Proof of the main theorem

Theorem

Let C be a Clifford circuit measuring computing Pauli operators $S_1, \ldots, S_r$. Then, for any subset of qubits L, we have

$$depth(C) \geq \frac{n_{cut}}{64|\partial L|}.$$

Corollary

For families of local-expander quantum LDPC codes of length n, a syndrome extraction circuit C implemented as a local Clifford circuit on a $\sqrt{N} \times \sqrt{N}$ grid of qubits satisfies

$$depth(C) \geq \Omega\left(\frac{n}{\sqrt{N}}\right).$$

Strategy

- Partition the circuit's qubits into two subsets L and R.

Strategy

- Partition the circuit's qubits into two subsets L and R.
- Lower bound the amount of correlation required between L and R to measure the Pauli operators.

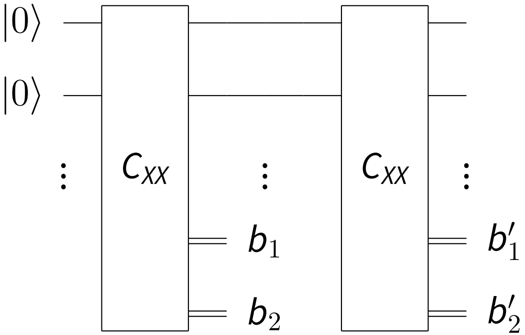
Strategy

- Partition the circuit's qubits into two subsets L and R.
- Lower bound the amount of correlation required between L and R to measure the Pauli operators.
- Upper bound the amount of correlation introduced per operation.

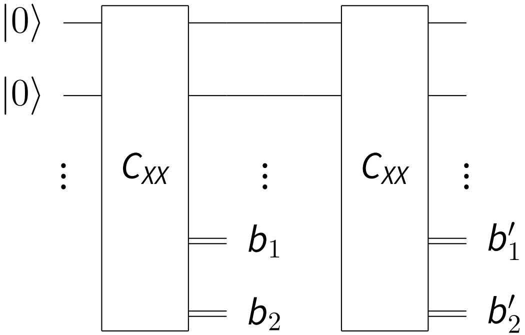
Strategy

- Partition the circuit's qubits into two subsets L and R.
- Lower bound the amount of correlation required between L and R to measure the Pauli operators.
- Upper bound the amount of correlation introduced per operation.
- Combine both arguments to derive a lower bound for the depth of the circuit.

Measuring correlations



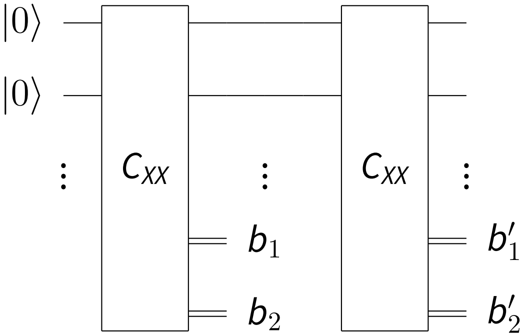
Measuring correlations



Mutual information

$$I(b_1; b_2) = 0$$

Measuring correlations

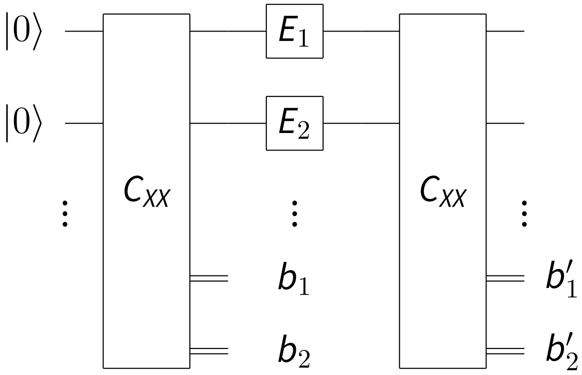


Mutual information

$$I(b_1; b_2) = 0$$

$$I(b'_1; b'_2) = 1$$

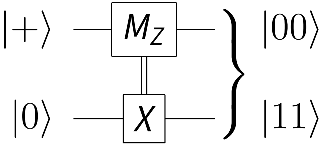
Measuring correlations



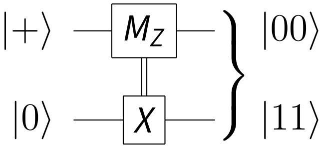
Mutual information

$$I(b'_1, b'_2, E_1; E_2) = 1$$

Measuring correlations



Measuring correlations



Classical operations can artificially boost mutual information.

Measuring correlations

- Build a circuit C' with the same action and similar depth as C by pushing all measurements and classical operations at the end.

Measuring correlations

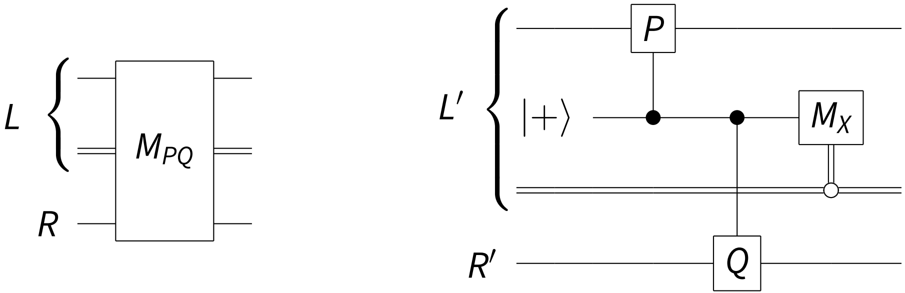
- Build a circuit C' with the same action and similar depth as C by pushing all measurements and classical operations at the end.
- Consider the circuit $C' \circ E \circ C'$.

Measuring correlations

- Build a circuit C' with the same action and similar depth as C by pushing all measurements and classical operations at the end.
- Consider the circuit $C' \circ E \circ C'$.
- Compute the mutual information

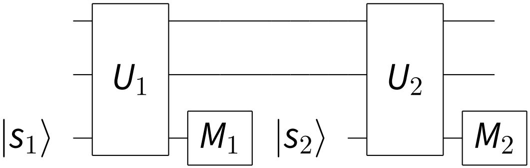
$$I(O_L^{(2)}, E_L; O_R^{(2)}, E_R | O^{(1)}).$$

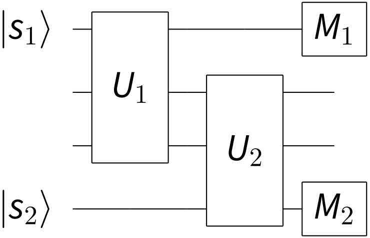
Circuit transformations



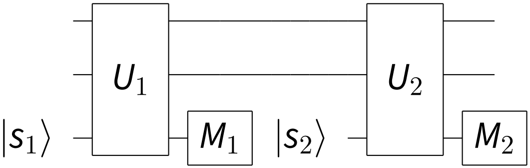
$$\mathrm{depth}(C') \leq 4 \cdot \mathrm{depth}(C) + 2$$

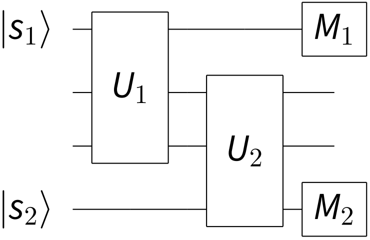
Circuit transformations





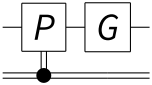
Circuit transformations

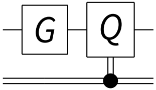




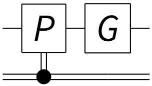
Both ancillas are the same node in the connectivity graph and in the same partition.

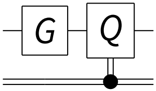
Circuit transformations

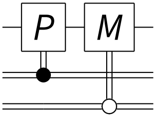


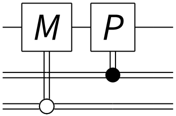


Circuit transformations

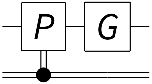


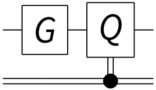


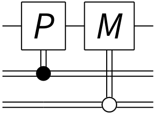


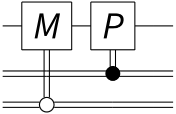


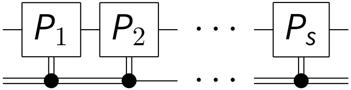
Circuit transformations

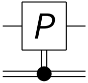




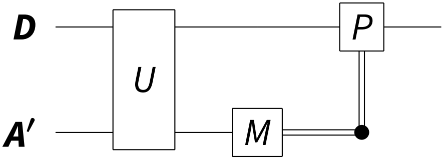




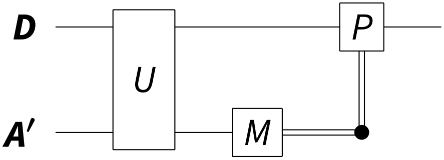




Circuit transformations

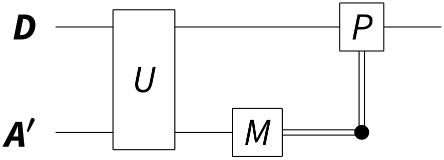


Circuit transformations



$$\mathsf{depth}(U) \leq 4 \cdot \mathsf{depth}(C)$$

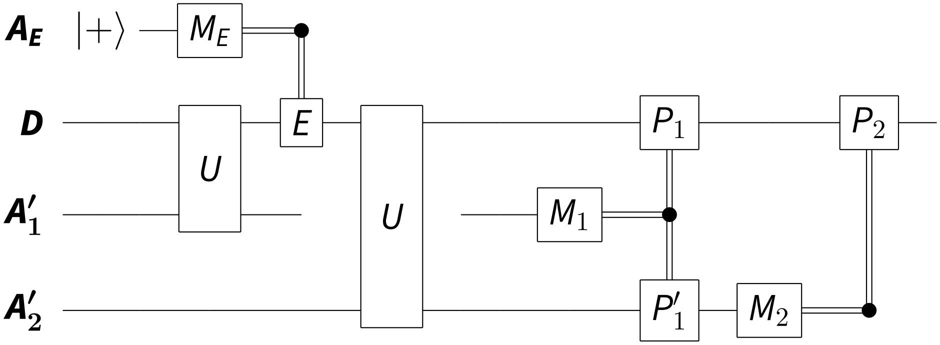
Circuit transformations



$$\mathsf{depth}(U) \leq 4 \cdot \mathsf{depth}(C)$$

$$|\partial L| = |\partial L'|$$

The double measurement circuit



$$I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \text{ with } \bar{L} = L' \cup A_E$$

Bounds on the mutual information

Lower bound

For the double measurement circuit, we have

$$I(O_{\overline{L}}^{(2)}, E_{\overline{L}}; O_{\overline{R}}^{(2)}, E_{\overline{R}} | O^{(1)}) \geq \frac{n_{\text{cut}}}{2}.$$

Bounds on the mutual information

Lower bound

For the double measurement circuit, we have

$$I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \geq \frac{n_{\text{cut}}}{2}.$$

Upper bound

For the double measurement circuit, we have

$$I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \leq 32 |\partial L| \text{depth}(C).$$

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Note $M_{\bar{L}}^{(t)} = \{m_{i,\bar{L}}^{(t)} = \bigoplus_{o \in O_i^{(t)} \cap \bar{L}} o\}$ and similarly for $M_{\bar{R}}^{(t)}$.

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Note $M_{\bar{L}}^{(t)} = \{m_{i,\bar{L}}^{(t)} = \bigoplus_{o \in O_i^{(t)} \cap \bar{L}} o\}$ and similarly for $M_{\bar{R}}^{(t)}$.

From the data processing inequality

$$I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \geq I(M_{\bar{L}}^{(2)}, E_{\bar{L}}; M_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)})$$

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Note $M_{\bar{L}}^{(t)} = \{m_{i,\bar{L}}^{(t)} = \bigoplus_{o \in O_i^{(t)} \cap \bar{L}} o\}$ and similarly for $M_{\bar{R}}^{(t)}$.

From the data processing inequality

$$\begin{aligned} I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) &\geq I(M_{\bar{L}}^{(2)}, E_{\bar{L}}; M_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \\ &= H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | O^{(1)}) - H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | M_{\bar{R}}^{(2)}, E_{\bar{R}}, O^{(1)}) \end{aligned}$$

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Note $M_{\bar{L}}^{(t)} = \{m_{i,\bar{L}}^{(t)} = \bigoplus_{o \in O_i^{(t)} \cap \bar{L}} o\}$ and similarly for $M_{\bar{R}}^{(t)}$.

From the data processing inequality

$$\begin{aligned} I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) &\geq I(M_{\bar{L}}^{(2)}, E_{\bar{L}}; M_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \\ &= H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | O^{(1)}) - H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | M_{\bar{R}}^{(2)}, E_{\bar{R}}, O^{(1)}) \\ &= H(M_{\bar{L}}^{(2)}, E_{\bar{L}}, O^{(1)}) - H(O^{(1)}) - H(E_{\bar{L}}) \end{aligned}$$

Proof of the lower bound

Note $m_i^{(t)} = \bigoplus_{o \in O_i^{(t)}} o$, the outcome for the measurement of S_i in circuit t.

Note $M_{\bar{L}}^{(t)} = \{m_{i,\bar{L}}^{(t)} = \bigoplus_{o \in O_i^{(t)} \cap \bar{L}} o\}$ and similarly for $M_{\bar{R}}^{(t)}$.

From the data processing inequality

$$
\begin{aligned}
I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) &\geq I(M_{\bar{L}}^{(2)}, E_{\bar{L}}; M_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \\
&= H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | O^{(1)}) - H(M_{\bar{L}}^{(2)}, E_{\bar{L}} | M_{\bar{R}}^{(2)}, E_{\bar{R}}, O^{(1)}) \\
&= H(M_{\bar{L}}^{(2)}, E_{\bar{L}}, O^{(1)}) - H(O^{(1)}) - H(E_{\bar{L}}) \\
&= H(M_{\bar{L}}^{(2)} | E_{\bar{L}}, O^{(1)}).
\end{aligned}
$$

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\mathrm{cut},\bar{L}}$ the operators $S_i \in S_{\mathrm{cut}}$ for which m_i depends on at least one outcome in O_L.

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\text{cut},\bar{L}}$ the operators $S_i \in S_{\text{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M_{\bar{L},\text{cut}}^{(t)}$ the outcome of $M_{\bar{L}}^{(t)}$ corresponding to $S_{\text{cut},\bar{L}}$.

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\text{cut},\bar{L}}$ the operators $S_i \in S_{\text{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M^{(t)}_{\bar{L},\text{cut}}$ the outcome of $M^{(t)}_{\bar{L}}$ corresponding to $S_{\text{cut},\bar{L}}$.

From the data processing inequality

$$H(M^{(2)}_{\bar{L}}|E_{\bar{L}}, O^{(1)}) \geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)})$$

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\text{cut},\bar{L}}$ the operators $S_i \in S_{\text{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M^{(t)}_{\bar{L},\text{cut}}$ the outcome of $M^{(t)}_{\bar{L}}$ corresponding to $S_{\text{cut},\bar{L}}$.

From the data processing inequality

$$
\begin{aligned}
H(M^{(2)}_{\bar{L}}|E_{\bar{L}}, O^{(1)}) &\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}) \\
&\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}})
\end{aligned}
$$

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\text{cut},\bar{L}}$ the operators $S_i \in S_{\text{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M^{(t)}_{\bar{L},\text{cut}}$ the outcome of $M^{(t)}_{\bar{L}}$ corresponding to $S_{\text{cut},\bar{L}}$.

From the data processing inequality

$$
\begin{aligned}
H(M^{(2)}_{\bar{L}}|E_{\bar{L}}, O^{(1)}) &\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}) \\
&\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}}) \\
&= H(m_i(E_{\bar{R}}) \;:\; S_i \in S_{\text{cut},\bar{L}}|E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}})
\end{aligned}
$$

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\text{cut},\bar{L}}$ the operators $S_i \in S_{\text{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M^{(t)}_{\bar{L},\text{cut}}$ the outcome of $M^{(t)}_{\bar{L}}$ corresponding to $S_{\text{cut},\bar{L}}$.

From the data processing inequality

$$\begin{aligned} H(M^{(2)}_{\bar{L}}|E_{\bar{L}}, O^{(1)}) &\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}) \\ &\geq H(M^{(2)}_{\bar{L},\text{cut}}|E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}}) \\ &= H(m_i(E_{\bar{R}}) \ : \ S_i \in S_{\text{cut},\bar{L}}|E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}}) \\ &= H(m_i(E_{\bar{R}}) \ : \ S_i \in S_{\text{cut},\bar{L}}) \end{aligned}$$

Proof of the lower bound

Note S_{cut} the operators with support on both L and R.

Note $S_{\mathrm{cut},\bar{L}}$ the operators $S_i \in S_{\mathrm{cut}}$ for which m_i depends on at least one outcome in O_L.

Note $M^{(t)}_{\bar{L},\mathrm{cut}}$ the outcome of $M^{(t)}_{\bar{L}}$ corresponding to $S_{\mathrm{cut},\bar{L}}$.

From the data processing inequality

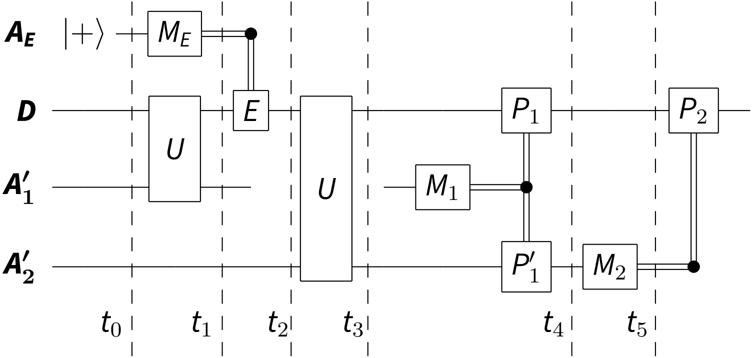
$$\begin{aligned}
H(M^{(2)}_{\bar{L}} | E_{\bar{L}}, O^{(1)}) &\geq H(M^{(2)}_{\bar{L},\mathrm{cut}} | E_{\bar{L}}, O^{(1)}) \\
&\geq H(M^{(2)}_{\bar{L},\mathrm{cut}} | E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}}) \\
&= H(m_i(E_{\bar{R}}) \ : \ S_i \in S_{\mathrm{cut},\bar{L}} | E_{\bar{L}}, O^{(1)}, M^{(2)}_{\bar{R}}) \\
&= H(m_i(E_{\bar{R}}) \ : \ S_i \in S_{\mathrm{cut},\bar{L}}) \\
&= |S_{\mathrm{cut},\bar{L}}|.
\end{aligned}$$

Proof of the lower bound

By symmetry

$$I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)}) \geq \max\{|S_{\mathrm{cut},\bar{L}}|, |S_{\mathrm{cut},\bar{R}}|\} \geq \frac{n_{\mathrm{cut}}}{2}.$$

Proof of the upper bound



$$S_{A_2',A_E}(\rho_{\bar{L}}(t_5);\rho_{\bar{R}}(t_5)) = I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}}) \geq I(O_{\bar{L}}^{(2)}, E_{\bar{L}}; O_{\bar{R}}^{(2)}, E_{\bar{R}} | O^{(1)})$$

Proof of the upper bound

- Given a set of qubits and a partition into subsets A, B. Let ρ be a density matrix on $A \cup B$ and G be a two-qubit unitary gate acting qubit of A and a qubit of B. Note $\rho' = G\rho G^\dagger$, then

$$S(\rho'_A; \rho'_B) \leq S(\rho_A, \rho_B) + 4.$$

- Single qubit gates and measurements are CPTP maps. Thus, they can't increase the mutual entropy.

Mariën et al, Communications in Mathematical Physics, 346(1), 2016

Proof of the upper bound

- Given a set of qubits and a partition into subsets A, B. Let ρ be a density matrix on $A \cup B$ and G be a two-qubit unitary gate acting qubit of A and a qubit of B. Note $\rho' = G\rho G^\dagger$, then

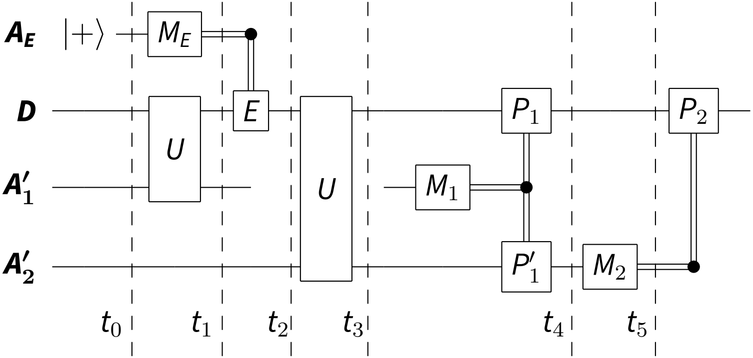
$$S(\rho'_A; \rho'_B) \leq S(\rho_A, \rho_B) + 4.$$

- Single qubit gates and measurements are CPTP maps. Thus, they can't increase the mutual entropy.
- Discarding a subsystem can't increase the mutual entropy.

Mariën et al, Communications in Mathematical Physics, 346(1), 2016

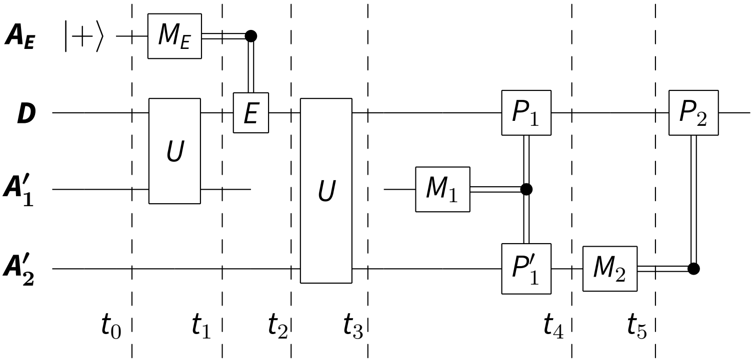
Proof of the upper bound

Proof of the upper bound



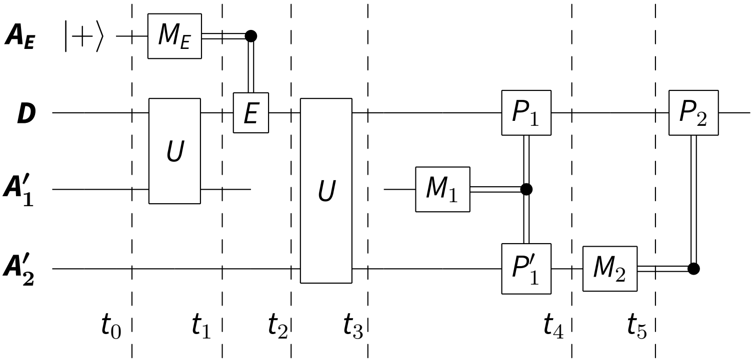
$$S(\rho_{\bar{L}}(t_0); \rho_{\bar{R}}(t_0)) = 0$$

Proof of the upper bound



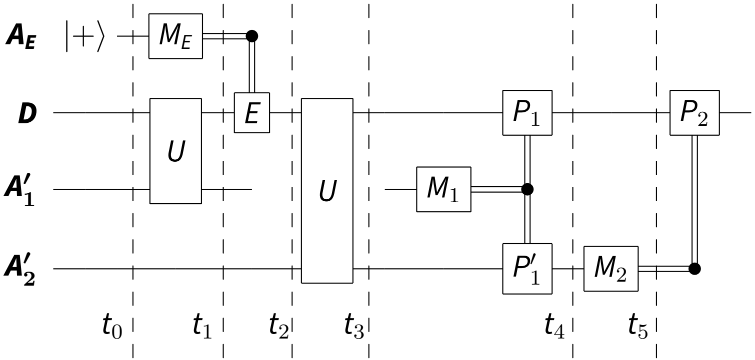
$$S(\rho_{\bar{L}}(t_1); \rho_{\bar{R}}(t_1)) \leq 4\mathrm{depth}(U)|\partial L|$$

Proof of the upper bound



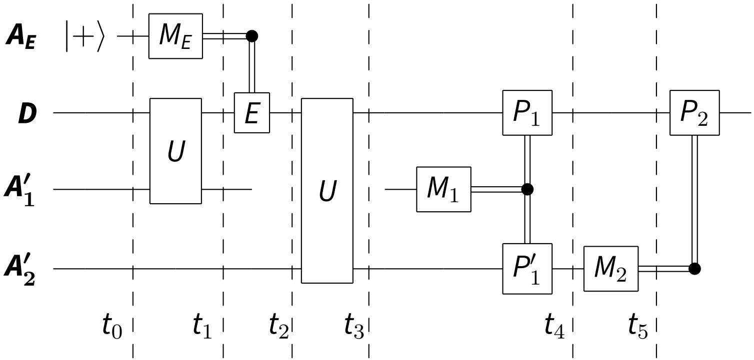
$$S(\rho_{\bar{L}}(t_2); \rho_{\bar{R}}(t_2)) \leq 4\mathrm{depth}(U)|\partial L|$$

Proof of the upper bound



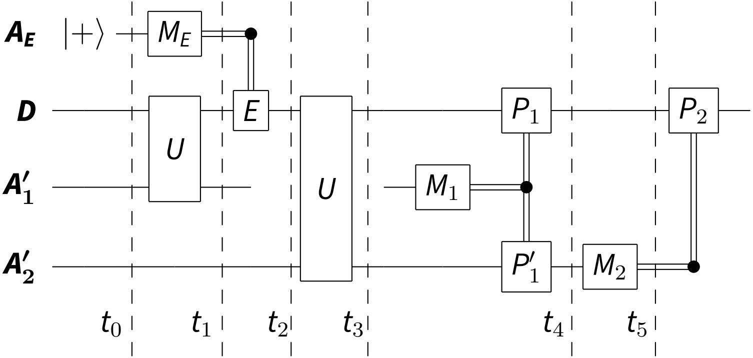
$$S(\rho_{\bar{L}}(t_3);\rho_{\bar{R}}(t_3)) \leq 8\mathrm{depth}(U)|\partial L|$$

Proof of the upper bound



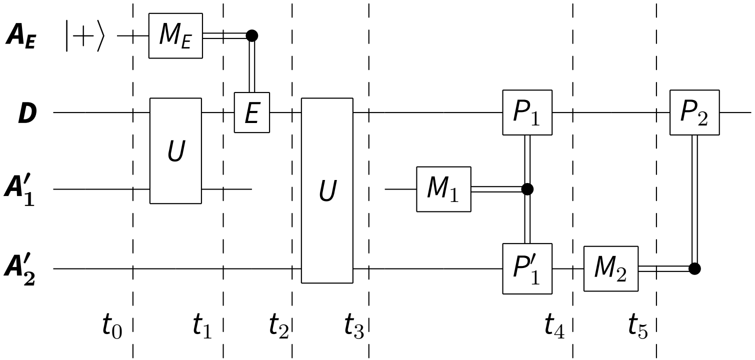
$$S(\rho_{\bar{L}}(t_4); \rho_{\bar{R}}(t_4)) \leq 8\mathrm{depth}(U)|\partial L|$$

Proof of the upper bound



$$S_{A'_2, A_E}(\rho_{\bar{L}}(t_4); \rho_{\bar{R}}(t_4)) \leq 8\,\mathrm{depth}(U)|\partial L|$$

Proof of the upper bound



$$S_{A'_2,A_E}(\rho_{\bar{L}}(t_5);\rho_{\bar{R}}(t_5)) \leq 8\mathrm{depth}(U)|\partial L|$$