Fault-tolerant Concatenated Bell-state Measurement with Coherent-state Qubits

Seokhyung Lee and Hyunseok Jeong

SNU Quantum Information Science Group

June 1, 2020

Table of Contents

Table of Contents

Concatenated Bell-state measurement

Parity encoding

$$|0_L\rangle := \left|+^{(m)}\right\rangle^{\otimes n}, \qquad |1_L\rangle := \left|-^{(m)}\right\rangle^{\otimes n}$$

where

$$\left|\pm^{(m)}\right\rangle := |H\rangle^{\otimes m} \pm |V\rangle^{\otimes m}$$

- Physical level: $|\pm\rangle := \left|\pm^{(1)}\right\rangle = |H\rangle \pm |V\rangle \rightarrow$ Concatenate to form a block level
- Block level: $\left|\pm^{(m)}\right\rangle \rightarrow$ Concatenate to form a logical level
- Logical Level: $|0_L\rangle$, $|1_L\rangle$
- Generalization of Shor's 9-qubit code ($n = 3$, $m = 3$ case)

Ref)
F. Ewert, M. Bergmann, and P. van Loock, *Ultrafast Long-Distance Quantum Communication with Static Linear Optics*, Phys. Rev. Lett. 177, 210510 (2016).

S.-W. Lee, T. C. Ralph, and H. Jeong, *Fundamental building block for all-optical scalable quantum networks*, Phys. Rev. A 100, 052303 (2019).

Concatenated Bell-state measurement (cont.)

Bell states

- Logical level

$$|\Phi_\pm\rangle := |0_L\rangle\,|0_L\rangle \pm |1_L\rangle\,|1_L\rangle$$
$$|\Psi_\pm\rangle := |0_L\rangle\,|1_L\rangle \pm |1_L\rangle\,|0_L\rangle$$

Concatenated Bell-state measurement (cont.)

Bell states

- Logical level

$$|\Phi_\pm\rangle := |0_L\rangle |0_L\rangle \pm |1_L\rangle |1_L\rangle$$
$$|\Psi_\pm\rangle := |0_L\rangle |1_L\rangle \pm |1_L\rangle |0_L\rangle$$

- Block level

$$\left|\phi_\pm^{(m)}\right\rangle := \left|+^{(m)}\right\rangle \left|+^{(m)}\right\rangle \pm \left|-^{(m)}\right\rangle \left|-^{(m)}\right\rangle$$
$$\left|\psi_\pm^{(m)}\right\rangle := \left|+^{(m)}\right\rangle \left|-^{(m)}\right\rangle \pm \left|-^{(m)}\right\rangle \left|+^{(m)}\right\rangle$$

Concatenated Bell-state measurement (cont.)

Bell states

- Logical level

$$|\Phi_\pm\rangle := |0_L\rangle|0_L\rangle \pm |1_L\rangle|1_L\rangle$$
$$|\Psi_\pm\rangle := |0_L\rangle|1_L\rangle \pm |1_L\rangle|0_L\rangle$$

- Block level

$$\left|\phi_\pm^{(m)}\right\rangle := \left|+^{(m)}\right\rangle\left|+^{(m)}\right\rangle \pm \left|-^{(m)}\right\rangle\left|-^{(m)}\right\rangle$$
$$\left|\psi_\pm^{(m)}\right\rangle := \left|+^{(m)}\right\rangle\left|-^{(m)}\right\rangle \pm \left|-^{(m)}\right\rangle\left|+^{(m)}\right\rangle$$

- Physical level

$$|\phi_\pm\rangle := \left|\phi_\pm^{(1)}\right\rangle = |+\rangle|+\rangle \pm |-\rangle|-\rangle$$
$$|\psi_\pm\rangle := \left|\psi_\pm^{(1)}\right\rangle = |+\rangle|-\rangle \pm |-\rangle|+\rangle$$

Concatenated Bell-state measurement (cont.)

Decomposition of Bell states

$$\left|\Phi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\phi_{-}^{(m)}\right\rangle^{\otimes j}\left|\phi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\psi_{-}^{(m)}\right\rangle^{\otimes j}\left|\psi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\phi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{even}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k}\left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

$$\left|\psi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{odd}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k}\left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

($\mathcal{P}[\cdot]$: summation of all possible permutations of input tensor products.)

- Logical Bell state
  - n block Bell states
- Block Bell state
  - m physical Bell states

Concatenated Bell-state measurement (cont.)

Decomposition of Bell states

$$\left|\Phi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\phi_{-}^{(m)}\right\rangle^{\otimes j} \left|\phi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\psi_{-}^{(m)}\right\rangle^{\otimes j} \left|\psi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\phi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{even}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k} \left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

$$\left|\psi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{odd}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k} \left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

($\mathcal{P}[\cdot]$: summation of all possible permutations of input tensor products.)

- Logical Bell state
  - n block Bell states
  - Symbol: Symbol of block states
  - Sign: Parity of number of (-) sign block states
- Block Bell state
  - m physical Bell states

Concatenated Bell-state measurement (cont.)

Decomposition of Bell states

$$\left|\Phi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\phi_{-}^{(m)}\right\rangle^{\otimes j}\left|\phi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=\text{even(odd)}\leq n} \mathcal{P}\left[\left|\psi_{-}^{(m)}\right\rangle^{\otimes j}\left|\psi_{+}^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\phi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{even}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k}\left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

$$\left|\psi_{\pm}^{(m)}\right\rangle = \frac{1}{\sqrt{2^{m-1}}} \sum_{k=\text{odd}\leq m} \mathcal{P}\left[\left|\psi_{\pm}\right\rangle^{\otimes k}\left|\phi_{\pm}\right\rangle^{\otimes m-k}\right]$$

($\mathcal{P}[\cdot]$: summation of all possible permutations of input tensor products.)

- Logical Bell state
  - n block Bell states
  - Symbol: Symbol of block states
  - Sign: Parity of number of (-) sign block states
- Block Bell state
  - m physical Bell states
  - Symbol: Parity of number of ψ physical states
  - Sign: Sign of physical states

Concatenated Bell-state measurement (cont).

Decomposition of Bell states (cont.)

- Logical Bell state: n block Bell states
  - Symbol: Symbol of block states
  - Sign: Parity of number of (-) sign block states
- Block Bell state: m physical Bell states
  - Symbol: Parity of number of ψ physical states
  - Sign: Sign of physical states

Concatenated Bell-state measurement (cont).

Decomposition of Bell states (cont.)

- Logical Bell state: n block Bell states
  - Symbol: Symbol of block states
  - Sign: Parity of number of (-) sign block states
- Block Bell state: m physical Bell states
  - Symbol: Parity of number of ψ physical states
  - Sign: Sign of physical states

Fault-tolerance

- Z errors (sign flip errors): Corrected at block level.
- X errors (symbol flip errors): Corrected at logical level.

Quantum repeater

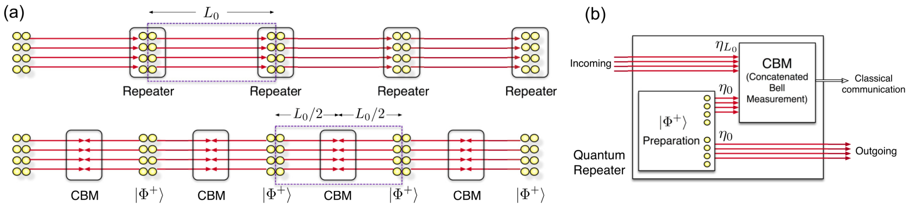


Figure: from S.-W. Lee et al. (2019)

- Photons travelling long-range distance have exponentially decreasing probability to survive.
- Quantum repeater enables long-range quantum communication using an error-correction scheme in repeater stations.
- In each station, a Bell state is prepared and the input state is teleported to the outgoing state with error correction.

Quantum repeater (cont.)

Quantifying quantum repeater

Ref) S. Muralidharan, J. Kim, N, Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. 112, 250501 (2014).

- Transmission probability

$$P_s^{tot} = P_{s,i}^{tot} + P_{s,x}^{tot} + P_{s,y}^{tot} + P_{s,z}^{tot} = \left(P_{s,i} + P_{s,x} + P_{s,y} + P_{s,z}\right)^{L/L_0}$$

Quantum repeater (cont.)

Quantifying quantum repeater

Ref) S. Muralidharan, J. Kim, N, Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. 112, 250501 (2014).

- Transmission probability

$$P_s^{tot} = P_{s,i}^{tot} + P_{s,x}^{tot} + P_{s,y}^{tot} + P_{s,z}^{tot} = (P_{s,i} + P_{s,x} + P_{s,y} + P_{s,z})^{L/L_0}$$

- Effective rate of X/Z errors

$$Q_{X/Z} = \frac{1}{2}\left[1 - \frac{(P_{s,i} \mp P_{s,x} \pm P_{s,z} - P_{s,y})^{L/L_0}}{(P_{s,i} + P_{s,x} + P_{s,y} + P_{s,z})^{L/L_0}}\right]$$

Quantum repeater (cont.)

Quantifying quantum repeater

Ref) S. Muralidharan, J. Kim, N, Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. 112, 250501 (2014).

- Transmission probability

$$P_s^{tot} = P_{s,i}^{tot} + P_{s,x}^{tot} + P_{s,y}^{tot} + P_{s,z}^{tot} = (P_{s,i} + P_{s,x} + P_{s,y} + P_{s,z})^{L/L_0}$$

- Effective rate of X/Z errors

$$Q_{X/Z} = \frac{1}{2}\left[1 - \frac{(P_{s,i} \mp P_{s,x} \pm P_{s,z} - P_{s,y})^{L/L_0}}{(P_{s,i} + P_{s,x} + P_{s,y} + P_{s,z})^{L/L_0}}\right]$$

- Asymptotic key generation rate in QKD

$$R = max[P_s^{tot}\{1 - 2h(Q)\}/t_0]$$

where $h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$, $Q = (Q_X + Q_Z)/2$, and t_0 is the time taken in one repeater station.

Coherent-state qubit

Coherent-state qubit: $\{|\alpha\rangle, |-\alpha\rangle\}$

Bell-state measurement of coherent-state qubits
Use a beam splitter (BS) & two photon number parity detectors (PNPDs).

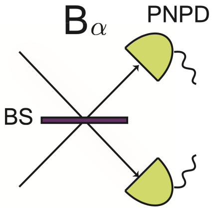


Figure: from S.-W. Lee & H. Jeong, arXiv:1304.1214 (2013)

$$|\alpha\rangle|\alpha\rangle \pm |-\alpha\rangle|-\alpha\rangle \xrightarrow{\text{BS}} \left(\left|\sqrt{2}\alpha\right\rangle \pm \left|-\sqrt{2}\alpha\right\rangle\right)|0\rangle$$

$$|\alpha\rangle|-\alpha\rangle \pm |-\alpha\rangle|\alpha\rangle \xrightarrow{\text{BS}} |0\rangle\left(\left|\sqrt{2}\alpha\right\rangle \pm \left|-\sqrt{2}\alpha\right\rangle\right)$$

Interpreting the BSM result

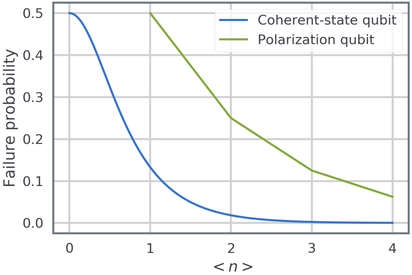
$$(\text{even}, 0): \ |\phi_+\rangle \qquad (0, \text{even}): \ |\psi_+\rangle$$
$$(\text{odd}, 0): \ |\phi_-\rangle \qquad (0, \text{odd}): \ |\psi_-\rangle$$

Coherent-state qubit (cont.)

Properties of coherent-state qubit

- Less failure probability of Bell-state measurement than the case of polarization qubit of same photon number. Average failure probability p_{fail} is:

$$p_{fail} = \frac{e^{-2|\alpha|^2}}{1 + e^{-4|\alpha|^2}}$$

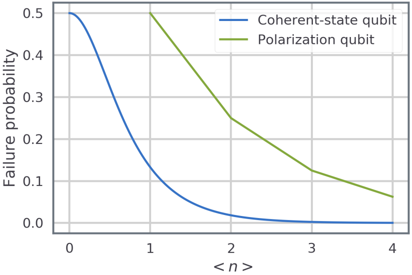


Coherent-state qubit (cont.)

Properties of coherent-state qubit

- Less failure probability of Bell-state measurement than the case of polarization qubit of same photon number. Average failure probability p_{fail} is:

$$p_{fail} = \frac{e^{-2|\alpha|^2}}{1 + e^{-4|\alpha|^2}}$$



- By photon loss, it does not jump into the orthogonal space, but loses coherence (dephasing).

$$|\alpha\rangle\langle\alpha| \rightarrow |\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|$$
$$|\alpha\rangle\langle-\alpha| \rightarrow e^{-2(1-\eta)|\alpha|^2} |\sqrt{\eta}\alpha\rangle\langle-\sqrt{\eta}\alpha|$$

Table of Contents

BSM of coherent-state qubits in lossy environment

Photon loss model

- Considering photon-loss model by
  - the Master equation under the Born-Markov approximation with the zero-temperature,

$$\frac{\partial \rho}{\partial \tau} = \gamma \sum_{i=1}^{N} \left(\hat{a}_i \rho \hat{a}_i^\dagger - \frac{1}{2} \hat{a}_i^\dagger \hat{a}_i \rho - \frac{1}{2} \rho \hat{a}_i^\dagger \hat{a}_i \right)$$

  - or equivalently beam splitter model where the system is mixed with vacuum state by beam splitter, $(\eta = e^{-\gamma\tau/2})$

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \rightarrow \begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}.$$

- Basis states of coherent-state qubit and their cross term transform as:

$$|\alpha\rangle\langle\alpha| \rightarrow |\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|, \quad |\alpha\rangle\langle-\alpha| \rightarrow e^{-2\left(1-\sqrt{\eta}^2\right)|\alpha|^2} |\sqrt{\eta}\alpha\rangle\langle-\sqrt{\eta}\alpha|,$$

where η is the survival rate of photons.

Ref) S. M. Barnett & P. M. Radmore, *Methods in Theoretical Quantum Optics*, Clarendon Press (1997).

Modified Bell-state measurement scheme

Let

- $\{\Pi_x : x \in \{0,1,2\}\}$: orthogonal projectors s.t.
  - $\Pi_0 := |0_\mathrm{F}\rangle\langle 0_\mathrm{F}|$
  - $\Pi_1 := \sum_{n:\mathrm{odd}} |n_\mathrm{F}\rangle\langle n_\mathrm{F}|$
  - $\Pi_2 := \sum_{n\neq 0:\mathrm{even}} |n_\mathrm{F}\rangle\langle n_\mathrm{F}|$

  ($|n_\mathrm{F}\rangle$: a Fock state with n photon numbers)
- $\Pi_{x,y} := \Pi_x \otimes \Pi_y$ where $x, y \in \{0,1,2\}$
- Λ_η: Photon loss channel with survival rate η
- $\Lambda_{\eta_1,\eta_2} := \Lambda_{\eta_1} \otimes \Lambda_{\eta_2}$
- $\mathcal{U}_\mathrm{BS}$: Unitary channel corresponding to a beam splitter

POVM elements of Bell-state measurement in lossy environment

Positive-operator valued measure (POVM) elements $\{M_{x,y}\}_{x,y}$ where $x, y \in \{0,1,2\}$ are defined as

$$M_{x,y} := \left(\mathcal{U}_\mathrm{BS} \circ \Lambda_{\eta_1,\eta_2}\right)^\dagger (\Pi_{x,y}),$$

Then

$$\mathbf{Pr}\,(x, y \,|\, \rho) = \mathrm{Tr}\left[\Pi_{x,y} \left(\mathcal{U}_\mathrm{BS} \circ \Lambda_{\eta_1,\eta_2}\right)(\rho)\right] = \mathrm{Tr}\left(M_{x,y}\rho\right)$$

Modified Bell-state measurement scheme (cont.)
Assuming preceding photon loss model, matrix elements of each POVM element $M_{x,y}$ is calculated as:

$$\begin{aligned}
\langle\phi_\pm| M_{x,y} |\phi_\pm\rangle &= c_\pm \left[1 \pm (-1)^{x+y} e^{-2(2-\eta_1-\eta_2)|\alpha|^2}\right] f_x(\eta_+) f_y(\eta_-) \\
\langle\psi_\pm| M_{x,y} |\psi_\pm\rangle &= c_\pm \left[1 \pm (-1)^{x+y} e^{-2(2-\eta_1-\eta_2)|\alpha|^2}\right] f_x(\eta_-) f_y(\eta_+) \\
\langle\phi_\pm| M_{x,y} |\psi_\pm\rangle &= c_\pm \left[\pm(-1)^{x+y} e^{-2(1-\eta_1)|\alpha|^2} + e^{-2(1-\eta_2)|\alpha|^2}\right] \\
&\qquad \times f_x\left(\sqrt{\eta_+\eta_-}\right) f_y\left(\sqrt{\eta_+\eta_-}\right) \\
\langle\phi_+| M_{x,y} |\psi_-\rangle &= \langle\psi_+| M_{x,y} |\psi_-\rangle = \langle\phi_\pm| M_{x,y} |\psi_\mp\rangle = 0
\end{aligned}$$

where

$$c_\pm := \frac{1}{1 \pm e^{-4|\alpha|^2}}, \quad f_i(\eta) := \begin{cases} 1 & \text{if } i = 0 \\ \sinh\left(\eta|\alpha|^2\right) & \text{if } i = 1 \\ \cosh\left(\eta|\alpha|^2\right) - 1 & \text{if } i = 2 \end{cases}, \quad \eta_\pm := \frac{\left(\sqrt{\eta_1} \pm \sqrt{\eta_2}\right)^2}{2}$$

BSM of coherent-state qubits in lossy environment (cont.)

Modified Bell-state measurement scheme (cont.)

From the measurement result (x, y), assuming equal prior probability of each Bell state, choose a Bell state $|B\rangle \in \mathcal{B} = \{|\phi_+\rangle, |\phi_-\rangle, |\psi_+\rangle, |\psi_-\rangle\}$ which maximize

$$\mathbf{Pr}(B \mid x, y) = \frac{\mathbf{Pr}(x, y \mid B)\,\mathbf{Pr}(B)}{\sum_{|B'\rangle \in \mathcal{B}} \mathbf{Pr}(x, y \mid B)\,\mathbf{Pr}(B)} \propto \mathbf{Pr}(x, y \mid B) = \langle B| M_{x,y} |B\rangle$$

$$\Rightarrow |B\rangle = \operatorname{argmax}_{|B'\rangle \in \mathcal{B}} \langle B'| M_{x,y} |B'\rangle$$

BSM of coherent-state qubits in lossy environment (cont.)

Modified Bell-state measurement scheme (cont.)

From the measurement result (x, y), assuming equal prior probability of each Bell state, choose a Bell state $|B\rangle \in \mathcal{B} = \{|\phi_+\rangle, |\phi_-\rangle, |\psi_+\rangle, |\psi_-\rangle\}$ which maximize

$$\mathbf{Pr}(B \,|\, x, y) = \frac{\mathbf{Pr}(x, y \,|\, B)\,\mathbf{Pr}(B)}{\sum_{|B'\rangle\in\mathcal{B}} \mathbf{Pr}(x, y \,|\, B)\,\mathbf{Pr}(B)} \propto \mathbf{Pr}(x, y \,|\, B) = \langle B| M_{x,y} |B\rangle$$

$$\Rightarrow |B\rangle = \mathrm{argmax}_{|B'\rangle\in\mathcal{B}} \langle B'| M_{x,y} |B'\rangle$$

By simple analysis, one can show the following result.
($M_{x,y}^{B} := \langle B| M_{x,y} |B\rangle$ for simplicity.)

$$\begin{cases} M_{x,y}^{\phi_+(\psi_+)} > M_{x,y}^{\phi_-(\psi_-)} & \text{if } x+y\text{: even} \\ M_{x,y}^{\phi_+(\psi_+)} < M_{x,y}^{\phi_-(\psi_-)} & \text{if } x+y\text{: odd} \end{cases}$$

$$\begin{cases} M_{x,y}^{\phi_\pm} > M_{x,y}^{\psi_\pm} & \text{if } x > y \\ M_{x,y}^{\phi_\pm} < M_{x,y}^{\psi_\pm} & \text{if } x < y \\ M_{x,y}^{\phi_\pm} = M_{x,y}^{\psi_\pm} & \text{if } x = y \end{cases}$$

$x \setminus y$	0	1	2
0	ϕ_+/ψ_+	ψ_-	ψ_+
1	ϕ_-	ϕ_+/ψ_+	ψ_-
2	ϕ_+	ϕ_-	ϕ_+/ψ_+

Table: Interpreting measurement results.

BSM of coherent-state qubits in lossy environment (cont.)

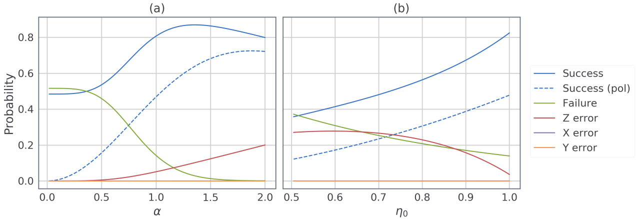
Success, failure, and error probs. of BSM

- Assume equal prior probs. for four Bell states.
- Possible errors
  - X error: Symbol flip ($\phi \leftrightarrow \psi$)
  - Z error: Sign flip ($+ \leftrightarrow -$)
  - Y error: Both symbol and sign flip
  - SND (or failure): Symbol is not determinable. ($x = y$)

BSM of coherent-state qubits in lossy environment (cont.)

Success, failure, and error probs. of BSM

- Assume equal prior probs. for four Bell states.
- Possible errors
  - X error: Symbol flip ($\phi \leftrightarrow \psi$)
  - Z error: Sign flip ($+ \leftrightarrow -$)
  - Y error: Both symbol and sign flip
  - SND (or failure): Symbol is not determinable. ($x = y$)
- Set $\eta_1 := \eta_0$, $\eta_2 := \eta_0 e^{-L_0/L_{att}}$
  - $L_0 = 1$ km and $L_{att} = 22$ km
  - Both systems suffer internal loss with survival rate of η_0.
  - Photons of second system travel distance of L_0.
- SND and Z error are much more probable then X and Y errors
  - $p_X, p_Y \lesssim 10^{-4}$.



Parity encoding using coherent-state qubits

Modified parity encoding for coherent-state qubits

$$|0_L(1_L)\rangle := \left[N^{(m)}\left\{(|\alpha\rangle + |-\alpha\rangle)^{\otimes m} \pm (|\alpha\rangle - |-\alpha\rangle)^{\otimes m}\right\}\right]^{\otimes n}$$

Basis of each level

- Logical level
  $|0_L\rangle$, $|1_L\rangle \rightarrow |\Phi_\pm\rangle$, $|\Psi_\pm\rangle$
- Block level
  $\left|\pm^{(m)}\right\rangle := N^{(m)}\left\{(|\alpha\rangle + |-\alpha\rangle)^{\otimes m} \pm (|\alpha\rangle - |-\alpha\rangle)^{\otimes m}\right\} \rightarrow \left|\phi_\pm^{(m)}\right\rangle, \left|\psi_\pm^{(m)}\right\rangle$
- Physical level
  $|\pm\alpha\rangle \rightarrow |\phi_\pm\rangle$, $|\psi_\pm\rangle$

Parity encoding using coherent-state qubits (cont.)

Decomposition of Bell states

- Logical level → Block level

$$\left|\Phi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\leq n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\phi_-^{(m)}\right\rangle^{\otimes j} \left|\phi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\leq n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\psi_-^{(m)}\right\rangle^{\otimes j} \left|\psi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

where

$$C_\pm^{(m)} = \sqrt{2}\left[1 \pm \left\{\frac{\left(1+e^{-2|\alpha|^2}\right)^m - \left(1-e^{-2|\alpha|^2}\right)^m}{\left(1+e^{-2|\alpha|^2}\right)^m + \left(1-e^{-2|\alpha|^2}\right)^m}\right\}^2\right]^{1/2}$$

- Block level → Physical level

$$\left|\phi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{even}\leq m} \mathcal{P}\left[\left|\psi_\pm\right\rangle^{\otimes k} \left|\phi_\pm\right\rangle^{\otimes m-k}\right]$$

$$\left|\psi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{odd}\leq m} \mathcal{P}\left[\left|\psi_\pm\right\rangle^{\otimes k} \left|\phi_\pm\right\rangle^{\otimes m-k}\right]$$

Naïve Bell-state measurement scheme

Logical level (BSM_2)

$$\left|\Phi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\leq n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\phi_-^{(m)}\right\rangle^{\otimes j} \left|\phi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\leq n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\psi_-^{(m)}\right\rangle^{\otimes j} \left|\psi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

- Symbol: by majority vote of symbols of block Bell states
- Sign: by parity of the number of block Bell states with minus sign

Naïve Bell-state measurement scheme

Logical level (BSM$_2$)

$$\left|\Phi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\le n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\phi_-^{(m)}\right\rangle^{\otimes j} \left|\phi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

$$\left|\Psi_{+(-)}\right\rangle = N_2^{(n)} \sum_{j=\text{even(odd)}\le n} \left(C_-^{(m)}\right)^j \left(C_+^{(m)}\right)^{n-j} \mathcal{P}\left[\left|\psi_-^{(m)}\right\rangle^{\otimes j} \left|\psi_+^{(m)}\right\rangle^{\otimes n-j}\right]$$

- Symbol: by majority vote of symbols of block Bell states
- Sign: by parity of the number of block Bell states with minus sign

Block level (BSM$_1$)

$$\left|\phi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{even}\le m} \mathcal{P}\left[\left|\psi_\pm\right\rangle^{\otimes k} \left|\phi_\pm\right\rangle^{\otimes m-k}\right]$$

$$\left|\psi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{odd}\le m} \mathcal{P}\left[\left|\psi_\pm\right\rangle^{\otimes k} \left|\phi_\pm\right\rangle^{\otimes m-k}\right]$$

- Symbol: by parity of the number of physical Bell states with ψ symbol
- Sign: by majority vote of signs of physical Bell states

Naïve Bell-state measurement scheme (cont.)

Physical level ($\mathbf{BSM_0}$)

- Sign: Always determinable.
- Symbol: Not determinable if $x = y$.

$x \setminus y$	0	1	2
0	ϕ_+/ψ_+	ψ_-	ψ_+
1	ϕ_-	ϕ_+/ψ_+	ψ_-
2	ϕ_+	ϕ_-	ϕ_+/ψ_+

Naïve Bell-state measurement scheme (cont.)

Physical level (BSM_0)

- Sign: Always determinable.
- Symbol: Not determinable if $x = y$.

$x \setminus y$	0	1	2
0	ϕ_+/ψ_+	ψ_-	ψ_+
1	ϕ_-	ϕ_+/ψ_+	ψ_-
2	ϕ_+	ϕ_-	ϕ_+/ψ_+

Overall

- Sign of a Bell state of each level: Always determinable, if m is an odd number.
  - Block level (BSM_1): Majority vote of signs of BSM_0 always gives result, if m is an odd number.
  - Logical level (BSM_2): The number of BSM_1 giving minus sign is well-defined.
- Symbol of a Bell state of each level: Not always determinable. If symbol is not determinable, it is called 'SND' for physical/block level, and 'failure' for logical level.
  - Block level (BSM_1): If at least one BSM_0 is SND, we cannot determine the parity of the number of BSM_0 giving ψ symbol, so the BSM_1 is also SND.
  - Logical level (BSM_2): We can perform majority vote of symbols of BSM_1 excluding SND BSM_1. If all BSM_1s are SND, or majority vote fails, the BSM_2 is SND.

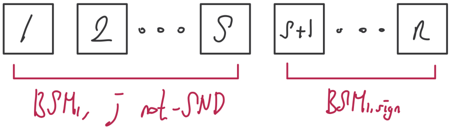
Bell-state measurement scheme with optimized cost

- Cost of concatenated BSM: Number of physical BSMs for one logical BSM.
- Naïve Bell-state measurement scheme have cost nm. How to optimize the cost?

Bell-state measurement scheme with optimized cost (cont.)

Logical level (BSM_2)

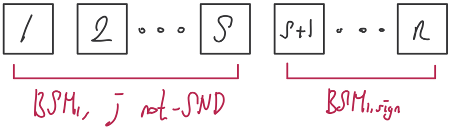
- Scheme
  - Perform BSM_1s until we have j BSM_1s which is not SND.
  - After that, perform $BSM_{1,\mathrm{sign}}$s for left block states, which determine only sign of a block Bell-state.



Bell-state measurement scheme with optimized cost (cont.)

Logical level (BSM_2)

- Scheme
  - Perform BSM_1s until we have j BSM_1s which is not SND.
  - After that, perform $BSM_{1,\mathrm{sign}}$s for left block states, which determine only sign of a block Bell-state.

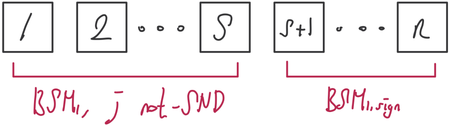


- Interpreting the results
  - Symbol: by majority vote among j not-SND BSM_1s.
  - Sign: by parity of the number of block Bell states with minus sign determined by BSM_1s and $BSM_{1,\mathrm{sign}}$s.

Bell-state measurement scheme with optimized cost (cont.)

Logical level (BSM_2)

- Scheme
  - Perform BSM_1s until we have *j* BSM_1s which is not SND.
  - After that, perform $\mathrm{BSM}_{1,\mathrm{sign}}$s for left block states, which determine only sign of a block Bell-state.

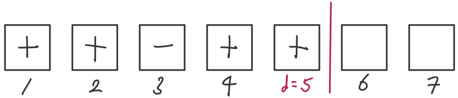


- Interpreting the results
  - Symbol: by majority vote among *j* not-SND BSM_1s.
  - Sign: by parity of the number of block Bell states with minus sign determined by BSM_1s and $\mathrm{BSM}_{1,\mathrm{sign}}$s.
- Since we expect X error (symbol flip error) is much less likely than Z error (sign flip error), majority vote among only *j* not-SND BSM_1s would be enough.

Bell-state measurement scheme with optimized cost (cont.)

Block level (BSM_1)

- d: Index of BSM_0
  $\rightarrow$ Enough to determine the sign of block Bell state.



Bell-state measurement scheme with optimized cost (cont.)

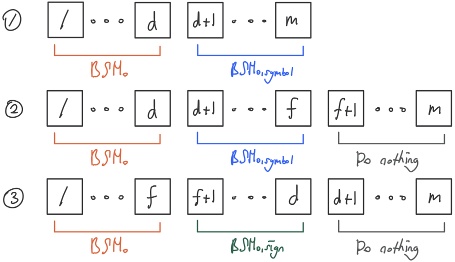
Block level (BSM_1)

- *d*: Index of BSM_0
  $\rightarrow$ Enough to determine the sign of block Bell state.
- *f*: Index of first SND BSM_0, if exists.

Bell-state measurement scheme with optimized cost (cont.)

Block level (BSM_1)

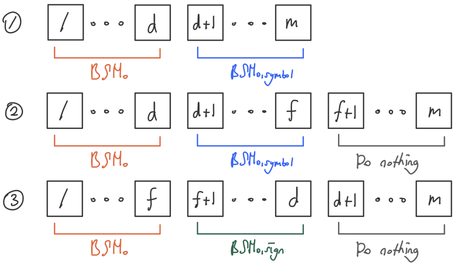
- *d*: Index of BSM_0
  → Enough to determine the sign of block Bell state.
- *f*: Index of first SND BSM_0, if exists.



Bell-state measurement scheme with optimized cost (cont.)

Block level (BSM_1)

- d: Index of BSM_0
  $\rightarrow$ Enough to determine the sign of block Bell state.
- f: Index of first SND BSM_0, if exists.

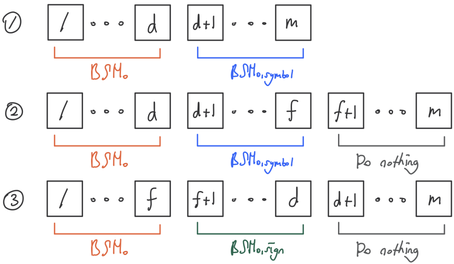


- Sign: Determined by signs of the first d BSM_0s for all cases.

Bell-state measurement scheme with optimized cost (cont.)

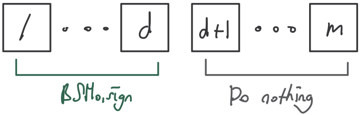
Block level (BSM_1)

- d: Index of BSM_0
  $\rightarrow$ Enough to determine the sign of block Bell state.
- f: Index of first SND BSM_0, if exists.

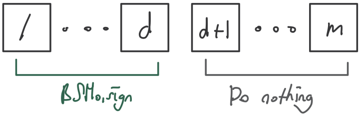


- Sign: Determined by signs of the first d BSM_0s for all cases.
- Symbol:
  - Case 1: Determined by the parity of the number of states with symbol ψ.
  - Case 2 and 3: SND, since the existence of SND BSM_0 makes the parity of the number of ψ states ambiguous.

Block level measuring only sign ($\text{BSM}_{1,\text{sign}}$)

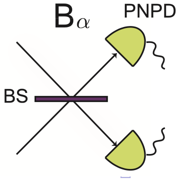


Block level measuring only sign ($\text{BSM}_{1,\text{sign}}$)

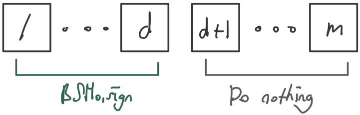


- Sign: Determined by signs of the first d BSM_0s.
- Symbol: No need to be determined

$x \setminus y$	0	1	2
0	ϕ_+/ψ_+	ψ_-	ψ_+
1	ϕ_-	ϕ_+/ψ_+	ψ_-
2	ϕ_+	ϕ_-	ϕ_+/ψ_+



Block level measuring only sign ($\mathrm{BSM}_{1,\mathbf{sign}}$)

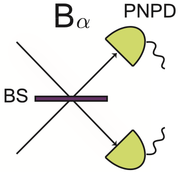


- Sign: Determined by signs of the first d BSM_0s.
- Symbol: No need to be determined

Physical level (BSM_0)

- Currently, BSM_0 and $\mathrm{BSM}_{0,\text{symbol}}$ are same.
- $\mathrm{BSM}_{0,\text{sign}}$
  - Only need to determine the parity of x + y.
  - Need one PNPD instead of two.
  - Assume half amount of contribution to cost than full BSM_0.

$x \setminus y$	0	1	2
0	ϕ_+/ψ_+	ψ_-	ψ_+
1	ϕ_-	ϕ_+/ψ_+	ψ_-
2	ϕ_+	ϕ_-	ϕ_+/ψ_+



Probabilities of specific measurement results

Probabilities of single block Bell-state measurement results

- Want: $\mathbf{Pr}\left(\mathbf{x},\mathbf{y}\,|\,B_1\right)$, where $\mathbf{x},\mathbf{y}\in\{0,1,2,3\}^m$ and $|B_1\rangle\in\mathcal{B}_1 := \left\{\left|\phi_\pm^{(m)}\right\rangle, \left|\psi_\pm^{(m)}\right\rangle\right\}$
- Remind:

$$\mathbf{Pr}\left(x,y\,|\,B_0\right) = \langle B_0|\,M_{x,y}\,|B_0\rangle \quad \text{for } B_0\in\mathcal{B}_0 = \{|\phi_\pm\rangle, |\psi_\pm\rangle\}$$

$$\left|\phi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{even}\le m} \mathcal{P}\left[|\psi_\pm\rangle^{\otimes k}\,|\phi_\pm\rangle^{\otimes m-k}\right]$$

$$\left|\psi_\pm^{(m)}\right\rangle = N_{1\pm}^{(m)} \sum_{k=\text{odd}\le m} \mathcal{P}\left[|\psi_\pm\rangle^{\otimes k}\,|\phi_\pm\rangle^{\otimes m-k}\right]$$

- For $B_1 = \left|\phi_\pm^{(m)}\right\rangle$,

$$\mathbf{Pr}\left(\mathbf{x},\mathbf{y}\,\middle|\,\phi_\pm^{(m)}\right) = \left\langle\phi_\pm^{(m)}\right|\bigotimes_{i=1}^{m} M_{x_i,y_i}\left|\phi_\pm^{(m)}\right\rangle$$

$$= \left(N_{1\pm}^{(m)}\right)^2 \sum_{k,k'=\text{even}\le m} \sum_{\substack{\otimes_{i=1}^m |P_i\rangle\in\text{Perm}\left[|\psi_\pm\rangle^{\otimes k}|\phi_\pm\rangle^{\otimes m-k}\right] \\ \otimes_{i=1}^m |P_i'\rangle\in\text{Perm}\left[|\psi_\pm\rangle^{\otimes k'}|\phi_\pm\rangle^{\otimes m-k'}\right]}} \prod_{i=1}^{m}\langle P_i|\,M_{x_i,y_i}\,|P_i'\rangle$$

$$:= \left(N_{1\pm}^{(m)}\right)^2 \sum_{k,k'=\text{even}\le m} g_\pm(m,k,k',\mathbf{x},\mathbf{y})$$

Probabilities of single block Bell-state measurement results (cont.)

- Recurrence relation of function g (omit $\mathbf{x}$ and $\mathbf{y}$)

$$g_{\pm}(m,k,k') = g_{\pm}(m-1,k,k')M_{11}^{(m)\pm} + \left[g_{\pm}(m-1,k,k'-1) + g_{\pm}(m-1,k-1,k')\right] M_{12}^{(m)\pm} + g_{\pm}(m-1,k-1,k'-1)M_{22}^{(m)\pm}$$

where

$$M_{11}^{(i)\pm} := \langle\phi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\phi_{\pm}\rangle\,,\ M_{12}^{(i)\pm} := \langle\phi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\psi_{\pm}\rangle\,,\ M_{22}^{(i)\pm} := \langle\psi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\psi_{\pm}\rangle\,.$$

- Define $\mathbf{H}_m^{\pm}$

$$\mathbf{H}_m^{\pm} := \begin{pmatrix} \sum_{k,k':\text{even}\leq m} g_{\pm}(m,k,k') & \sum_{\substack{k:\text{even}\leq m \\ k':\text{odd}\leq m}} g_{\pm}(m,k,k') \\ \sum_{\substack{k:\text{odd}\leq m \\ k':\text{even}\leq m}} g_{\pm}(m,k,k') & \sum_{k,k':\text{odd}\leq m} g_{\pm}(m,k,k'). \end{pmatrix}$$

- Recurrence relation of $\tilde{\mathbf{H}}_m^{\pm} := \left(H_{m,11}^{\pm}, H_{m,12}^{\pm}, H_{m,21}^{\pm}, H_{m,22}^{\pm}\right)$

$$\tilde{\mathbf{H}}_m^{\pm} = \begin{pmatrix} M_{11}^{(m)\pm} & M_{12}^{(m)\pm} & M_{12}^{(m)\pm} & M_{22}^{(m)\pm} \\ M_{12}^{(m)\pm} & M_{11}^{(m)\pm} & M_{22}^{(m)\pm} & M_{12}^{(m)\pm} \\ M_{12}^{(m)\pm} & M_{22}^{(m)\pm} & M_{11}^{(m)\pm} & M_{12}^{(m)\pm} \\ M_{22}^{(m)\pm} & M_{12}^{(m)\pm} & M_{12}^{(m)\pm} & M_{11}^{(m)\pm} \end{pmatrix} \tilde{\mathbf{H}}_{m-1}^{\pm} := \tilde{\mathbf{M}}_m^{\pm}\tilde{\mathbf{H}}_{m-1}^{\pm}$$

$$\longrightarrow \tilde{\mathbf{M}}_m^{\pm}\cdots\tilde{\mathbf{M}}_1^{\pm}(1,\ 0,\ 0,\ 0)^T$$

Probabilities of specific measurement results (cont.)

Simple matrix-form expression of $\mathbf{Pr}\left(\mathbf{x},\mathbf{y}\,|\,B_1\right)$

$$\mathbf{Pr}\left(\mathbf{x},\mathbf{y}\,\middle|\,\phi_{\pm}^{(m)}\right) = \left(N_{1\pm}^{(m)}\right)^2 \tilde{H}_{m1}^{\pm}(\mathbf{x},\mathbf{y}),$$

$$\mathbf{Pr}\left(\mathbf{x},\mathbf{y}\,\middle|\,\psi_{\pm}^{(m)}\right) = \left(N_{1\pm}^{(m)}\right)^2 \tilde{H}_{m4}^{\pm}(\mathbf{x},\mathbf{y}),$$

where

$$\tilde{\mathbf{H}}_m^{\pm}(\mathbf{x},\mathbf{y}) = \tilde{\mathbf{M}}_m^{\pm}(\mathbf{x},\mathbf{y})\cdots\tilde{\mathbf{M}}_1(\mathbf{x},\mathbf{y})(1,0,0,0)^T$$

with

$$\tilde{\mathbf{M}}_i^{\pm}(\mathbf{x},\mathbf{y}) = \begin{pmatrix} M_{11}^{(i)\pm} & M_{12}^{(i)\pm} & M_{12}^{(i)\pm} & M_{22}^{(i)\pm} \\ M_{12}^{(i)\pm} & M_{11}^{(i)\pm} & M_{22}^{(i)\pm} & M_{12}^{(i)\pm} \\ M_{12}^{(i)\pm} & M_{22}^{(i)\pm} & M_{11}^{(i)\pm} & M_{12}^{(i)\pm} \\ M_{22}^{(i)\pm} & M_{12}^{(i)\pm} & M_{12}^{(i)\pm} & M_{11}^{(i)\pm} \end{pmatrix}$$

and

$$M_{11}^{(i)\pm} := \langle\phi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\phi_{\pm}\rangle\,,\ M_{12}^{(i)\pm} := \langle\phi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\psi_{\pm}\rangle\,,\ M_{22}^{(i)\pm} := \langle\psi_{\pm}|\,\hat{M}_{x_i,y_i}\,|\psi_{\pm}\rangle\,.$$

Probabilities of specific measurement results (cont.)

Probabilities of logical Bell-state measurement results (cont.)

- Want: $\mathbf{Pr}(\mathbf{X}, \mathbf{Y} \mid B_2)$, where $\mathbf{X}, \mathbf{Y} \in \{0,1,2,3\}^{n \times m}$ and $|B_2\rangle \in \mathcal{B}_2 := \{|\Phi_\pm\rangle, |\Psi_\pm\rangle\}$

Simple matrix-form expression of $\mathbf{Pr}(\mathbf{X}, \mathbf{Y} \mid B_2)$

$$\mathbf{Pr}(\mathbf{X}, \mathbf{Y} \mid \Phi_+) = \left(N_2^{(n)}\right)^2 \tilde{H}_{n1}(\mathbf{X}, \mathbf{Y}),$$

$$\mathbf{Pr}(\mathbf{X}, \mathbf{Y} \mid \Phi_-) = \left(N_2^{(n)}\right)^2 \tilde{H}_{n2}(\mathbf{X}, \mathbf{Y}),$$

where

$$\tilde{\mathbf{H}}_n(\mathbf{X}, \mathbf{Y}) = \tilde{\mathbf{M}}_n(\mathbf{X}, \mathbf{Y}) \cdots \tilde{\mathbf{M}}_1(\mathbf{X}, \mathbf{Y}) \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{with} \quad \tilde{\mathbf{M}}_i(\mathbf{X}, \mathbf{Y}) = \begin{pmatrix} M_{11}^{(i)} & M_{22}^{(i)} \\ M_{22}^{(i)} & M_{11}^{(i)} \end{pmatrix},$$

and

$$M_{11}^{(i)} := \left(C_+^{(m)}\right)^2 \left\langle \phi_+^{(m)} \middle| \hat{M}_B^{(i)} \middle| \phi_+^{(m)} \right\rangle, \ M_{22}^{(i)} := \left(C_-^{(m)}\right)^2 \left\langle \phi_-^{(m)} \middle| \hat{M}_B^{(i)} \middle| \phi_-^{(m)} \right\rangle, \quad \text{and} \quad \hat{M}_B^{(i)} = \bigotimes_{j=1}^{m} \hat{M}_{X_{ij}, Y_{ij}}$$

Table of Contents

Methods for Monte-Carlo simulation

- Parameters: n, m, α, η_1, η_2, j
- We tried Monte-Carlo simulation, which randomly samples results and counts the number of success or error.

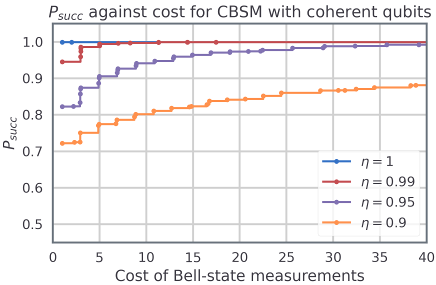
Randomly sampling measurement results

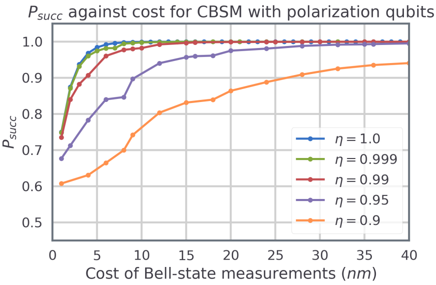
- Assume a prior distribution for four logical Bell states $\mathcal{B}_2 = \{\Phi_\pm, \Psi_\pm\}$.
- Need to sample nm BSM_0 measurement results, each of which gives (x, y) where $x, y \in \{0, 1, 2\} \longrightarrow x_{11}, y_{11}, \cdots, x_{nm}, y_{nm}$
- Sample each BSM_0 measurement result one by one with conditional probability where $B_2 \in \mathcal{B}_2$:

$$\mathbf{Pr}\left(x_{pq}, y_{pq} \,|\, x_{11}, y_{11}, \cdots, x_{p,q-1}, y_{p,q-1}; B_2\right) \propto \mathbf{Pr}\left(x_{11}, y_{11}, \cdots, x_{p,q}, y_{p,q} \,|\, B_2\right)$$

- The conditional probability can be expressed with $\tilde{H}$ we used for matrix-form expression of $\mathbf{Pr}\left(\mathbf{X}, \mathbf{Y} \,|\, B_2\right)$ and $\mathbf{Pr}\left(\mathbf{x}, \mathbf{y} \,|\, B_1\right)$.

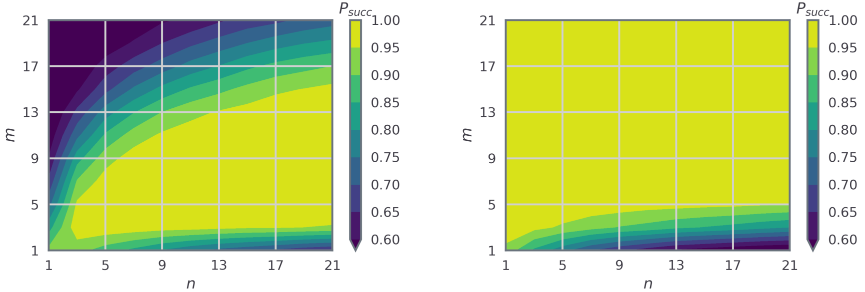
Success probability of single logical CBSM against cost





- $\eta_1 = \eta_2 = \eta$. Optimization of α is taken in range of $\alpha \leq 2$

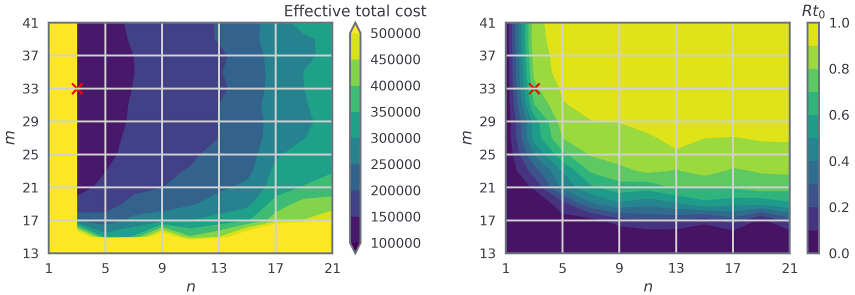
Success probability of single logical CBSM against α



- $\alpha = 1.2$ (left), $\alpha = 1.8$ (right).
- $\eta_1 = \eta_2 = \eta = 0.99$.
- α should be large enough to make efficient CBSM possible.

Simulation results (cont.)

Key generation rate R for quantum key distribution

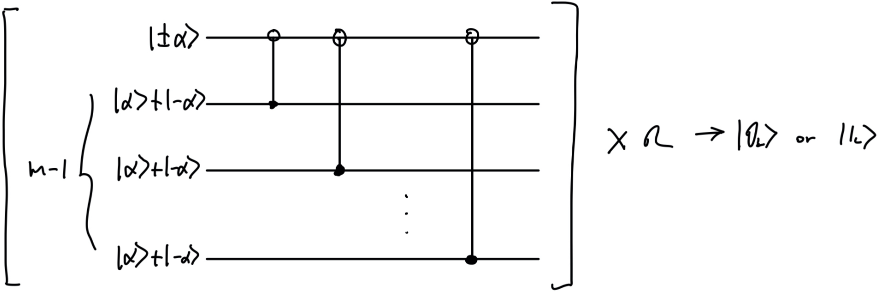


- Effective total cost optimizing for α, L_0, and j, when $L = 1000$ km.
- Rt_0 optimizing for α and j, when $L_0 = 0.8$ km and $L = 1000$ km.
- Effective total cost $C_{tot} = C_{BSM}\left(\frac{L}{L_0}\right)/(Rt_0)$
- Optimal at $n = 3,\ m = 33,\ \alpha = 1.95,\ L_0 = 0.75km,\ j = 1.$
  $C_{tot} = (1.00 \pm 0.01) \times 10^5$.

Table of Contents

Implementation of the scheme

Preparation of $|0_L\rangle$ and $|1_L\rangle$



Implementation of the scheme

CNOT gate

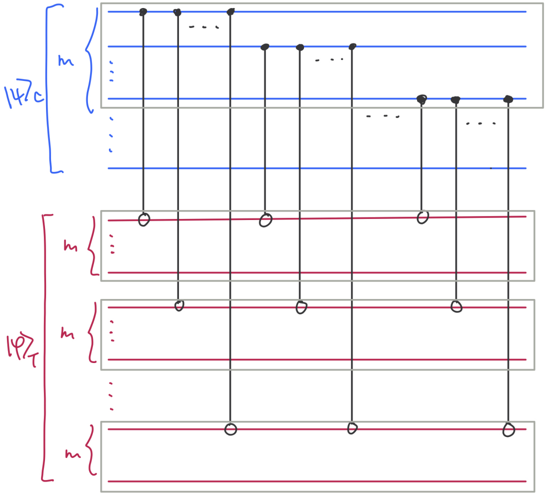


Table of Contents

Conclusion

- We investigated Bell-state measurement scheme with coherent-state qubits in lossy environment.
- We suggested parity encoding scheme using coherent-state qubits and concatenated Bell-state measurement (CBSM) scheme with optimized cost.
- We got analytic expressions of probabilities for getting each specific measurement results, and then performed Monte-Carlo simulations for success probabilities and error rates.
- Numerical calculation shows that CBSM with coherent-state can achieve high success probability and high key generation rate $Rt_0 \approx 0.8$. For that to be possible, α should be large enough ($\alpha \gtrapprox 1.2$) and $m \gtrapprox 35$, while n does not affect the performance much.
- However, suggested CBSM protocol with coherent state is not yet good enough compared to CBSM with polarization qubit in S.-W. Lee et al. (2019).
- Future works will include developing $\mathrm{BSM}_{0,symbol}$, simulating for $j \geq 2$, simulating for larger m, and methods to physically realize this CBSM scheme.

Thank you for your attention!