universität ulm

On the Role of Coherence in Shor's algorithm

Introduction to QRTs and applications

Felix Ahnefeld

Institute of Theoretical Physics
Ulm University, Germany

QLOC Seminar
September 28, 2022

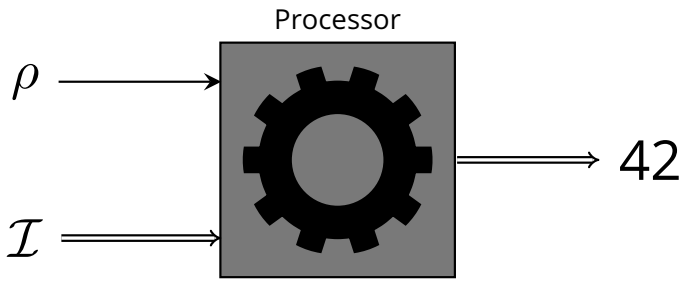

Hamburg
Berlin
Köln
Frankfurt am Main
Stuttgart
Ulm
München
© mixmaps.de

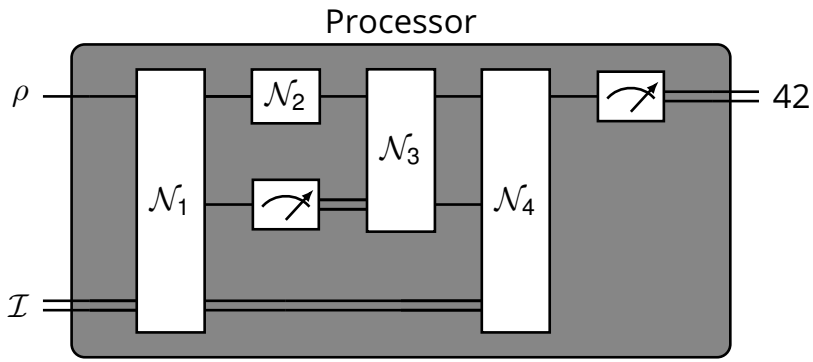
In this episode...

1. Quantum resource theories

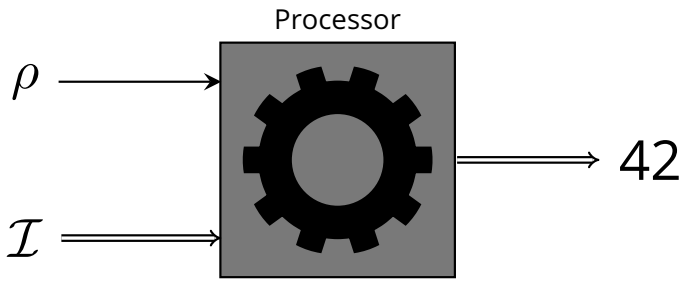
2. Coherence as a resource in quantum algorithms

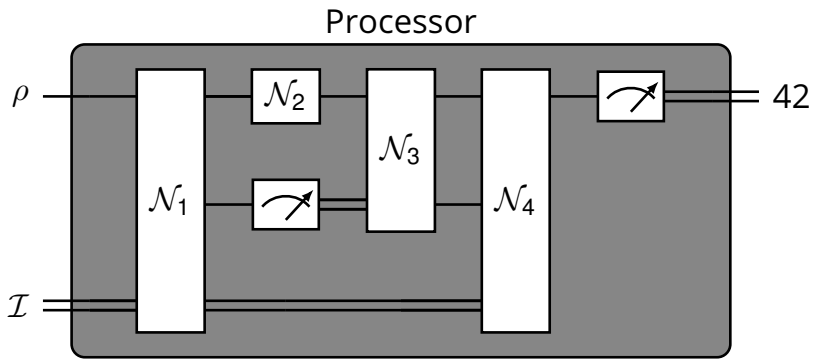
Motivation

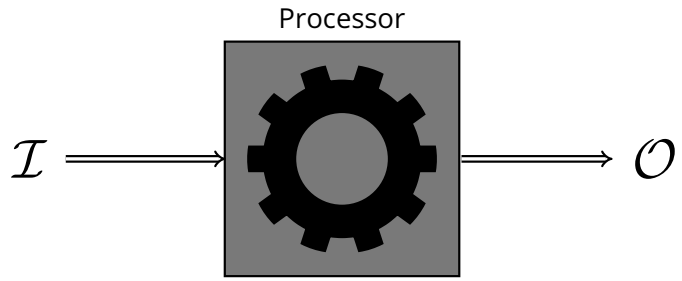

Processor
ρ
$\mathcal{I}$
42

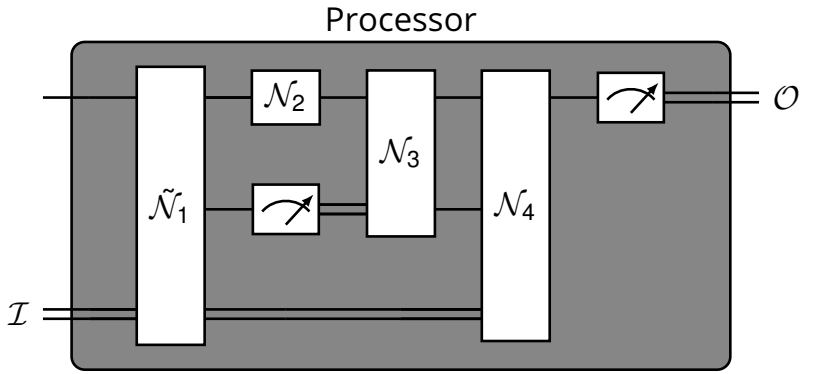

Processor
ρ
$\mathcal{I}$
$\mathcal{N}_1$
$\mathcal{N}_2$
$\mathcal{N}_3$
$\mathcal{N}_4$
42

Motivation









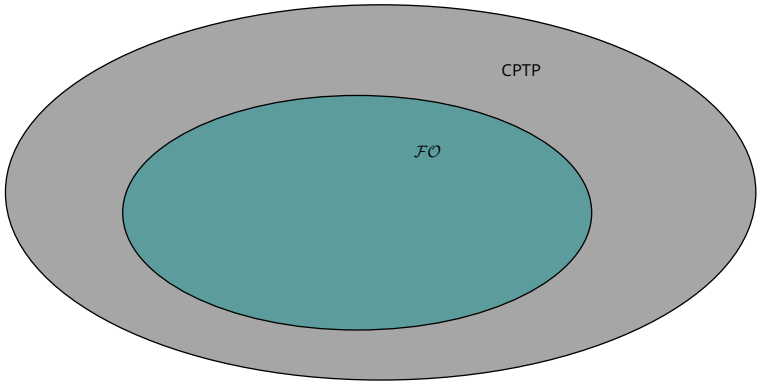
What fuels the processor?

Operations and free operations

Definition

Let $\mathcal{FO}$ be a the set of maps which assigns a map $\mathcal{FO}(A \to B) \subset \mathrm{CPTP}(A \to B)$ to any two systems A and B . The set $\mathcal{FO}$ is referred to as the set of *free operations* if

1. For any system A, the set $\mathcal{FO}(A \to A)$ contains the identity channel id_A.
2. For any systems A, B, C, if $\Phi_1 \in \mathcal{FO}(A \to B)$ and $\Phi_2 \in \mathcal{FO}(B \to C)$ the composition of maps is closed, i.e., $\Phi_1 \circ \Phi_2 \in \mathcal{FO}(A \to C)$.



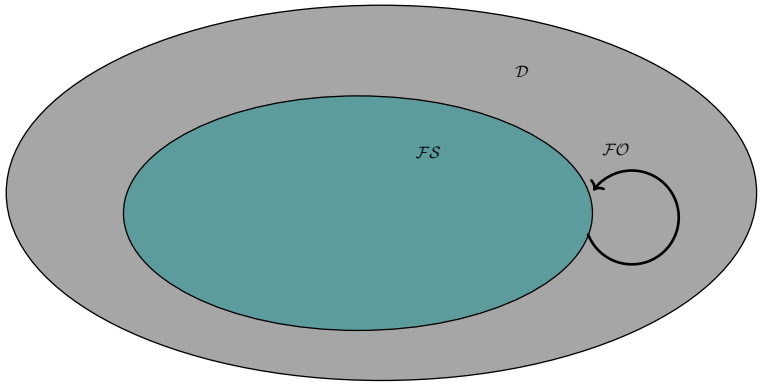
Chitamber, Gour (2018). Rev. Mod. Phys. 91, 025001

Free states & the golden rule

Definition

The set of *free states* is defined as $\mathcal{F} = \mathcal{FO}(\mathbb{C} \to A)$ for any system A.

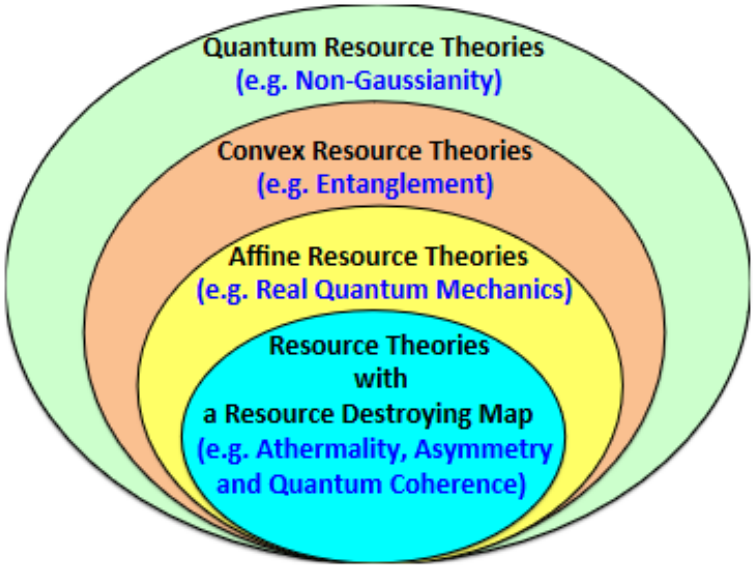
Golden rule
For any A and B, if
$\Phi \in \mathcal{FO}(A \to B)$ and $\rho \in \mathcal{F}$,
then $\Phi(\rho) \in \mathcal{F}$.



Definition

The tupel $\mathcal{R} = (\mathcal{F}, \mathcal{FO})$ defines a *static* resource theory.

QRT hierarchy & examples



Borrowed from Chitamber and Gour

- Entanglement

$$\Lambda_{\text{free}}(.) = \sum_k \left(\otimes_i M_{k,i}^{A_i}\right) (.) \left(\otimes_i M_{k,i}^{A_i}\right)^\dagger$$

$$\rho \in \text{SEP} \Leftrightarrow \rho = \sum_k p_k \bigotimes_i \rho_{i,k}^{A_i}$$

- Imaginary QM

$$\Lambda \in \mathcal{FO} \Leftrightarrow J_\Lambda = (\text{id} \otimes \Lambda)|\Omega\rangle\langle\Omega| \quad \text{real}$$

$$\rho \in \mathbb{R}\mathcal{S} \Leftrightarrow \rho \quad \text{real}$$

- Coherence: Resource destroying map Δ

$$\Delta(.) = \sum_i |i\rangle\langle i|(.)|i\rangle\langle i| \qquad \Lambda \in \mathcal{FO} \Leftrightarrow \Lambda \circ \Delta = \Delta \circ \Lambda \circ \Delta \qquad \rho \in \mathcal{I} \Leftrightarrow \Delta(\sigma) = \sigma$$

Chitamber, Gour (2018). Rev. Mod. Phys. 91, 025001
Horodecki family (2009). Rev. Mod. Phys. 81, 865
Hickey, Gour (2018) J. Phys. A: Math. Theor. 51 414009
Liu, Hu, Lloyd (2017). Phys. Rev. Lett. 118, 060502
Streltsov, Adesso, Plenio (2017). Rev. Mod. Phys. 89, 041003

Super-operators and free super-operators

Lemma

A linear map $S : CPTP(A \to B) \to CPTP(C \to D)$ can be represented as

$$S[\Lambda] = \Theta \Leftrightarrow \Theta_2(\Lambda \otimes \mathbb{1})\Theta_1 = \Theta.$$

This map is referred to as a super-operation.

- Sequential and parallel concatenation is free

$$\Phi_2\Phi_1 \in \mathcal{F} \quad \text{and} \quad \Phi_1 \otimes \Phi_2 \in \mathcal{F} \qquad \forall \Phi_1, \Phi_2 \in \mathcal{F}$$

Definition

A super-operation is called *free* if any free operation is transformed into a free operations, i.e., S free $\Leftrightarrow S[\Lambda] = \Phi_2(\Lambda \otimes \mathbb{1})\Phi_1 \quad \Phi_1, \Phi_2 \in \mathcal{F}$.

G. Chiribella et al 2008 EPL 83 30004

Coecke, Fritz, Spekkens, Inf. Comp. 2016

Pre-order and resource measures

$$\rho_2 \preceq \rho_1 \Leftrightarrow \exists \Phi \in \mathcal{FO} : \Phi(\rho_1) = \rho_2$$

$\rightarrow \rho_1$ more valuable

$$\Theta_2 \preceq \Theta_1 \Leftrightarrow \exists \mathbf{S} \in \mathcal{FSO} : \mathbf{S}[\Theta_1] = \Theta_2$$

$\rightarrow \Theta_1$ more valuable

Chitamber, Gour (2018). Rev. Mod. Phys. 91, 025001

Pre-order and resource measures

$$\rho_2 \preceq \rho_1 \Leftrightarrow \exists \Phi \in \mathcal{FO} : \Phi(\rho_1) = \rho_2 \qquad \Theta_2 \preceq \Theta_1 \Leftrightarrow \exists S \in \mathcal{FSO} : S[\Theta_1] = \Theta_2$$

$\rightarrow \rho_1$ more valuable $\qquad$ $\rightarrow \Theta_1$ more valuable

Does a Φ or S exist?
$\rightarrow$ Resource measures

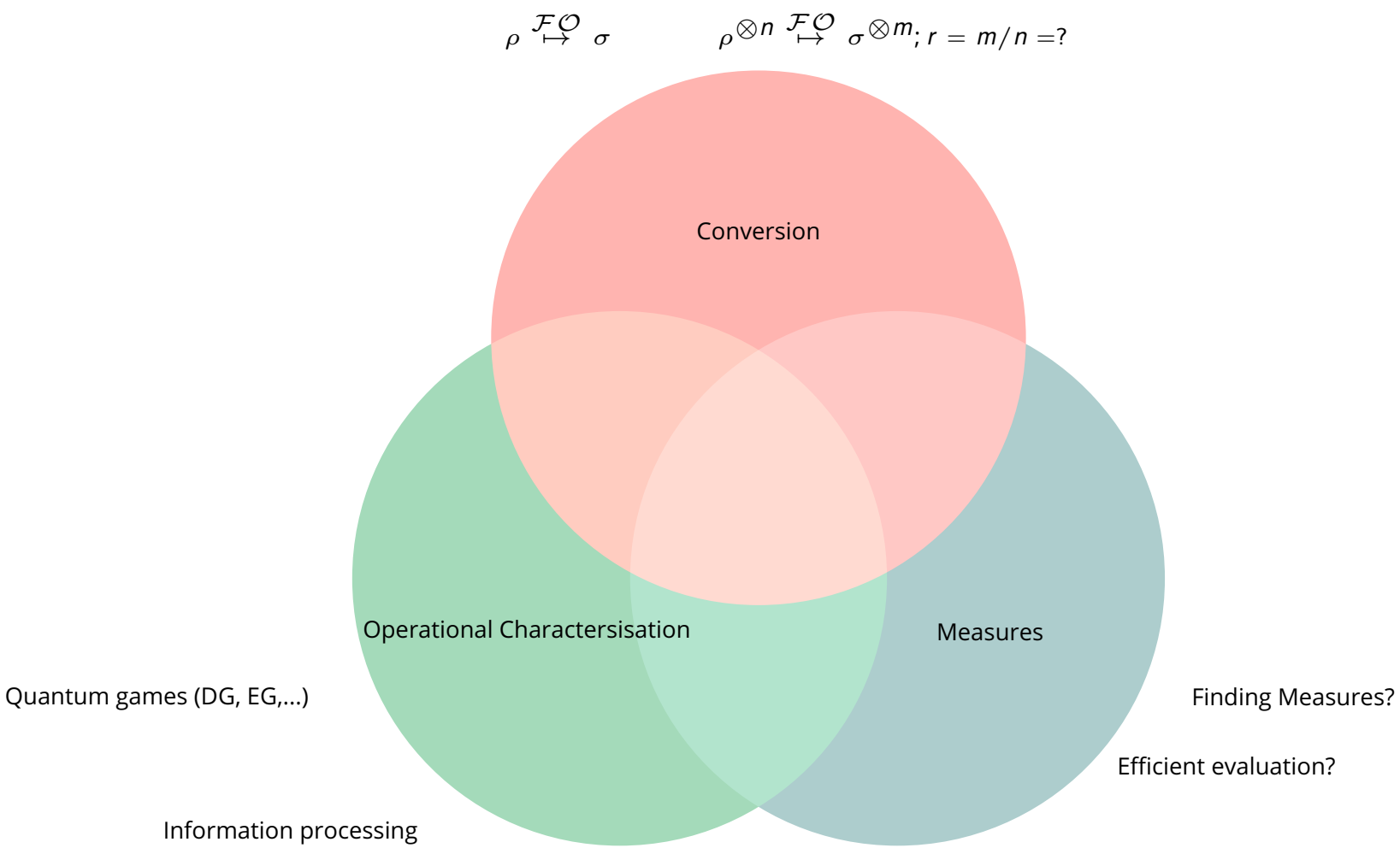
Definition

A positive functional M is called a static (dynamic) resource measure if is satisfies:

1. Monotonicity: $M(\Phi(\rho)) \leq M(\rho)\ \forall \rho \quad \left(M(S[\Theta]) \leq M(\Theta)\ \forall \Theta\right)$
2. Faithfulness: $M(\rho) = 0 \Leftrightarrow \rho \in \mathcal{F} \quad \left(M(\Theta) = 0 \Leftrightarrow \Theta \in \mathcal{FO}\right)$
3. Convexity: M is convex (for convex QRT)

Chitamber, Gour (2018). Rev. Mod. Phys. 91, 025001

Problems to study



Chitamber, Gour (2018). Rev. Mod. Phys. 91, 025001

Streltsov, Adesso, Plenio (2017) Rev. Mod. Phys. 89,041003

Concrete example: Coherence

$$\{|0\rangle, |1\rangle\} \quad \text{and} \quad \{|+\rangle = |0\rangle + |1\rangle, \; |-\rangle = |0\rangle - |1\rangle\}$$

Concrete example: Coherence

$$\{|0\rangle, |1\rangle\} \quad \text{and} \quad \{|+\rangle = |0\rangle + |1\rangle, \; |-\rangle = |0\rangle - |1\rangle\}$$

$$\{|+\rangle, |-\rangle\} \quad \text{and} \quad \{|0\rangle = |+\rangle + |-\rangle, \; |1\rangle = |+\rangle - |-\rangle\}$$

Concrete example: Coherence

$$\{|0\rangle, |1\rangle\} \quad \text{and} \quad \{|+\rangle = |0\rangle + |1\rangle, \; |-\rangle = |0\rangle - |1\rangle\}$$

$$\{|+\rangle, |-\rangle\} \quad \text{and} \quad \{|0\rangle = |+\rangle + |-\rangle, \; |1\rangle = |+\rangle - |-\rangle\}$$

1. Fix a preferred basis $\{|i\rangle\}_i$ and

$$\Delta(.) = \sum_i |i\rangle\langle i|(.)|i\rangle\langle i|$$

2. RNG set of free operations $\mathcal{MIO}$

$$\Phi \in \mathcal{MIO} \Leftrightarrow \Phi\Delta = \Delta\Phi\Delta$$

Application: Playing discrimination games

Discrimination game

Let $\{p_i, \mathcal{N}_i\}_{i=1\ldots N}$ be a black-box operation that implements a channel $\mathcal{N}_i$ with probability p_i. The probability to successfully discriminate which channel was applied is given by

$$P^{\text{succ}}(\rho) = \max_{\{M_n\}} \sum_n p_n \, \text{Tr}\left[\mathcal{N}_n(\rho) M_n\right]$$

Piani et al (2017). Phys. Rev. A 93, 042107

Napoli et al)2017). Phys. Rev. Lett. 116, 150502

Application: Playing discrimination games

Discrimination game

Let $\{p_i, \mathcal{N}_i\}_{i=1\ldots N}$ be a black-box operation that implements a channel $\mathcal{N}_i$ with probability p_i. The probability to successfully discriminate which channel was applied is given by

$$P^{\text{succ}}(\rho) = \max_{\{M_n\}} \sum_n p_n \,\text{Tr}\left[\mathcal{N}_n(\rho) M_n\right]$$

Lemma

For $\{\frac{1}{N}, \mathcal{U}_n\}$, with $U_n = \sum_m e^{i\phi_n m} |m\rangle\langle m|$, any non-free state provides an advantage, i.e.,

$$P^{succ}(\rho) \geq P^{succ}(\sigma)\ \forall \sigma \in \mathcal{F}.$$

Piani et al (2017). Phys. Rev. A 93, 042107

Napoli et al)2017). Phys. Rev. Lett. 116, 150502

Proof.

Take $\rho = V\sigma V^\dagger$ and since $P^{\text{succ}}(\sigma_1) = P^{\text{succ}}(\sigma_2)\ \forall \sigma_1, \sigma_2$

$$\begin{aligned} P^{\text{succ}}(\rho) &= \max_{\{M_n\}} \sum_n p_n \operatorname{Tr}\left[UV\sigma V^\dagger U^\dagger M_n\right] \\ &= \max_{\{M_n\}} \sum_n p_n \operatorname{Tr}\left[\sigma(V^\dagger U^\dagger M_n UV)\right] \\ &\geq P^{\text{succ}}(\sigma) \end{aligned}$$

□

Proof.

Take $\rho = V\sigma V^\dagger$ and since $P^{\text{succ}}(\sigma_1) = P^{\text{succ}}(\sigma_2)\ \forall \sigma_1, \sigma_2$

$$\begin{aligned} P^{\text{succ}}(\rho) &= \max_{\{M_n\}} \sum_n p_n \operatorname{Tr}\left[UV\sigma V^\dagger U^\dagger M_n\right] \\ &= \max_{\{M_n\}} \sum_n p_n \operatorname{Tr}\left[\sigma(V^\dagger U^\dagger M_n UV)\right] \\ &\geq P^{\text{succ}}(\sigma) \end{aligned}$$

□

Proposition

The optimal advantage for any discrimination game $\{p_n, \mathcal{U}_n\}$ is quantified by

$$\max_{\{p_n\}} \frac{P^{succ}(\rho)}{P^{succ}(\sigma \in \mathcal{I})} = 1 + C(\rho) \quad \textit{where} \quad C(\rho) = \min_{\tau \in \mathcal{D}} \left\{ r \geq 0 : \frac{\rho + r\tau}{1+r} =: \sigma \in \mathcal{I} \right\}.$$

Motive to name these frameworks as resource theories.

Why resource theories are important?

PHYSICAL REVIEW LETTERS **129,** 120501 (2022)

Coherence as a Resource for Shor's Algorithm

Felix Ahnefeld,[1,*] Thomas Theurer,[2,†] Dario Egloff,[3,‡] Juan Mauricio Matera,[4,§] and Martin B. Plenio[1,‖]
[1]*Institute of Theoretical Physics, Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany*
[2]*Department of Mathematics and Statistics, Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*
[3]*Institute of Theoretical Physics, Technical University Dresden, D-01062 Dresden, Germany*
[4]*IFLP-CONICET, Departamento de Física, Facultad de Ciencias Exactas, Universidad Nacional de La Plata, C.C. 67, La Plata 1900, Argentina*


Thomas


Dario


Mauricio

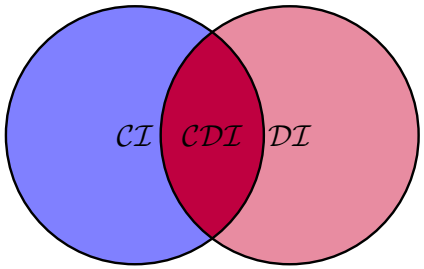

Martin

Dynamical QRT of Coherence I

- Resource destroying map

$$\Delta(\rho) = \sum_i |i\rangle\langle i|\rho|i\rangle\langle i|$$

- Free Operations
  1. Creation-incoherent: $\Phi\Delta = \Delta\Phi\Delta$
  2. Detection-incoherent: $\Delta\Phi = \Delta\Phi\Delta$



Streltsov, Adesso, Plenio (2017). Rev. Mod. Phys. 89, 041003

Theurer, Egloff, Plenio (2019). Phys. Rev. Lett. 122, 190405

Saxena, Chitambar, Gour (2020). Phys. Rev. Research 2, 023298

Dynamical QRT of Coherence II

- Incoherent measurements $M = \{P_n\}$

$$\mathrm{Tr}\left[P_n \rho\right] = \mathrm{Tr}\left[P_n \Delta \rho\right] \; \forall n, \rho$$

$$\text{M free} \Leftrightarrow P_n = \sum_i P_i^{(n)} |i\rangle\langle i|$$

- Incoherent states: $\Delta(\sigma) = \sigma$

Theurer, Egloff, Plenio (2019). Phys. Rev. Lett. 122, 190405

Dynamical QRT of Coherence II

- Incoherent measurements $M = \{P_n\}$

$$\mathrm{Tr}\left[P_n \rho\right] = \mathrm{Tr}\left[P_n \Delta \rho\right] \; \forall n, \rho$$

$$\text{M free} \Leftrightarrow P_n = \sum_i P_i^{(n)} |i\rangle\langle i|$$

- Incoherent states: $\Delta(\sigma) = \sigma$

Creation-Incoherent

1. $\mathcal{MIO}$ free operations
2. $\mathcal{MIOS}$ free super-operations
3. $\mathcal{I}$ inc. states

Detection-Incoherent

1. $\mathcal{DI}$ free operations
2. $\mathcal{DIS}$ free super-operations
3. $\mathcal{IM}$ inc. measurements

Theurer, Egloff, Plenio (2019). Phys. Rev. Lett. 122, 190405

Previous works?

Shor's coup

Goal: Factor integer N
$\Rightarrow$ Solve order-finding via $\{\frac{1}{r}, \mathcal{E}_j\}_{j=0..r-1}$

$$\mathcal{E}_j \equiv \sum_n e^{2\pi i \frac{j}{r}} |n\rangle\langle n|$$

Recover integer r?
$\Rightarrow$ Efficient post-processing via CFA

Parker, Plenio (2000). Phys. Rev. Lett. 85, 3049

Shor's coup

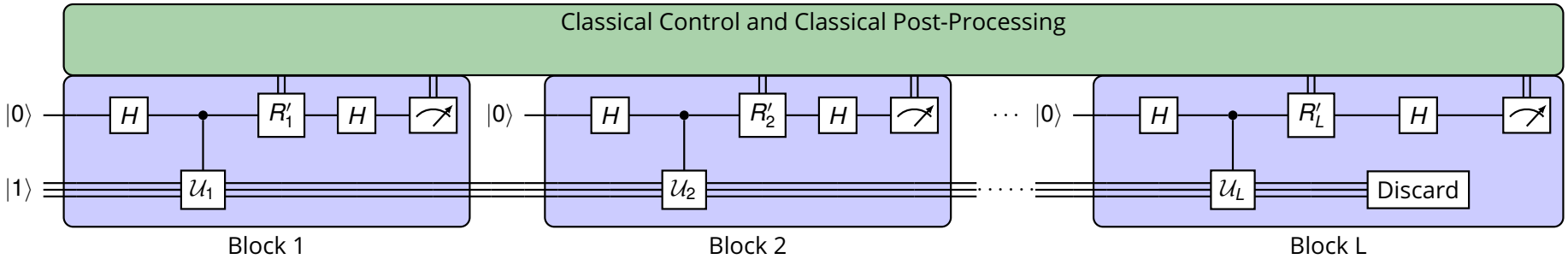
Goal: Factor integer N

$\Rightarrow$ Solve order-finding via $\{\frac{1}{r}, \mathcal{E}_j\}_{j=0..r-1}$

$$\mathcal{E}_j \equiv \sum_n e^{2\pi i \frac{j}{r}} |n\rangle\langle n|$$

Recover integer r?

$\Rightarrow$ Efficient post-processing via CFA

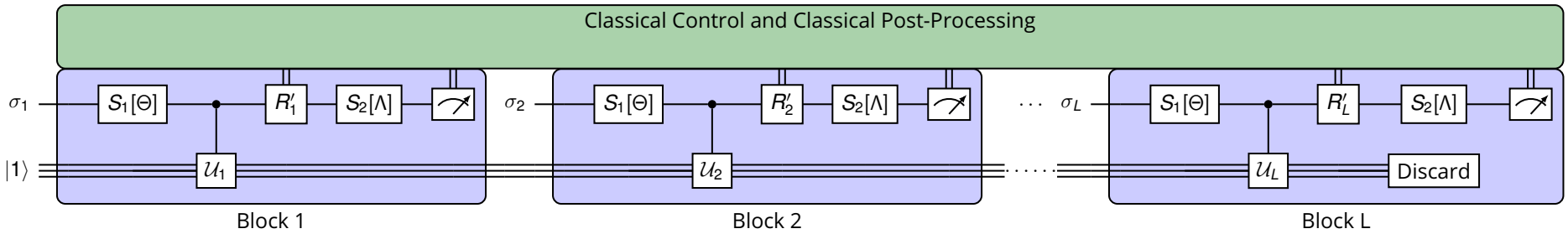


$$N^2 < 2^L < 2N^2$$

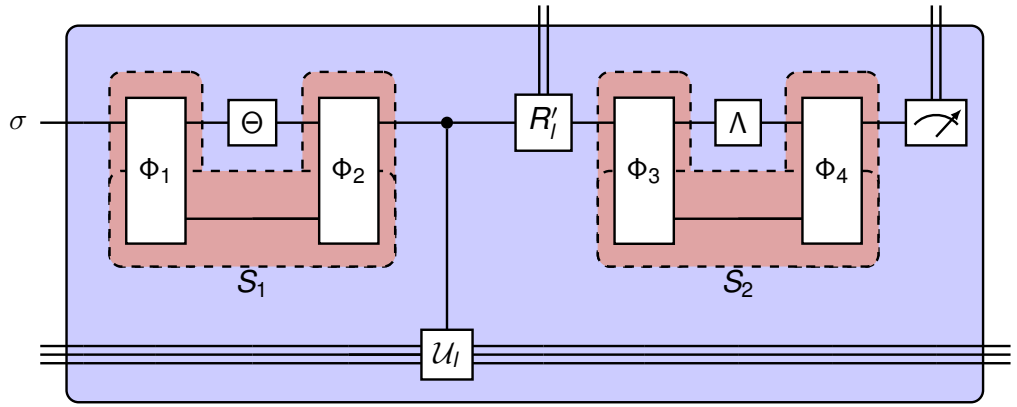
Parker, Plenio (2000). Phys. Rev. Lett. 85, 3049

A partially coherent protocol

- Keep all incoherent and classical operations
  $\Rightarrow$ Replace all others



Success Probability



$$P^{\text{succ}}(\Theta, \Lambda) = \max_{\sigma \in \mathcal{I}} \max_{\substack{\mathcal{S}_1 \in \mathcal{MIOS} \\ \mathcal{S}_2 \in \mathcal{DIS}}} \sum_k P(k \to r \,|\, \text{CFA})\, p_k(\mathcal{S}_1[\Theta], \mathcal{S}_2[\Lambda]; \sigma, \mathbb{P})$$

Lower Bound

Theorem

The success probability of the order-finding protocol with operations Θ and unital Λ for creation and detection respectively is bounded by

$$P^{succ}(\Theta,\Lambda) \geq \frac{4}{\pi^2}\left(\frac{\varphi(r)}{r}\right)\left[\frac{1+\mathscr{C}(\Theta)\tilde{M}_\diamond(\Lambda)}{2}\right]^L$$

- Euler's totient function

$$\frac{\varphi(r)}{r} \approx \frac{const.}{\log\log r}$$

- Cohering power $\mathcal{C}(\Theta) = \max_{\sigma\in\mathcal{I}} C(\Theta(\sigma))$

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

- NSID measure

$$\tilde{M}_\diamond(\Lambda) = \min_{\Phi\in\mathcal{DI}} \max_{\sigma} \|\Delta(\Lambda-\Phi)\sigma\|_1$$

$$0 \leq \mathscr{C}(\Theta),\ \tilde{M}_\diamond(\Lambda) \leq 1$$

Upper Bound

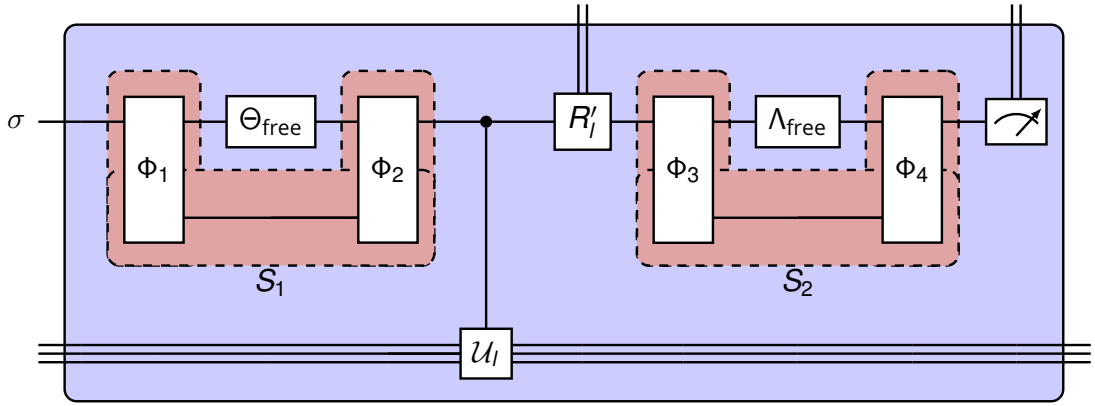
Theorem

The success probability of the order-finding protocol with operations Θ and unital Λ for creation and detection respectively is bounded by

$$P^{succ}(\Theta,\Lambda) \leq \varphi(r)\left(1+2\left\lfloor\frac{2^L}{r^2}\right\rfloor\right)\left[\frac{1+\mathscr{C}(\Theta)\tilde{M}_\diamond(\Lambda)}{2}\right]^L$$

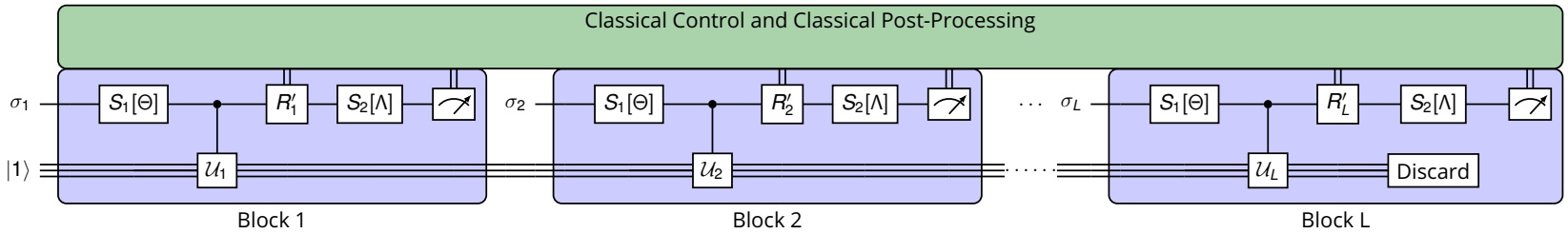
- Non-trivial in 'most' cases?
- Limitations of the prefactor?

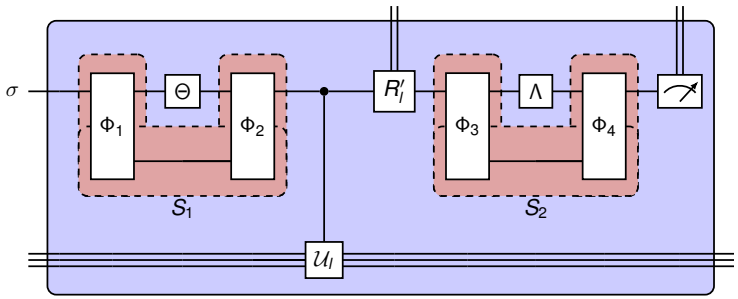
How to define the classical limit?



$$\frac{2\varphi(r)}{2^L}\left\lfloor\frac{2^L-1}{2r^2}\right\rfloor \leq P^{\text{succ}}(\Theta,\Lambda) \leq \frac{\varphi(r)}{2^L}\left(1+2\left\lfloor\frac{2^L}{r^2}\right\rfloor\right)$$

Take-home message





$$P^{\text{succ}}(\Theta,\Lambda) \sim \left[\frac{1+\mathscr{C}(\Theta)\tilde{M}_\diamond(\Lambda)}{2}\right]^L$$

Entanglement and coherence in Bernstein-Vazirani algorithm

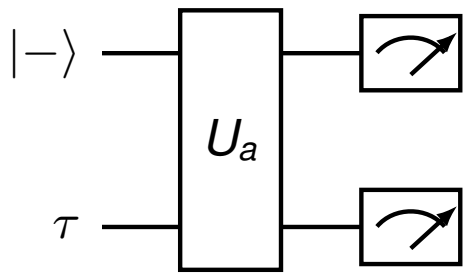
Moein Naseri, Tulja Varun Kondra, Suchetana Goswami, Marco Fellous-Asiani, and Alexander Streltsov
Centre for Quantum Optical Technologies, Centre of New Technologies,
University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland

- Find bit string a

$$f(x) = a \cdot x = \left(\sum_{k=0}^{N} x_k a_k \right) \bmod 2$$

- Via an oracle

$$U_a |i\rangle |x\rangle = |i \oplus f(x)\rangle |x\rangle$$



- Optimal measurement

$$P^{\text{succ}}(\rho) = \max_{\{M_a\}} \sum_a \frac{1}{2^N} \text{Tr}\left[\mathcal{U}_a(\rho) M_a\right]$$

- NO entanglement required

$$P^{\text{succ}}(|-\rangle\langle-| \otimes \tau) = \frac{1 + C(\tau)}{2^N}$$

Naseri et al (2022). arXiv:2205.13610v1

Need for a dynamical approach?