Coherence as a Resource for Shor's Algorithm

Felix Ahnefeld*, Thomas Theurer, Dario Egloff, Juan Mauricio Matera, Martin B. Plenio*

*Institute of Theoretical Physics
Ulm University

Quantum Resources 2022

Phys. Rev. Lett. 129, 120501 (2022)

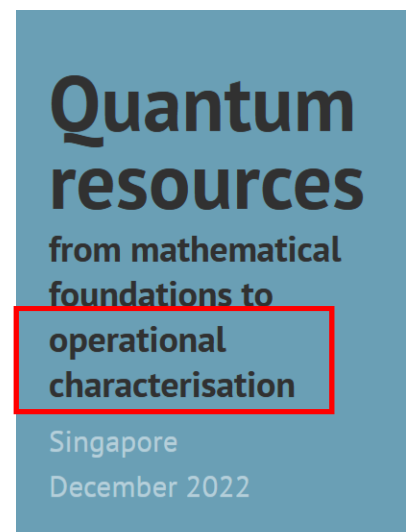
Coherence as a Resource for Shor’s Algorithm

Felix Ahnefeld*, Thomas Theurer, Dario Egloff, Juan Mauricio Matera, Martin B. Plenio*

*Institute of Theoretical Physics
Ulm University

Quantum Resources 2022

Phys. Rev. Lett. 129, 120501 (2022)

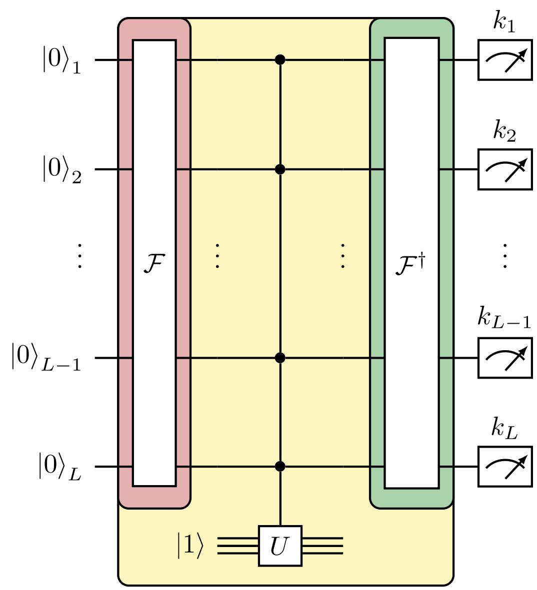


Factoring à la Shor

Factor N via order finding of r: $U^r = \mathbb{1}$

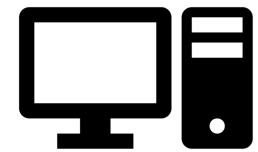
L qubits

$N^2 < 2^L < 2N^2$



Shor, SIAM 26, 5 (1997)

k →

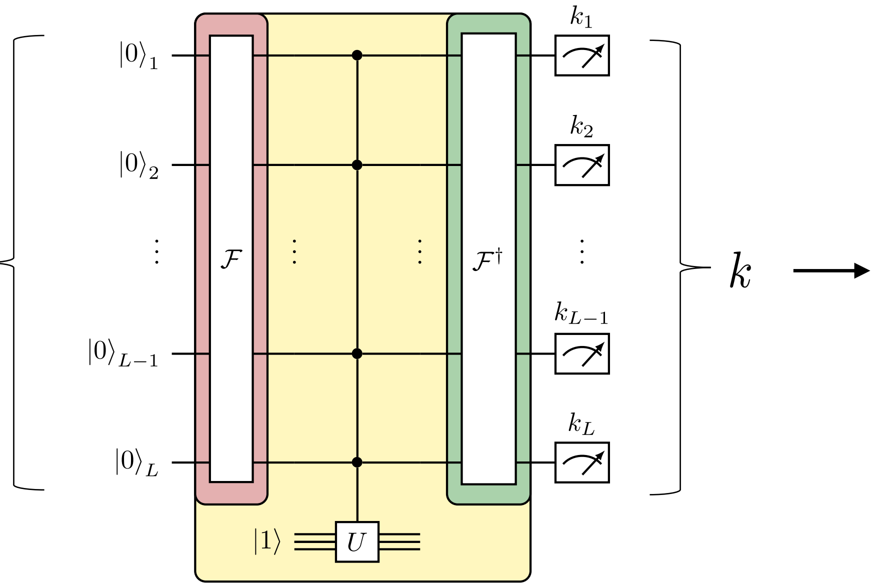


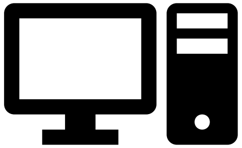
Classical Processing

Factoring à la Shor

Factor N via finding the order r: $U^r = \mathbb{1}$

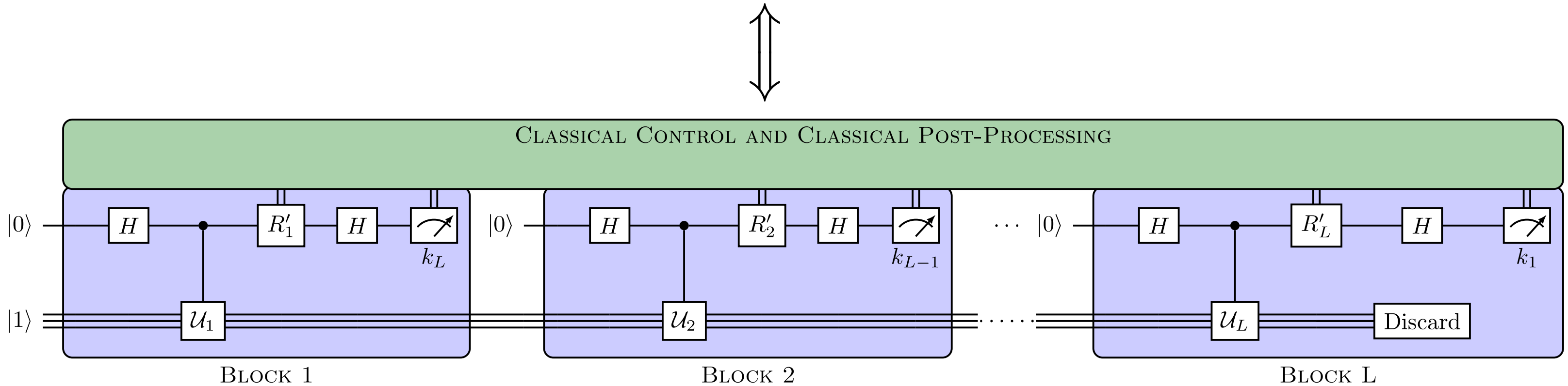
L qubits
$N^2 < 2^L < 2N^2$





Classical Processing

Shor, SIAM 26, 5 (1997)



Griffiths and Niu, PRL 76, 3228 (1996)
Parker and Plenio, PRL 85, 304 (2000)

Coherence

$$\mathcal{N} \in \mathcal{MIO}: \quad \mathcal{N}\Delta = \Delta\mathcal{N}\Delta$$

Åberg, arXiv: 0612146 (2006)
Liu et al, PRL 118, 060502 (2017)
García Díaz et al, Quantum 2, 100 (2018)

Incoherent states $\mathcal{I}$

$$\sigma \in \mathcal{I}: \quad \Delta(\sigma) = \sigma$$

Coherence

Free operations

$$\mathcal{N} \in \mathcal{MIO}: \quad \mathcal{N}\Delta = \Delta\mathcal{N}\Delta$$

Åberg, arXiv: 0612146 (2006)
Liu et al, PRL 118, 060502 (2017)
García Díaz et al, Quantum 2, 100 (2018)

Incoherent states $\mathcal{I}$

$$\sigma \in \mathcal{I}: \quad \Delta(\sigma) = \sigma$$

$$\mathcal{M} \in \mathcal{DI}: \quad \Delta\mathcal{M} = \Delta\mathcal{M}\Delta$$

Liu et al, PRL 118, 060502 (2017)
Theurer et al, PRL 122, 190405 (2019)

Incoherent measurements $\mathcal{IM}$

$$\mathbb{M} \in \mathcal{IM}:$$

$$\mathrm{Tr}\left[M_n \Delta(\rho)\right] = \mathrm{Tr}\left[M_n \rho\right] \quad \forall \rho, M_n$$

Coherence

Free operations

$$\mathcal{N} \in \mathcal{MIO}: \quad \mathcal{N}\Delta = \Delta\mathcal{N}\Delta$$

Åberg, arXiv: 0612146 (2006)
Liu et al, PRL 118, 060502 (2017)
García Díaz et al, Quantum 2, 100 (2018)

Incoherent states $\mathcal{I}$

$$\sigma \in \mathcal{I}: \quad \Delta(\sigma) = \sigma$$

$$\mathcal{M} \in \mathcal{DI}: \quad \Delta\mathcal{M} = \Delta\mathcal{M}\Delta$$

Liu et al, PRL 118, 060502 (2017)
Theurer et al, PRL 122, 190405 (2019)

Incoherent measurements $\mathcal{IM}$

$$\mathbb{M} \in \mathcal{IM}:$$

$$\mathrm{Tr}\left[M_n \Delta(\rho)\right] = \mathrm{Tr}\left[M_n \rho\right] \quad \forall \rho, M_n$$

$$\mathscr{C}(\mathcal{N}) = \max_{\sigma \in \mathcal{I}} C(\mathcal{N}(\sigma))$$

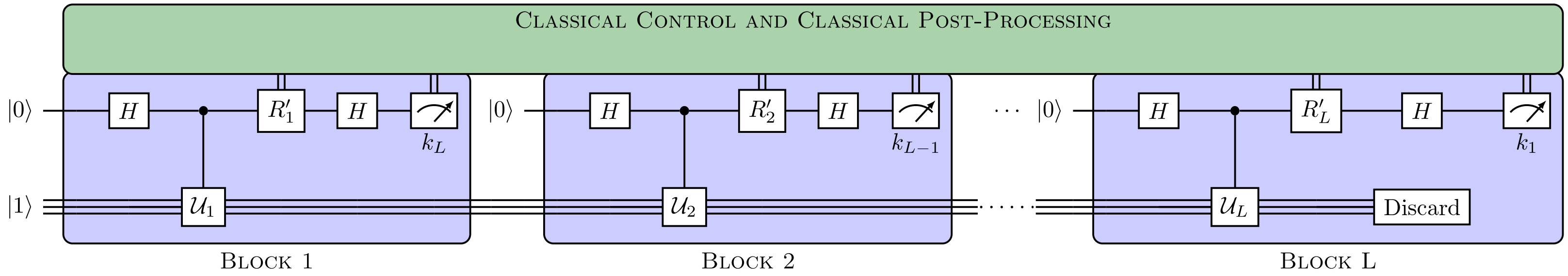
$$C(\rho) = \min_{\tau} \left\{ r \geq 0 \mid \frac{\rho + r\tau}{1+r} \in \mathcal{I} \right\}$$

Vidal and Tarrach, PRA 59, 141 (1999)
Napoli et al, PRL 116, 150502 (2016)

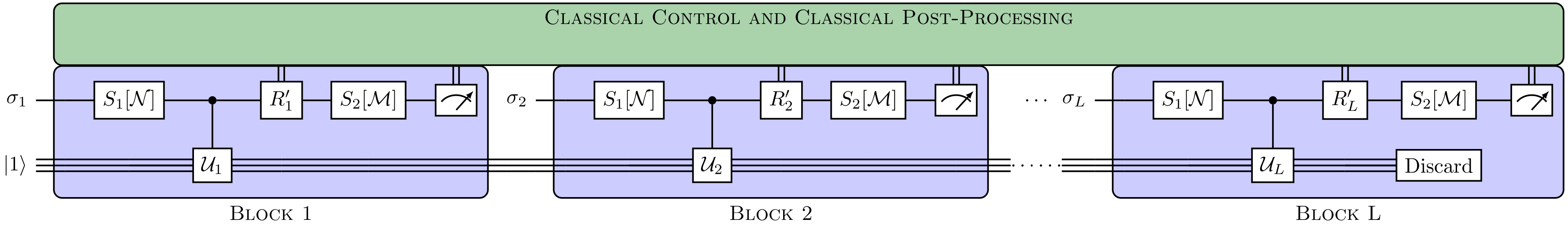
$$\mathscr{D}(\mathcal{M}) = \min_{\mathcal{D} \in \mathcal{DI}} \max_{\rho} \|\Delta(\mathcal{M} - \mathcal{D})\rho\|_1$$

Theurer et al, PRL 122, 190405 (2019)

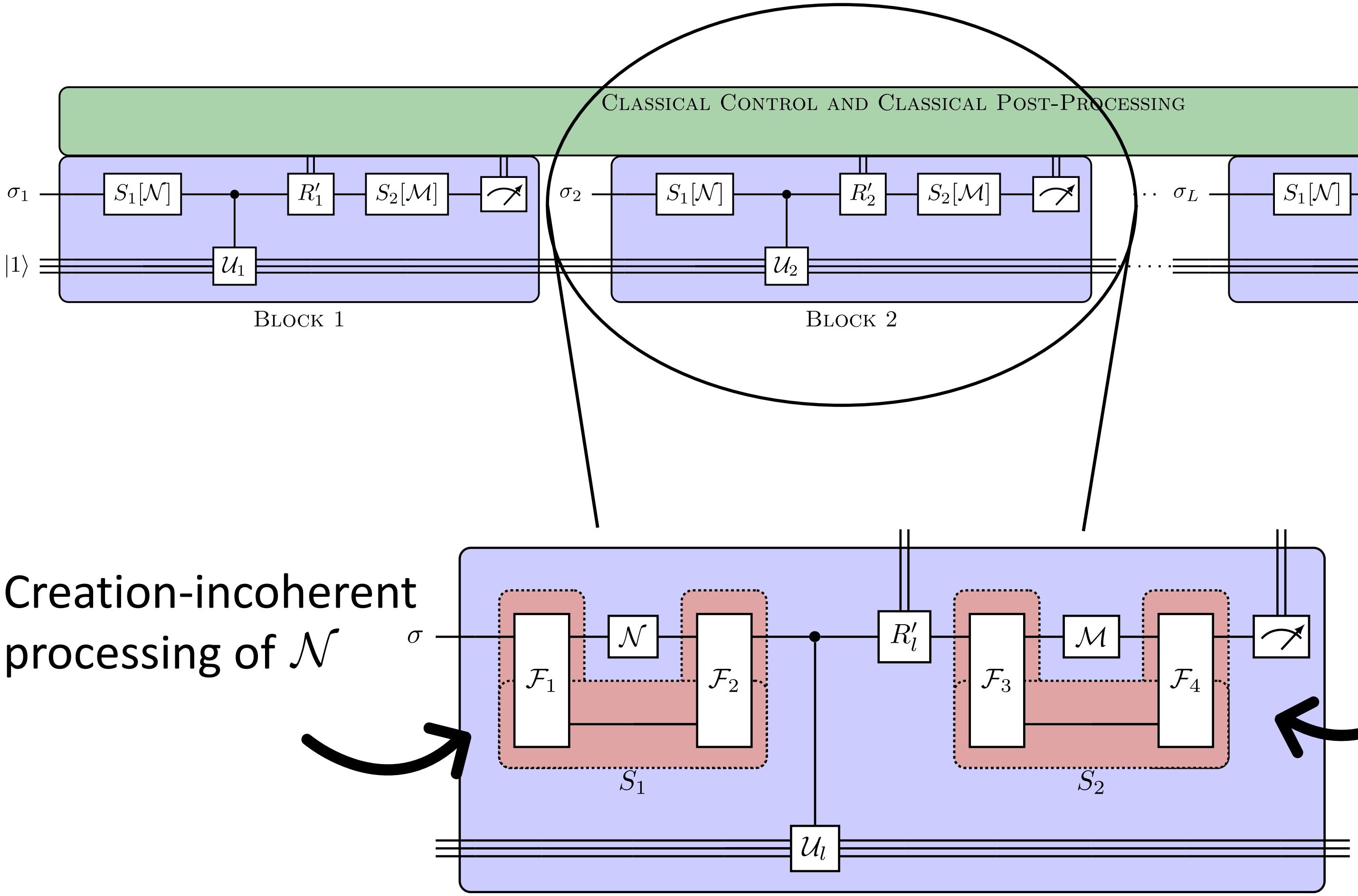
A level playing field



A level playing field



A level playing field



Creation-incoherent processing of $\mathcal{N}$

Detection-incoherent processing of $\mathcal{M}$

Bounds on success probability

Optimal usage of resources by maximizing over all free super-channels, free states and free measurements

Result 1 : For coherence creating channels $\mathcal{N}$ and unital detection channels $\mathcal{M}$

$$P^{\text{succ}}(\mathcal{N},\mathcal{M}) \geq c(r)\left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^{L}$$

Bounds on success probability

Optimal usage of resources by maximizing over all free super-channels, free states and free measurements

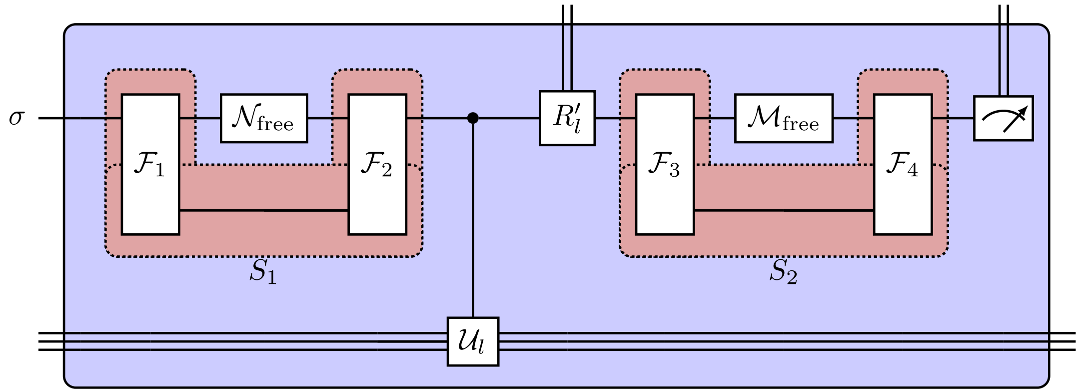
Result 1 & 2: For coherence creating channels $\mathcal{N}$ and unital detection channels $\mathcal{M}$

$$P^{\mathrm{succ}}(\mathcal{N},\mathcal{M}) \geq c(r)\left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^{L}$$

&

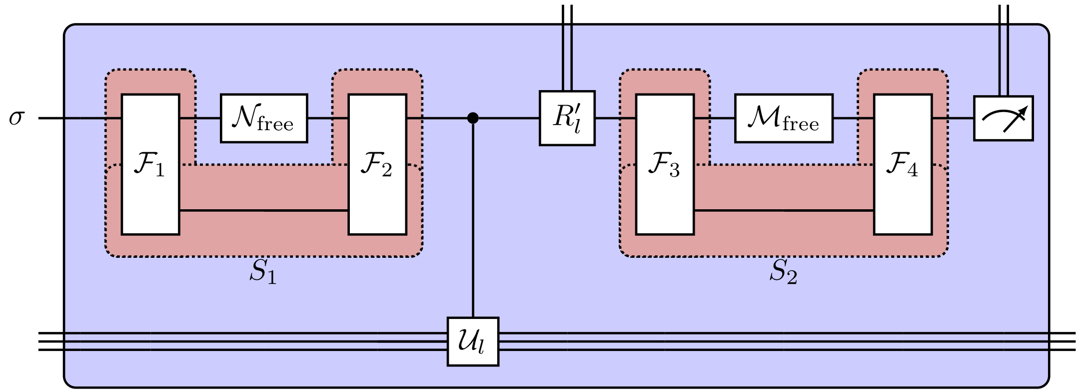
$$P^{\mathrm{succ}}(\mathcal{N},\mathcal{M}) \leq C(L,r)\left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^{L}$$

Free limit



No coherence; no entanglement generation

Free limit



No usage of coherence in this protocol; no entanglement generation

$$\left[C(L,r) - \tilde{c}(L,r)\right] \frac{1}{2^L} \leq P^{\text{succ}}(\mathcal{N}_{\text{free}}, \mathcal{M}_{\text{free}}) \leq C(L,r) \frac{1}{2^L}$$

$$c(r) \left[\frac{1 + \mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^L \leq P^{\text{succ}}(\mathcal{N}, \mathcal{M}) \leq C(L,r) \left[\frac{1 + \mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^L$$

Conclusion

- ◊ Coherence as a resource bounds performance
- ◊ Creation and detection on equal footing by optimal usage

$$P^{\text{succ}}(\mathcal{N},\mathcal{M}) \sim \left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^L$$

(for a algorithms with a fixed structure)

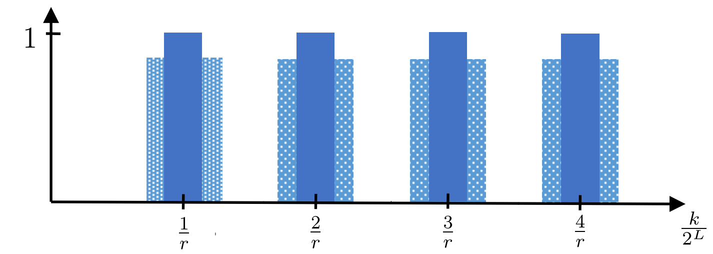
- ◊ Generalizations to other (factorization) algorithms?
- ◊ Interplay with other resources?

Phys. Rev. Lett. 129, 120501 (2022)

Thank you!

Success probability and post-processing

Optimizing over free states, measurements and super-channels gives



$$P^{\text{succ}}(\mathcal{N},\mathcal{M}) = \max_{\substack{\sigma\in\mathcal{I}\\ \mathbb{M}\in\mathcal{IM}}} \max_{\substack{S_1\in\mathcal{MIOS}\\ S_2\in\mathcal{DIS}}} \sum_k P(k\to r\,|\,\mathrm{CFA})\, p_k(S_1[\mathcal{N}], S_2[\mathcal{M}];\sigma,\mathbb{M})$$

Precise bounds

Lower Bound: For creating operations $\mathcal{N}$ and unital detection operations $\mathcal{M}$

$$P^{\text{succ}}(\mathcal{N},\mathcal{M}) \geq \frac{4}{\pi^2}\left(\frac{\varphi(r)}{r}\right)\left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^L .$$

Upper Bound: For creating operation $\mathcal{N}$ and unital detecting operation $\mathcal{M}$

$$P^{\text{succ}}(\mathcal{N},\mathcal{M}) \leq \varphi(r)\left(1+2\left\lfloor\frac{2^L}{r^2}\right\rfloor\right)\left[\frac{1+\mathscr{C}(\mathcal{N})\mathscr{D}(\mathcal{M})}{2}\right]^L$$