On the Role of Coherence in 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-89069 Ulm, Germany*
[2]*Department of Mathematics and Statistics, Institute for Quantum Science and Technology, University of Calgary, AB, Canada T2N 1N4*
[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
(Dated: July 4, 2022)

Shor's factoring algorithm provides a super-polynomial speed-up over all known classical factoring algorithms. Here, we address the question of which quantum properties fuel this advantage. We investigate a sequential variant of Shor's algorithm with a fixed overall structure and identify the role of coherence for this algorithm quantitatively. We analyze this protocol in the framework of dynamical resource theories, which capture the resource character of operations that can create and detect coherence. This allows us to derive a lower and an upper bound on the success probability of the protocol, which depend on rigorously defined measures of coherence as a dynamical resource. We compare these bounds with the classical limit of the protocol and conclude that within the fixed structure that we consider, coherence is the quantum resource that determines its performance by bounding the success probability from below and above. Therefore, we shine new light on the fundamental role of coherence in quantum computation.

Introduction.– Factoring large integers is considered to be a notoriously hard problem on a classical device. No classical factoring algorithm with polynomial run time is known, and the assumption that none exists lies at the heart of the widely used RSA cryptosystem [1]. Therefore, Shor's discovery of a quantum algorithm capable of factoring in polynomial time [2] not only attracted interest in this algorithm itself but the field of quantum computation in general: It is an example of a quantum algorithm that provides a super-polynomial computational speed-up over its best known classical counterpart (see also Refs. [3–6]). Since quantum devices are governed by laws different to those of classical physics, in principle, it might not seem too surprising that they can outperform them in certain applications. But which properties of quantum mechanics not present in classical physics fuel the speed-up in Shor's algorithm? And can they be used to explain speed-ups for the solution of other problems too? It is known that the presence of an unbounded amount of multipartite entanglement is necessary for exponential speed-ups in circuit-based pure state quantum computation because every protocol that does not exhibit this property can be simulated efficiently on a classical device [7]. This result, therefore, describes a necessary condition for exponential speed-ups in *arbitrary* protocols but *not* a sufficient condition as the presence of unbounded entanglement does not gaurantee efficient quantum computation. This and the lack of a connection of entanglement and classical simulability in the case of mixed states might give a hint that deeper concepts underpin the computational speed-up.

Here, we go one step further and instead of asking whether a resource is necessary to obtain speed-ups or describing its evolution during a protocol [7–11], we explore the speed-up that it actually grants. To start this exploration, we retreat from the general computational setting and focus on a specific algorithm with a fixed overall structure, namely a variant of Shor's algorithm introduced by Parker and Plenio [12]. The

focus allows us to present lower and upper bounds on the performance of this algorithm that hold for mixed states too and are expressed in terms of coherence measures, which are derived in the framework of quantum resource theories [13].

Quantum resource theories, see for example Refs. [13–25], are mathematical tools developed to describe the resource character of quantum properties. Their central idea is to impose additional restrictions on the laws of quantum mechanics, which single out the resources and allows to quantify them rigorously. Whilst the abstract mathematical frameworks have seen rapid development in recent years, rigorous quantitative relations between coherence and performance beyond variations of discrimination, exclusion, and detection games [26–37] are surprisingly rare [38–40]. This is problematic, since the study of coherence as a resource is primarily motivated by the desire to understand if and how it is responsible for quantum advantages. Besides the insights that our results grant on Shor's algorithm, they therefore also show that the study of coherence theories is of practical relevance.

First, we carefully motivate and describe what algorithm we are considering and how this allows us to investigate the role of coherence. This is crucial because we need to fix the overall structure of our algorithm: The most general approach to an investigation of the speed-up quantum resources grant in factoring would be to compare an ideal quantum algorithm (given fixed resources) to an ideal classical algorithm. Since it is unknown what such algorithms are, this is however out of reach. Instead, we focus on the quantum part in Shor's algorithm, namely the order-finding protocol, and fix its core, the modular exponentiation, whilst varying the remainder. This approach provides enough freedom while giving enough structure to observe interesting quantitative connections. We conclude with a discussion and outlook and refer to the SM for proofs and further details.

Quantum resource theories.– Generally, resource theories emerge from restrictions that are frequently motivated exper-

imentally. Here we restrict ourselves to finite-dimensional quantum systems and focus on constraints concerning the ability to create and detect coherence, but the concepts can be analogously applied to other restrictions. We begin by fixing the incoherent basis $\{|i\rangle\}_i$, i.e., the basis with respect to which we are going to describe coherence. Since we are considering circuit-based quantum computation, the computational basis in which we are encoding and extracting our classical information is the natural choice: If we never create coherence with respect to the computational basis, we are essentially reduced to the (classical) application of stochastic matrices onto probability vectors.

A quantum state σ is now considered incoherent and equivalent to a probability vector iff it is diagonal in the incoherent basis, i.e., iff $\Delta(\sigma) = \sigma$, where

$$\Delta(\rho) = \sum_i |i\rangle\langle i|\rho|i\rangle\langle i| \tag{1}$$

denotes total dephasing in the incoherent (computational) basis $\{|i\rangle\}_i$. We denote the set of incoherent states by $\mathcal{I}$ and call the maximal set of channels Φ that cannot create coherence, i.e., turn an incoherent state into a coherent one, the *maximally incoherent* channels and denote it by $\mathcal{MIO}$ [17, 42–44]. This set constitutes of all channels Φ that satisfy $\Phi\Delta = \Delta\Phi\Delta$. To exploit coherence, we do not only need to create it, but also use it. Using coherence is only possible if we have access to measurements that can detect it in the sense that its presence makes a difference in measurement statistics [44–46].

As detailed in Ref. [44], it is possible to identify all instruments that cannot detect coherence with the *detection-incoherent* channels $\mathcal{DI}$, i.e., all channels Φ satisfying $\Delta\Phi = \Delta\Phi\Delta$ [42, 44, 47, 48]. With the set of channels that cannot create/detect coherence and are thus considered free for the respective task identified, they can be used to build dynamical resource theories [29, 44, 49–62] introduced only recently to quantify how well non-free channels can create/detect coherence. The missing pieces are the super-channels that map quantum channels to quantum channels. A super-channel S can be represented by two quantum channels Θ_1, Θ_2 that are used as pre-and post-processing, i.e., $S[\Lambda] = \Theta_2(\mathbb{1} \otimes \Lambda)\Theta_1$ [63]. Also the super-channels are divided into free and non-free. In this work, we consider a super-channel free iff it can be represented by a free pre-and postprocessing [64, 65]. The set of free super-channels in the resource theory concerning the creation/detection of coherence is labeled by $\mathcal{MIOS}/\mathcal{DIS}$. This concept allows us to compare the value of channels via (dynamical) resource measures [44]: These are functionals M that map quantum operations to the non-negative numbers and satisfy (i) monotonicity: $M(\Theta) \geq M(S[\Theta])$ for all free super-channels S, i.e., they respect the preorder that the free super-channels impose on the channels and therefore their relative value, (ii) faithfulness: $M(\Theta) = 0$ iff Θ is free, (iii) convexity.

To quantify the connection between coherence and the performance of Shor's algorithm, we use two dynamical mea-

sures. One is the resource generation capacity [66–71]

$$\mathscr{C}(\Theta) = \max_{\tau \in \mathcal{I}} C(\Theta\tau) \tag{2}$$

based on the robustness of coherence [26]

$$C(\rho) = \min\left\{s \geq 0 : \frac{\rho + s\tau}{1 + s} \in \mathcal{I}, \tau \text{ a state}\right\}, \tag{3}$$

i.e., a measure with respect to $\mathcal{MIO}$ that describes how well a channel can create coherence. The other, with respect to $\mathcal{DI}$, is the NSID-measure [44] (non-stochastic in detection)

$$\tilde{M}_\diamond(\Lambda) = \min_{\Phi \in \mathcal{DI}} \max_\sigma \|\Delta(\Lambda - \Phi)\sigma\|_1, \tag{4}$$

which describes how well a channel can detect coherence. Although not the main purpose of this Letter, we show in the SM that an intuitive candidate for a measure, namely $\mathscr{D}(\Lambda) = \max_\rho \|\Delta\Lambda(\mathbb{1} - \Delta)\rho\|_1$, fails to form a measure in the $\mathcal{DI}$ setting, as it violates monotonicity.

Shor's algorithm.– Let N denote an integer to factor. The factorization problem can be reduced to the order-finding problem: given integers N and x where $x < N$ and x co-prime to N, find the order r defined as the smallest integer such that $x^r = 1 \pmod N$ (see Ref. [2] and the SM for more information). Solving order-finding for a randomly chosen x with the above properties allows to solve factoring with high probability, and it is exactly what the quantum parts of the various versions of Shor's algorithm accomplish efficiently.

For the standard quantum order-finding protocol one uses two quantum systems A and B of dimension q and N respectively, where system A consists of L qubits with $N^2 < q = 2^L < 2N^2$. Furthermore, one defines a unitary by $U_B |n\rangle = |xn \pmod N\rangle$ that acts on system B and the modular exponentiation via $U_c = \sum_{n=0}^{q-1} |n\rangle\langle n|_A \otimes U_B^n$. Important from a resource theoretical perspective, U_c is both in $\mathcal{DI}$ and in $\mathcal{MIO}$, i.e., it can neither produce nor detect coherence and is thus considered free in both resource theories. The standard order-finding protocol works then as follows: Initialize system AB in the state $|0\rangle_A^{\otimes L} |1\rangle_B$, first apply Hadamard gates to each qubit, apply U_c, followed by an inverse Fourier transform $\mathcal{F}^\dagger$ on A and then a measurement in the computational basis. A particular implementation of the Fourier transform is given by sequentially applied controlled phase gates and Hadamard gates [74], which allows to derive an equally efficient sequential variant of the order-finding protocol that requires only a single control qubit which is being recycled [12], see Fig. 1a. Inserting the measurement outcome into the classical post-processing via the continued fraction algorithm, both variants estimate r with sufficiently high probability to factor in polynomial runtime [2, 12, 72, 73].

Results.– We now describe the setup to which our results apply, namely the order-finding protocol depicted in Fig. 1a, and connect its performance to coherence. The quantum advantage in this protocol is obviously not emerging from the classical control and post-processing, so we keep this part
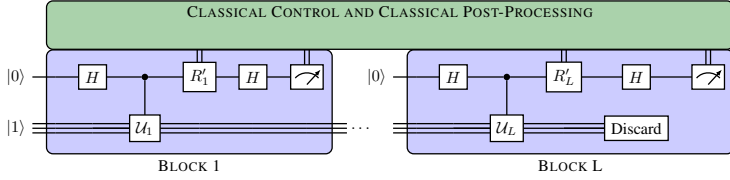
Figure 1a: A sequential variant of the order-finding algorithm, where the R'_n denote phase gates that depend on the outcomes of the previous measurements and $\mathcal{U}_l = U_B^{2^{L-l}}$. See the main text and the SM for further details.
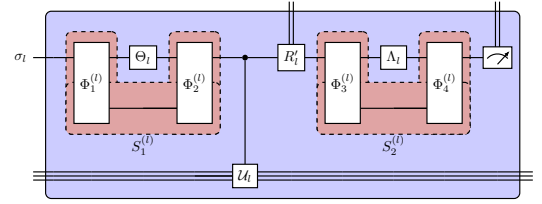
Figure 1b: A single modified block of the sequential order-finding algorithm with super-channels to make optimal use of the resources in the protocol.

fixed. Now looking at a single block, we remind that the controlled unitary $\mathcal{U}_l = U_B^{2^{L-l}}$ as well as the phase gate R'_l (see the SM for details) can neither create nor detect coherence and are thus free in both resource theories. Therefore, we keep them fixed as well and treat them as a black-box that we can probe. The remaining ingredients of each block become the main focus of study: If we would replace the initial state $H|0\rangle = |+\rangle$ of the control qubit, which is a maximally coherent state [23], with an incoherent one, the block would be seriously flawed, in the sense that it does not encode information about r, since the black-box only affects the coherences of the control qubit (see the SM for more information). Incoherent and maximally coherent states are extreme cases, and to connect the performance of the algorithm quantitatively to coherence, we investigate the impact on efficiency if we replace the initial control state with a partially coherent state. Since every quantum state can be identified with its replacements channel, we replace it with a fixed qubit channel Θ_l that is used to create an initial (partially coherent) control qubit state from an incoherent state σ_l. We further allow Θ_l to be transformed by arbitrary super-channels $S_1^{(l)} \in \mathcal{MIOS}$ since this is free from a resource perspective and ensures that we use the resource at hand appropriately. In this spirit, $S_1^{(l)}$ allows for a fair comparison of different resourceful operations. Note that another approach would be to optimize over different U_l (see Refs. [37, 39] for related approaches in different settings).

Furthermore, after the application of $\mathcal{U}_l$, we must extract the desired information, which is encoded exclusively in the coherences of the control qubit, hence we must detect coherence exactly in the sense that it makes a difference in the measurement statistics. The application of a Hadamard gate, which maximizes the NSID-measure among all qubit channels, is thus an extremal case too [44]. In contrast, a channel that cannot detect coherence would not be able to recover any of the available information on the prime factors. The ability to detect coherence, therefore, plays a vital role after the application of $\mathcal{U}_l$, and to investigate its precise contribution, we replace H with a fixed channel Λ_l, that interpolates between the optimal H and a completely incoherent measurement. We now allow to apply an arbitrary super-channel $S_2^{(l)} \in \mathcal{DIS}$ that is unitality preserving (we comment on this requirement in the SM), for the same reasoning as for $S_1^{(l)}$. The result-

ing block is depicted in Fig. 1b. To simplify our analysis for the main text, we further assume here that in each block, we use the same channel Θ/Λ for the creation/detection of coherence (see the SM for the more general version). For fixed Θ and Λ, we then define $P^{\text{succ}}(\Theta, \Lambda)$ to be the probability (maximized over the $S_1^{(l)}$, $S_2^{(l)}$, and σ_l) that a single run of this order-finding protocol leads to the correct order and bound it by the following Theorem.

Theorem 1. – The success probability of the order-finding protocol as described above with qubit operations Θ and unital Λ for creation and detection respectively is lower bounded by

$$P^{\text{succ}}(\Theta, \Lambda) \geq \frac{4}{\pi^2} \frac{\varphi(r)}{r} \left(\frac{1 + \mathscr{C}(\Theta)\tilde{M}_\diamond(\Lambda)}{2} \right)^L, \quad (5)$$

where $\varphi(r)$ denotes Euler's totient function.

The presence of $\mathscr{C}(\Theta)$ is intuitive as it quantifies the ability of Θ to create coherence in the control qubit [69–71], which is exactly what we use the channel Θ for. We note that for any qubit channel Θ, we have $\mathscr{C}(\Theta) \leq 1$, with equality iff Θ can create a maximally coherent qubit state [71]. Moreover, for qubit operations Λ, $\tilde{M}_\diamond(\Lambda) \leq 1$, and the bound is saturated for a Hadamard gate [44]. The measures enter the bound on equal footing, which indicates that the ability to create and detect coherence are equally important, as one would intuitively expect. In case both Θ and Λ are Hadamard gates, we recover the bound presented in Refs. [2, 12], which is used to prove the polynomial runtime of the algorithm. If the abilities to create and detect coherence decrease, this influences our bound exponentially in L. This suggests that the polynomial runtime of the fully coherent protocol becomes degraded exponentially in L by the lack of coherence and the ability to detect it. However, one needs to ask whether the performance actually decreases exponentially with less coherence, or if only our bound does so. To address this question, we continue to present a sufficiently general upper bound.

Theorem 2. – The success probability of the order-finding protocol as described above with qubit operations Θ and unital Λ for creation and detection respectively is upper bounded by

$$P^{\text{succ}}(\Theta, \Lambda) \leq \min\left\{ \varphi(r)\left(1 + 2\lfloor \tfrac{2^L}{r^2} \rfloor\right)\left(\tfrac{1 + \mathscr{C}(\Theta)\tilde{M}_\diamond(\Lambda)}{2}\right)^L, 1 \right\}. \quad (6)$$

We notice that this bound depends on both the problem and the employed coherence. The bound becomes trivial if the first

term exceeds unit probability, which is sensitively dependent on the ratio of 2^L and r. Nevertheless, this is a rather gentle restriction on our upper bound, which can be justified by comparing the bounds on the resourceful success probability with the classical limit of the algorithm. We define the classical limit as the corresponding protocol if we are only allowed to use operations that cannot detect or create coherence, i.e., if both Θ and Λ are free in their respective resource theories. In this case, we are in a classical regime and all states and operations can be reduced to probability vectors and stochastic matrices. The success probability is then determined by the uniform measurement statistic and the probability that the post-processing works, which results in

$$2\frac{\varphi(r)}{2^L}\lfloor \frac{2^L-1}{2r^2}\rfloor \leq P^{\text{succ}}(\Theta_{\text{free}}, \Lambda_{\text{free}}) \leq \frac{\varphi(r)}{2^L}\left(1+2\lfloor\frac{2^L}{r^2}\rfloor\right), \quad (7)$$

as we show in the SM. If we compare the bounds on the classical limit of the success probability with the one in Thm. 2, we see that the same prefactor occurs. In this sense, the slightly limited upper bound in Thm. 2 can be regarded as an artifact of the problem-dependence (see the SM for a visualization). If the fixed protocol does not perform well in the classical limit (which is the case of interest), we conclude that coherence is the quantum resource that determines the success probability by bounding it from below and above.

Discussion and outlook.– In our work, we have used resource theories to derive quantitative upper and lower bounds on the success probability of the quantum part of a sequential version of Shor's algorithm in terms of measures of (dynamical) coherence. Since the full algorithm repeats the quantum part until it succeeds, this also quantifies the total run time and speed-up in terms of the available resources. It is a novelty of our approach that we do not only observe how a resource evolves or depletes during an algorithm [8–11] but determine quantitatively the performance advantage that it grants. Moreover, our approach differs from Ref. [7], where a necessary condition for the presence of a resource (here entanglement) to admit a speed-up in pure state quantum computing was derived. The argumentation of Ref. [7] is based on the observation that a quantum protocol with limited multi-partite entanglement operating on pure states can be simulated efficiently on a classical device. As already pointed out in Ref. [7], this approach is incapable of establishing a (quantitative) sufficient condition for the contribution of entanglement as a resource as the presence of certain forms of large scale multi-partite entanglement can permit efficient classical simulation when employing a suitable mathematical data structure such as the stabilizer formalism [75].

In contrast, we derive bounds that hold even for mixed states and show quantitatively that coherence is necessary and sufficient to achieve an advantage over the classical limit of the investigated algorithm with a fixed overall structure. This, however, comes at the price that at present these quantitative connections are tied to a specific family of factoring algorithms. Furthermore, we remark that whilst the way we fixed the overall structure of the protocol and our choice of the free

operations is natural, well-motivated, and models the operations that are available to a classical computer, other choices may be considered too. Indeed, introducing restrictions that model the capabilities of a classical computer more accurately is an open problem that would lead to different (and potentially more involved) resource theories. As an example, one can additionally restrict the ability to preserve coherence [57], or more generally states [76]. It is an interesting open question whether other restrictions and the corresponding resources would lead to relations comparable to those we found; see for instance the discussion in the SM why we did not choose operations that can neither create nor detect coherence as free.

A closely related question is to what extent the overall structure of the protocol can be generalized whilst still obtaining meaningful bounds. As we discuss in the SM, our findings hold for the standard order-finding protocol too if the first register is in a product state and if the inverse Fourier transform is implemented in a way that leads to the sequential version. Indeed, generalizing the structure and choosing other free operations may reveal additional resources to underpin the efficiency of the quantum processor. One may for example argue that the implementation of the modular exponentiation, which is assumed to be free in our framework, does carry a cost. Relaxing this assumption may establish entanglement as a resource that bounds the efficiency of the protocol. However, as incoherent operations such as the modular exponentiation can convert coherence to entanglement [77–79] it may also be possible to reduce the resource entanglement to coherence when it comes to computation. In summary, our results depend on the choice of free operations and overall structure and we do not claim that coherence is *the* quantum resource for factoring alone, but we show that it is *a* quantum resource that lower and upper bounds the performance. In fact, it might well be that other resources not captured in our framework contribute (in other factoring algorithms) too. Exploring this is an interesting starting point for future work. Furthermore, using our technique to fix the structure of a protocol and to define a free limit, one can investigate the role of quantum resources in other quantum algorithms too. Since general statements about the role of quantum resources in computation are often out of reach, such an algorithm and implementation specific approach might lead to further insights into the value of quantum resources in computation, which might help to understand separation between classical and quantum computing.

* felix.ahnefeld@uni-ulm.de
† thomas.theurer@ucalgary.ca
‡ dario.egloff@mailbox.tu-dresden.de
§ matera@fisica.unlp.edu.ar
¶ martin.plenio@uni-ulm.de

[1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120 (1978).

[2] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. **26**, 1484 (1997).

[3] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation, Proc. R. Soc. A **439**, 553 (1992).

[4] D. R. Simon, On the power of quantum computation, SIAM J. Comput. **26**, 1474 (1997).

[5] E. Knill and R. Laflamme, Power of one bit of quantum information, Phys. Rev. Lett. **81**, 5672 (1998).

[6] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum algorithm for linear systems of equations, Phys. Rev. Lett. **103**, 150502 (2009).

[7] R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, Proc. R. Soc. A **459**, 20112032 (2003).

[8] M. Hillery, Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation, Phys. Rev. A **93**, 012111 (2016).

[9] N. Anand and A. K. Pati, Coherence and entanglement monogamy in the discrete analogue of analog Grover search, arXiv:1611.04542 (2016).

[10] H.-L. Shi, S.-Y. Liu, X.-H. Wang, W.-L. Yang, Z.-Y. Yang, and H. Fan, Coherence depletion in the Grover quantum search algorithm, Phys. Rev. A **95**, 032307 (2017).

[11] Y.-C. Liu, J. Shang, and X. Zhang, Coherence depletion in quantum algorithms, Entropy **21**, 260 (2019).

[12] S. Parker and M. B. Plenio, Efficient factorization with a single pure qubit and $\log N$ mixed qubits, Phys. Rev. Lett. **85**, 3049 (2000).

[13] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. **89**, 041003 (2017).

[14] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying entanglement, Phys. Rev. Lett. **78**, 2275 (1997).

[15] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619 (1998).

[16] M. Horodecki, P. Horodecki, and J. Oppenheim, Reversible transformations from pure to mixed states and the unique measure of information, Phys. Rev. A **67**, 062104 (2003).

[17] J. Aberg, Quantifying superposition, arXiv:quant-ph/0612146 (2006).

[18] G. Gour and R. W. Spekkens, The resource theory of quantum reference frames: manipulations and monotones, New J. Phys. **10**, 033023 (2008).

[19] M. Horodecki and J. Oppenheim, (quantumness in the context of) resource theories, Int. J. Mod. Phys. B **27**, 1345019 (2013).

[20] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Resource theory of quantum states out of thermal equilibrium, Phys. Rev. Lett. **111**, 250404 (2013).

[21] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New J. Phys. **16**, 013009 (2014).

[22] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik, Quantifying contextuality, Phys. Rev. Lett. **112**, 120401 (2014).

[23] T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying coherence, Phys. Rev. Lett. **113**, 140401 (2014).

[24] L. del Rio, L. Kraemer, and R. Renner, Resource theories of knowledge, arXiv:1511.08818 (2015).

[25] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[26] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Robustness of coherence: An operational and observable measure of quantum coherence, Phys. Rev. Lett. **116**, 150502 (2016).

[27] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso, Robustness of asymmetry and coherence of quantum states, Phys. Rev. A **93**, 042107 (2016).

[28] R. Takagi, B. Regula, K. Bu, Z.-W. Liu, and G. Adesso, Operational advantage of quantum resources in subchannel discrimination, Phys. Rev. Lett. **122**, 140402 (2019).

[29] R. Takagi and B. Regula, General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks, Phys. Rev. X **9**, 031053 (2019).

[30] P. Skrzypczyk and N. Linden, Robustness of measurement, discrimination games, and accessible information, Phys. Rev. Lett. **122**, 140403 (2019).

[31] P. Skrzypczyk, I. Šupić, and D. Cavalcanti, All sets of incompatible measurements give an advantage in quantum state discrimination, Phys. Rev. Lett. **122**, 130403 (2019).

[32] R. Uola, T. Kraft, J. Shang, X.-D. Yu, and O. Gühne, Quantifying quantum resources with conic programming, Phys. Rev. Lett. **122**, 130404 (2019).

[33] J. Mori, Operational characterization of incompatibility of quantum channels with quantum state discrimination, Phys. Rev. A **101**, 032331 (2020).

[34] A. F. Ducuara and P. Skrzypczyk, Operational interpretation of weight-based resource quantifiers in convex quantum resource theories, Phys. Rev. Lett. **125**, 110401 (2020).

[35] A. F. Ducuara, P. Lipka-Bartosik, and P. Skrzypczyk, Multiobject operational tasks for convex quantum resource theories of state-measurement pairs, Phys. Rev. Research **2**, 033374 (2020).

[36] R. Uola, T. Bullock, T. Kraft, J.-P. Pellonpää, and N. Brunner, All quantum resources provide an advantage in exclusion tasks, Phys. Rev. Lett. **125**, 110402 (2020).

[37] M. Masini, T. Theurer, and M. B. Plenio, Coherence of operations and interferometry, Phys. Rev. A **103**, 042426 (2021).

[38] J. M. Matera, D. Egloff, N. Killoran, and M. B. Plenio, Coherent control of quantum systems as a resource theory, Quantum Sci. Technol. **1**, 01LT01 (2016).

[39] T. Biswas, M. García Díaz, and A. Winter, Interferometric visibility and coherence, Proc. R. Soc. A **473**, 20170170 (2017).

[40] I. Marvian, Coherence distillation machines are impossible in quantum thermodynamics, Nat. Commun. **11**, 25 (2020).

[41] See the Supplemental Material, which includes Refs. [84–97], for proofs and further details.

[42] Z.-W. Liu, X. Hu, and S. Lloyd, Resource destroying maps, Phys. Rev. Lett. **118**, 060502 (2017).

[43] M. García Díaz, K. Fang, X. Wang, M. Rosati, M. Skotiniotis, J. Calsamiglia, and A. Winter, Using and reusing coherence to realize quantum processes, Quantum **2**, 100 (2018).

[44] T. Theurer, D. Egloff, L. Zhang, and M. B. Plenio, Quantifying operations with an application to coherence, Phys. Rev. Lett. **122**, 190405 (2019).

[45] B. Yadin, J. Ma, D. Girolami, M. Gu, and V. Vedral, Quantum processes which do not use coherence, Phys. Rev. X **6**, 041028

(2016).

[46] A. Smirne, D. Egloff, M. G. Díaz, M. B. Plenio, and S. F. Huelga, Coherence and non-classicality of quantum Markov processes, Quantum Sci. Technol. **4**, 01LT01 (2018).

[47] S. Meznaric, S. R. Clark, and A. Datta, Quantifying the non-classicality of operations, Phys. Rev. Lett. **110**, 070502 (2013).

[48] H. Xu, F. Xu, T. Theurer, D. Egloff, Z.-W. Liu, N. Yu, M. B. Plenio, and L. Zhang, Experimental quantification of coherence of a tunable quantum detector, Phys. Rev. Lett. **125**, 060404 (2020).

[49] K. Ben Dana, M. García Díaz, M. Mejatty, and A. Winter, Resource theory of coherence: Beyond states, Phys. Rev. A **95**, 062327 (2017).

[50] Q. Zhuang, P. W. Shor, and J. H. Shapiro, Resource theory of non-Gaussian operations, Phys. Rev. A **97**, 052317 (2018).

[51] X. Wang, M. M. Wilde, and Y. Su, Quantifying the magic of quantum channels, New J. Phys. **21**, 103002 (2019).

[52] X. Wang and M. M. Wilde, Resource theory of asymmetric distinguishability for quantum channels, Phys. Rev. Research **1**, 033169 (2019).

[53] Y. Liu and X. Yuan, Operational resource theory of quantum channels, Phys. Rev. Research **2**, 012035(R) (2020).

[54] Z.-W. Liu and A. Winter, Resource theories of quantum channels and the universal role of resource erasure, arXiv:1904.04201 (2019).

[55] G. Gour and A. Winter, How to quantify a dynamical quantum resource, Phys. Rev. Lett. **123**, 150401 (2019).

[56] G. Gour and C. M. Scandolo, Entanglement of a bipartite channel, Phys. Rev. A **103**, 062422 (2021).

[57] G. Saxena, E. Chitambar, and G. Gour, Dynamical resource theory of quantum coherence, Phys. Rev. Research **2**, 023298 (2020).

[58] G. Gour and C. M. Scandolo, Dynamical entanglement, Phys. Rev. Lett. **125**, 180505 (2020).

[59] S. Bäuml, S. Das, X. Wang, and M. M. Wilde, Resource theory of entanglement for bipartite quantum channels, arXiv:1907.04181 (2019).

[60] L. Li, K. Bu, and Z.-W. Liu, Quantifying the resource content of quantum channels: An operational approach, Phys. Rev. A **101**, 022335 (2020).

[61] R. Takagi, K. Wang, and M. Hayashi, Application of the resource theory of channels to communication scenarios, Phys. Rev. Lett. **124**, 120502 (2020).

[62] R. Takagi, Optimal resource cost for error mitigation, Phys. Rev. Research **3**, 033178 (2021).

[63] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Transforming quantum operations: Quantum supermaps, Europhys. Lett. **83**, 30004 (2008).

[64] G. Gour and A. Winter, How to quantify a dynamical quantum resource, Phys. Rev. Lett. **123**, 150401 (2019).

[65] G. Gour and C. M. Scandolo, Dynamical resources, arXiv:2101.01552 (2020).

[66] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, On the capacities of bipartite Hamiltonians and unitary gates, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[67] A. Mani and V. Karimipour, Cohering and decohering power of quantum channels, Phys. Rev. A **92**, 032331 (2015).

[68] Z. Xi, M. Hu, Y. Li, and H. Fan, Entropic characterization of coherence in quantum evolutions, arXiv:1510.06473 (2015).

[69] M. García-Díaz, D. Egloff, and M. B. Plenio, A note on coherence power of n-dimensional unitary operators, Quantum Inf. Comput. **16**, 12821294 (2016).

[70] K. Bu and C. Xiong, A note on cohering power and de-cohering power, Quantum Inf. Comput. **17**, 1206 (2017).

[71] K. Bu, A. Kumar, L. Zhang, and J. Wu, Cohering power of quantum operations, Phys. Lett. A **381**, 1670 (2017).

[72] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Clarendon Press, 1979).

[73] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2016).

[74] R. B. Griffiths and C.-S. Niu, Semiclassical Fourier transform for quantum computation, Phys. Rev. Lett. **76**, 3228 (1996).

[75] D. Gottesman, Stabilizer codes and quantum error correction, arXiv:quant-ph/9705052 (1997).

[76] D. Rosset, F. Buscemi, and Y.-C. Liang, Resource theory of quantum memories and their faithful verification with minimal assumptions, Phys. Rev. X **8**, 021033 (2018).

[77] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Measuring quantum coherence with entanglement, Phys. Rev. Lett. **115**, 020403 (2015).

[78] D. Egloff, J. M. Matera, T. Theurer, and M. B. Plenio, Of local operations and physical wires, Phys. Rev. X **8**, 031005 (2018).

[79] T. Theurer, S. Satyajit, and M. B. Plenio, Quantifying dynamical coherence with dynamical entanglement, Phys. Rev. Lett. **125**, 130401 (2020).

[80] A. Kay, Tutorial on the quantikz package, arXiv:1809.03842 (2018).

[81] J. Löfberg, YALMIP : A toolbox for modeling and optimization in MATLAB, in *In Proceedings of the CACSD Conference* (Taipei, Taiwan).

[82] J. F. Sturm, Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones, Optim. Methods Softw. **11**, 625 (1999).

[83] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, http://cvxr.com/cvx (2014).

[84] V. Vedral, A. Barenco, and A. Ekert, Quantum networks for elementary arithmetic operations, Phys. Rev. A **54**, 147 (1996).

[85] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Efficient networks for quantum factoring, Phys. Rev. A **54**, 1034 (1996).

[86] C. Zalka, Fast versions of Shor's quantum factoring algorithm, arXiv:quant-ph/9806084 (1998).

[87] G. Gour and R. W. Spekkens, The resource theory of quantum reference frames: manipulations and monotones, New J. Phys. **10**, 033023 (2008).

[88] G. Gour, I. Marvian, and R. W. Spekkens, Measuring the quality of a quantum reference frame: The relative entropy of frameness, Phys. Rev. A **80**, 012307 (2009).

[89] I. Marvian and R. W. Spekkens, The theory of manipulations of pure state asymmetry: I. basic tools, equivalence classes and single copy transformations, New J. Phys. **15**, 033001 (2013).

[90] I. Marvian, R. W. Spekkens, and P. Zanardi, Quantum speed limits, coherence, and asymmetry, Phys. Rev. A **93**, 052331 (2016).

[91] S. J. Miller and R. Takloo-Bighash, *An Invitation to Modern Number Theory* (Princeton University Press, 2006).

[92] E. Gerjuoy, Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers, Am. J. Phys. **73**, 521 (2005).

[93] P. S. Bourdon and H. T. Williams, Sharp probability estimates for Shor's order-finding algorithm, arXiv:quant-ph/0607148 (2006).

[94] E. Chitambar and G. Gour, Comparison of incoherent operations and measures of coherence, Phys. Rev. A **94**, 052336 (2016).

[95] I. Marvian and R. W. Spekkens, How to quantify coherence: Distinguishing speakable and unspeakable notions, Phys. Rev.

A **94**, 052324 (2016).

[96] E. Chitambar and G. Gour, Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence, Phys. Rev. Lett. **117**, 030401 (2016).

[97] S. G. Moreno and E. M. García-Caballero, On Viète-like formulas, J. Approx. Theory **174**, 90 (2013).