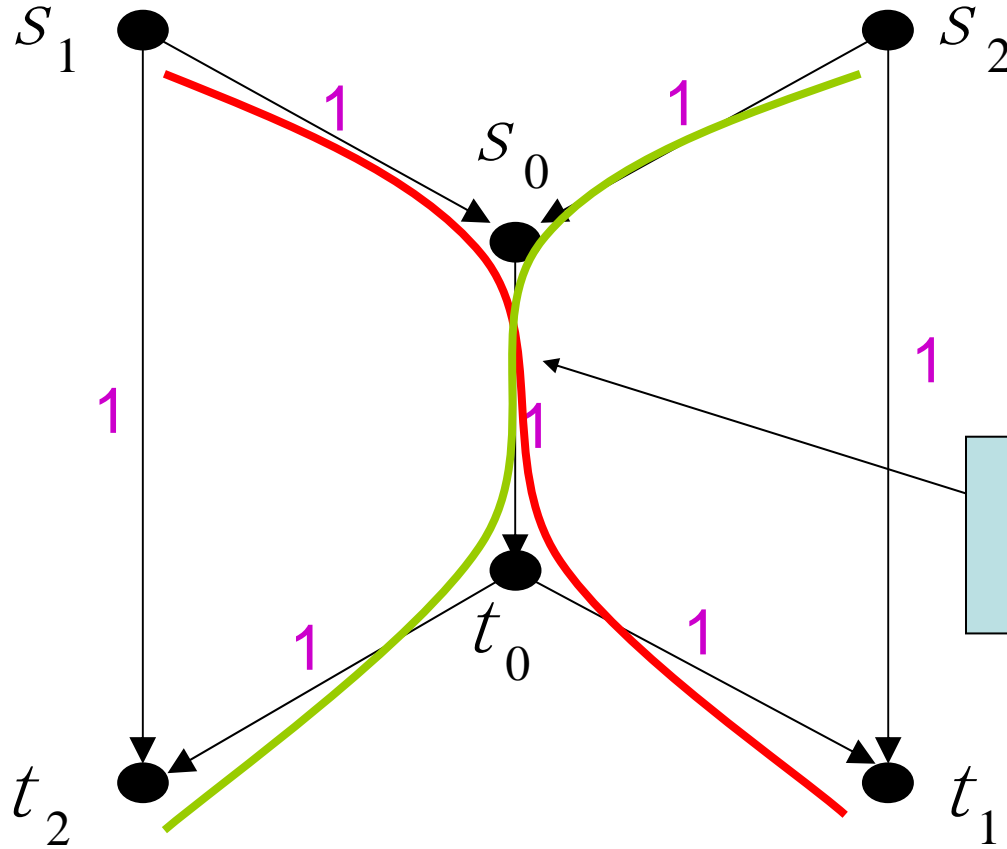
Liquid Flow



s_1



s_2

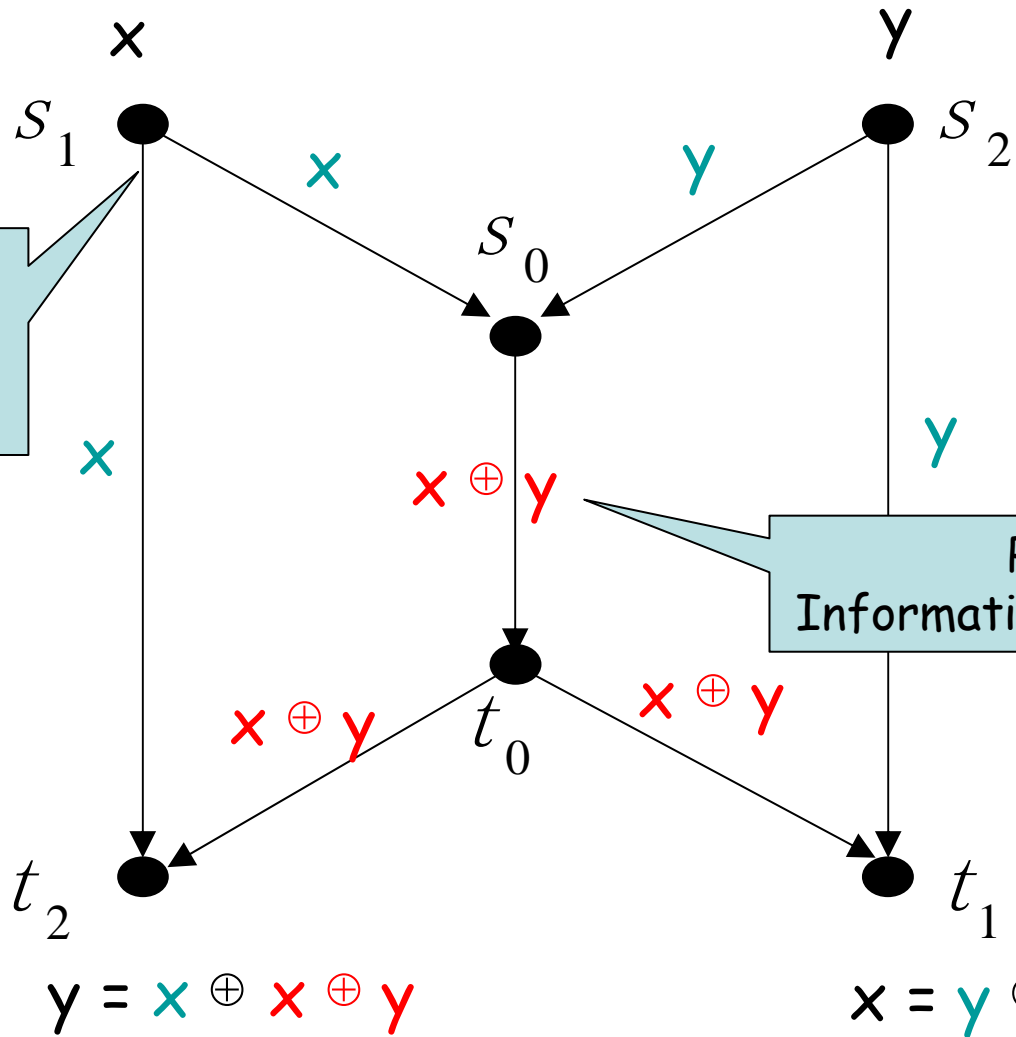


No solution by routing

Butterfly Network (B-Net)

Information Flow

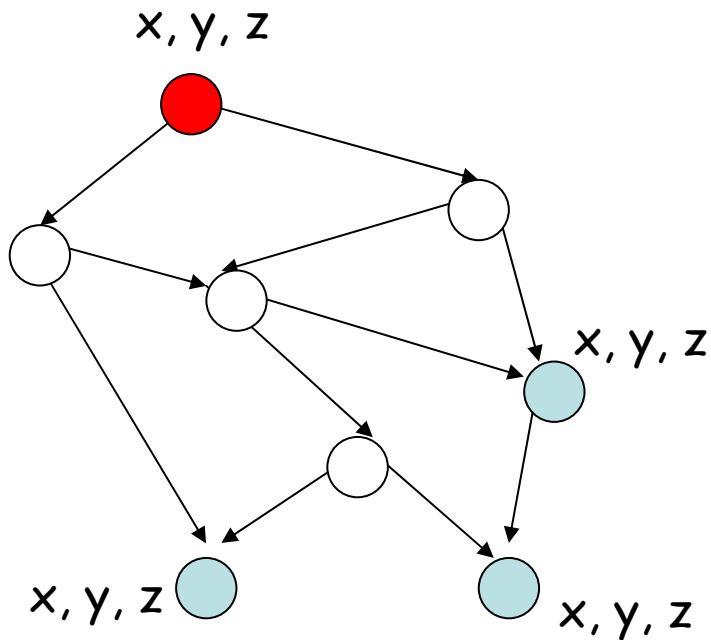
[Ahlsweide et al. 2000]



POINT 1
Information can
be copied

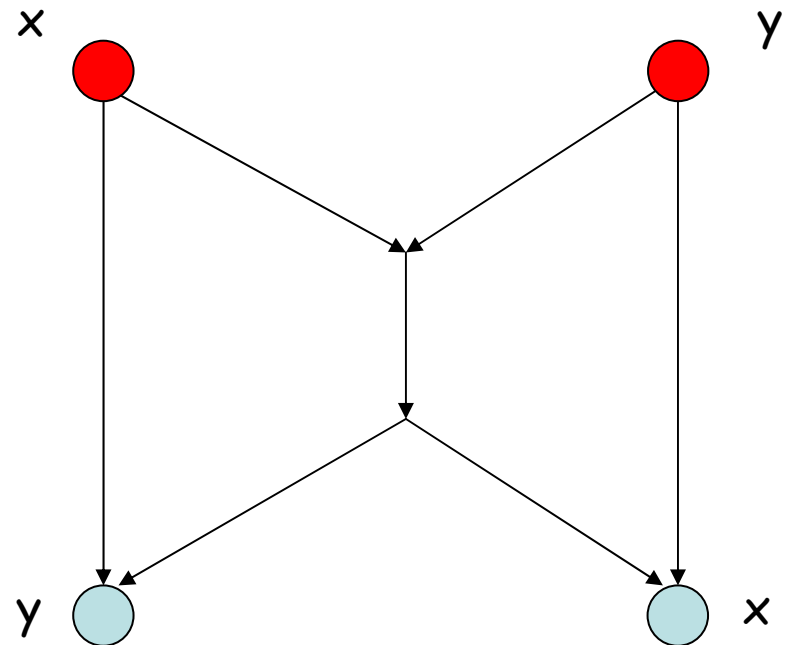
POINT 2
Information can be encoded

Well-studied Network



Multicast:

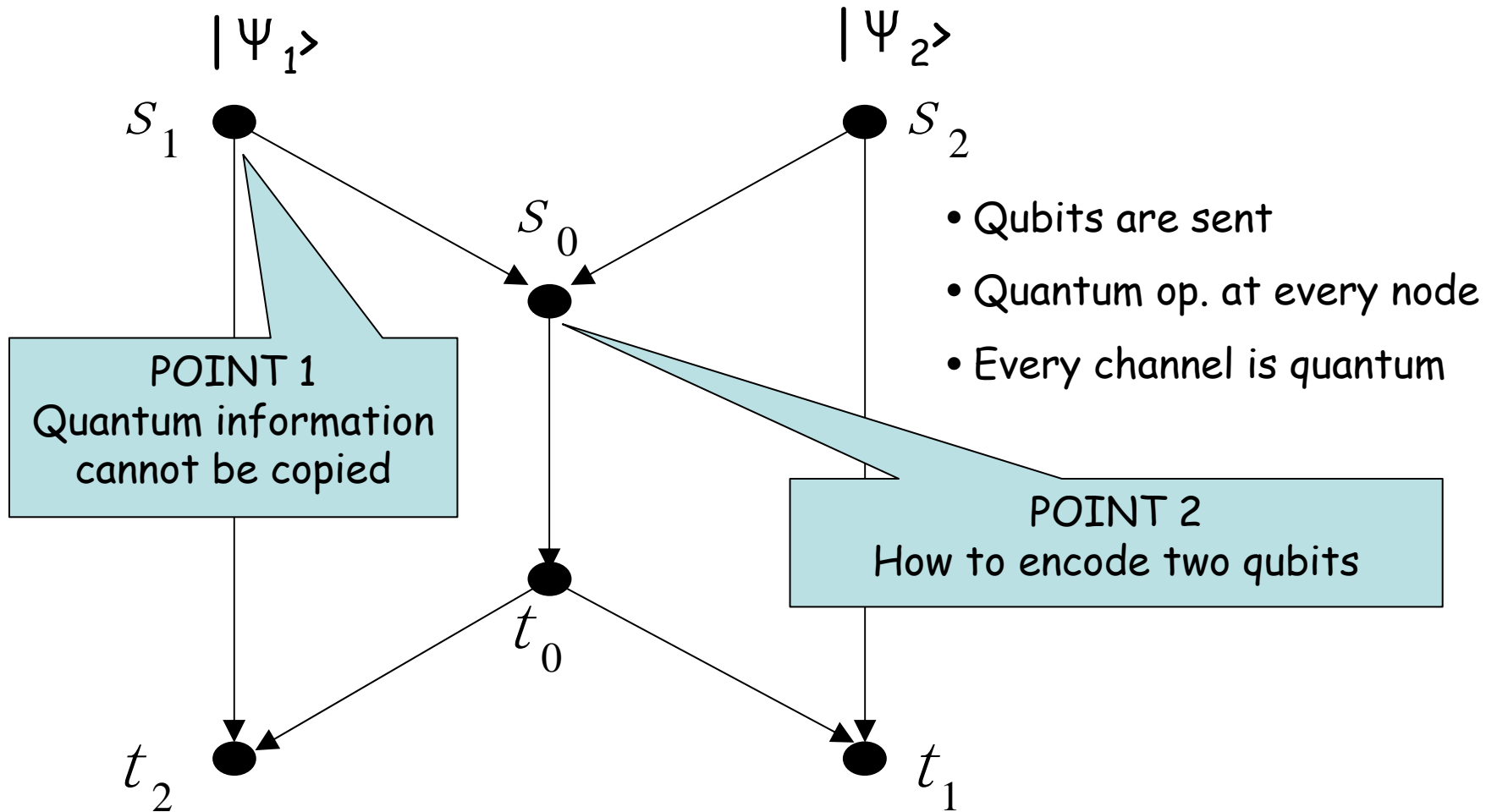
Every sink requires all messages which a source has.



k -Pairs Communication:

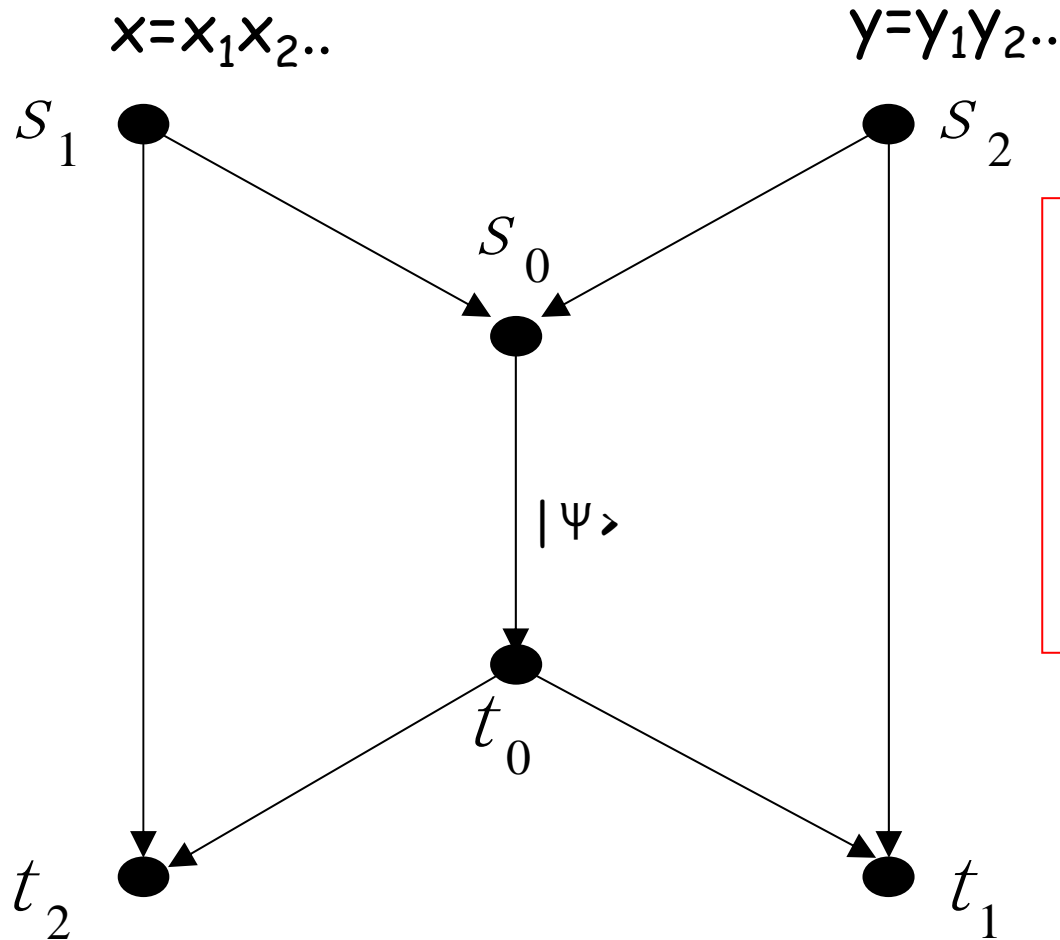
Each commodity has one source-sink pair. Butterfly network is 2-pairs communication problem.

Quantum Information Flow



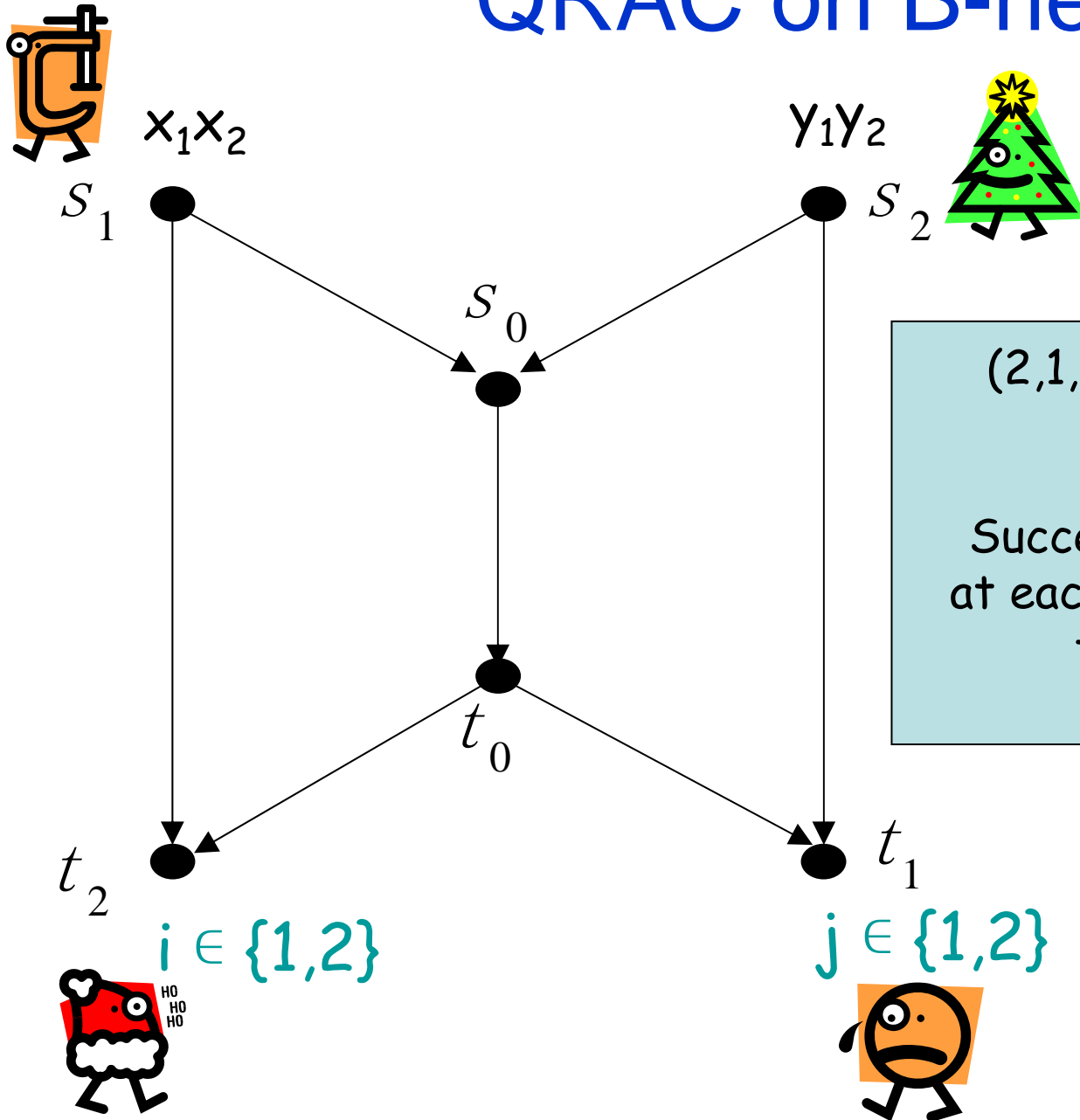
See [quant-ph/0601088](https://arxiv.org/abs/quant-ph/0601088)

Information Flow by Using Quantum



- **Many bits** are sent
- Problem: Success prob. of sending n bits by one-qubit is at most $1/2^n$
- Quantum op. at every node
- Quantum channel

QRAC on B-net



(2,1,p)-QRAC on B-net
(X2C2C)

Success decoding prob.
at each sink t is required
to be $p > 1/2$.

QRAC on B-net

- Success prob. $\doteq 0.59$ for **X2C2C on B-net** [Hayashi-Iwama-N-Yamashita-Raymond 06]
 - Classically, at most $1/2$
 - For the case of 3bits (X3C3C), success probability is still $> 1/2$ ($\doteq 0.525$)
 - X4C4C is impossible

X2C2C

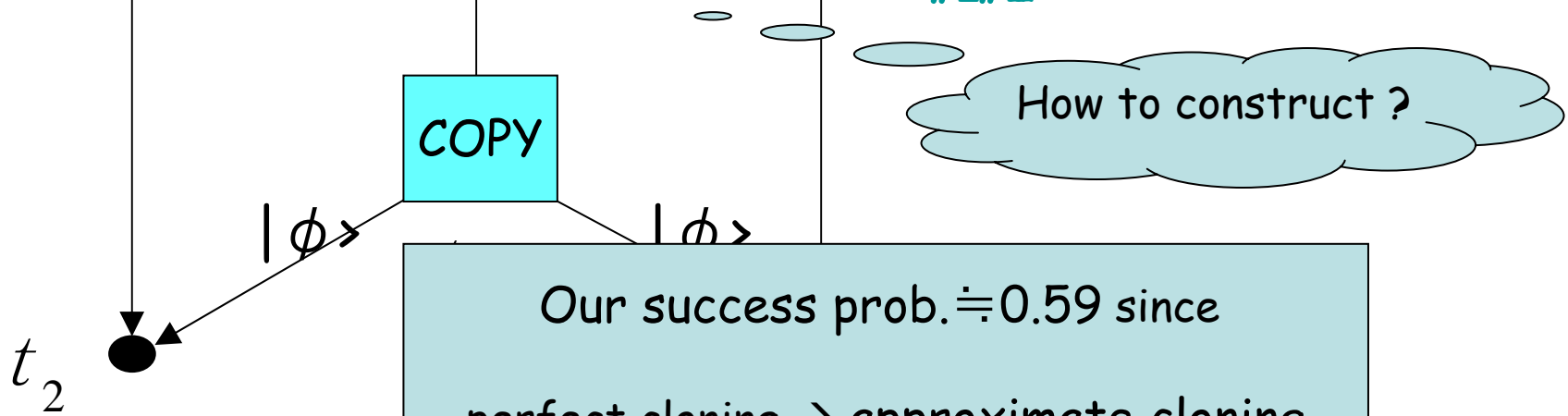
x_1x_2

y_1y_2

Success decoding prob. (DP) at t_2 (assuming that COPY is "perfect")

$$\begin{aligned}
 &= [\text{Success DP of } |\Phi(x_1x_2)\rangle] \times [\text{Success DP of } |\Phi(x_1 \oplus y_1, x_2 \oplus y_2)\rangle] \\
 &+ [\text{Fail DP of } |\Phi(x_1x_2)\rangle] \times [\text{Fail DP of } |\Phi(x_1 \oplus y_1, x_2 \oplus y_2)\rangle] \\
 &\doteq (0.85)(0.85) + (1-0.85)(1-0.85) = 0.75
 \end{aligned}$$

$|\phi(x_1x_2)\rangle$ $|\phi(x_1 \oplus y_1, x_2 \oplus y_2)\rangle$ $|\phi(y_1y_2)\rangle$



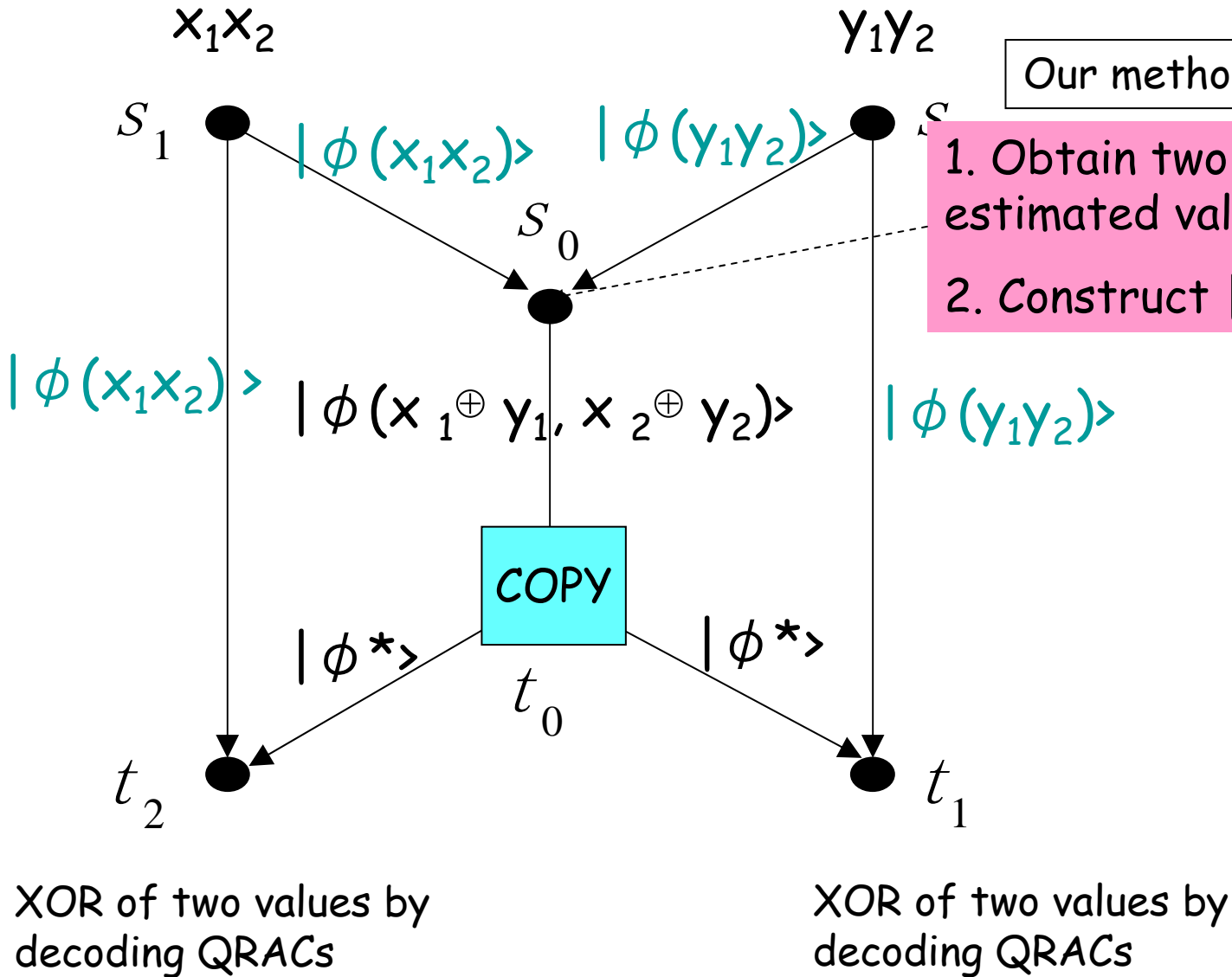
Our success prob. $\doteq 0.59$ since

perfect cloning \rightarrow approximate cloning operations at $s_0 \rightarrow$ success prob with 0.75

XOR of two values by decoding QRACs

by decoding QRACs

X2C2C



Our method

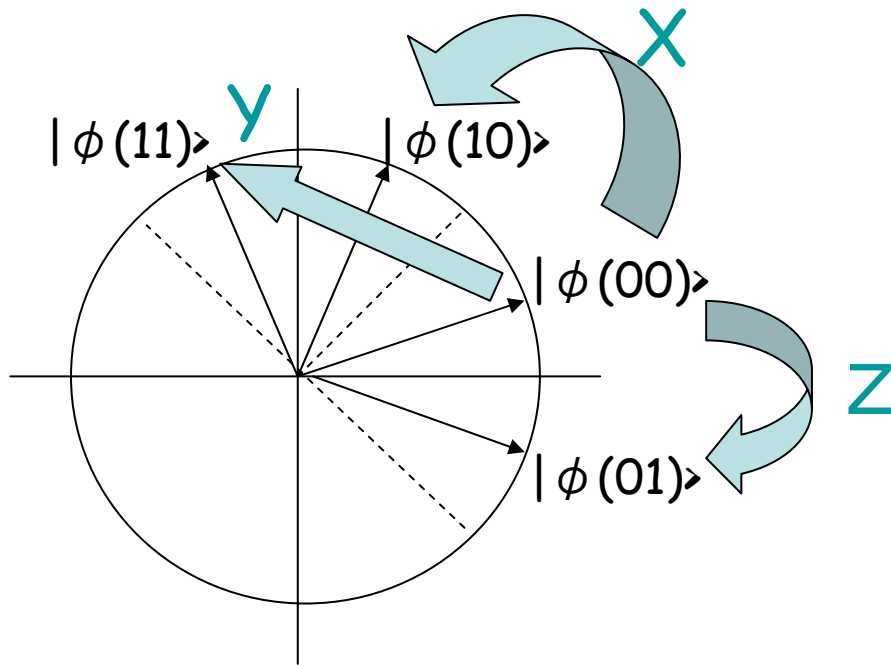
1. Obtain two bits z_1z_2 as an estimated value of y_1y_2
2. Construct $|\Phi(x_1 \oplus z_1, x_2 \oplus z_2)\rangle$

XOR of two values by decoding QRACs

XOR of two values by decoding QRACs

Operation at s_0 : If we know $y_1 y_2$

$|\phi(x_1 x_2)\rangle \rightarrow |\phi(x_1 \oplus y_1, x_2 \oplus y_2)\rangle$ is possible



Group operation

If $y_1 y_2 = 00$,

Apply $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

If $y_1 y_2 = 01$,

Apply $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ **phase flip**

If $y_1 y_2 = 11$,

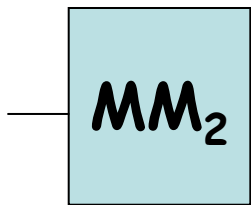
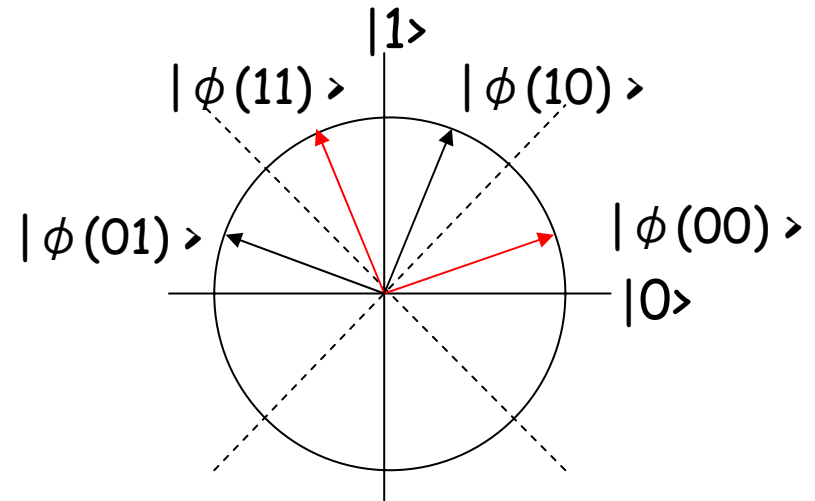
Apply $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

If $y_1 y_2 = 10$,

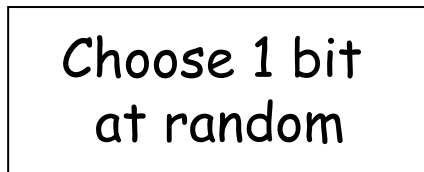
Apply $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ **bit flip**

Operation at s_0 : Estimate y_1y_2

Random projective measurement MM_2



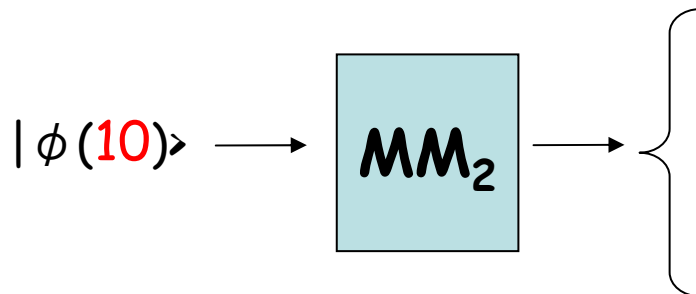
=



basis $\{|\phi(01)\rangle, |\phi(10)\rangle\}$

If 0 is obtain, output 00

If 1 is obtain, output 11



- 00 with prob. 1/4
- 01 with prob. 0
- 10 with prob. 1/2
- 11 with prob. 1/4

Conclusion

- Quantum random access coding has some advantage over classical one (even for on some network)
- Asymptotically, no advantage
 - $(1 - H(p))m + O(\log m)$ bits are enough for m bits
 - needs $(1 - H(p))m$ qubits
- Including its variants, QRAC has many applications to computational complexity

