One-shot operational quantum resource theory
(With applications to quantum computation)

Zi-Wen Liu
Perimeter Institute

QIST 2019, YITP, Kyoto

1904.05840, joint with Kaifeng Bu (Zhejiang, Harvard) and Ryuji Takagi (MIT)
And several works in progress

Outline

- Background and overview
- <u>Preliminaries</u>: Theory of resource destroying maps, one-shot divergences and resource monotones
- <u>Framework</u>: Resource currencies, golden states, modification coefficients
- <u>Main results</u>: Collapse of modification coefficients, optimal rates of one-shot formation and distillation tasks, some general implications
- Applications to quantum computation via e.g. magic states
- Outlook

Resource theory

- Useful
- Hard to gain, easy to lose
- The more, the better

Resource theory

$$\frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}}$$

- Useful (communication, teleportation, wormholes...)
- Hard to gain, easy to lose (LOCC $\longrightarrow$ separable states)
- The more, the better (telep.: n ebits + 2n cbits $\geq$ n qubits)

Resource theory

A mathematical framework aiming at rigorously, quantitatively characterizing the above resource features.

- Building blocks, abstract formulations [Coecke/Fritz/Spekkens, IC '16]:
    - Free objects (quantum states/density operators): objects that carry no resource
    - Free morphisms (quantum operations/cptp maps): manipulations that are considered easy
- Central problem: quantification of resource
    - Axiomatic: basic criteria, e.g. vanish on free objects, monotonicity under free morphisms
    - Operational: physical meanings of the resource measure
        - Performance/usefulness in specific tasks/scenarios
        - Value in direct trading between resource entities (more universal and fundamental)

In this talk, we focus on the state theory.
Recently: quantum channels, GPTs [ZWL/Winter, 1904.04201...]

Resource theory

This scheme has been used to understand and characterize many important quantum features and their power in many scenarios...

Theory	Free states	Free operations	Applications
Entanglement	Separable states	LOCC, non-entangling ops...	Q. communication, information scrambling...
Thermal non-equilibrium	Gibbs state	Thermal ops, Gibbs-preserving ops...	Work extraction...
Coherence	Incoherent (diagonal) states	IO, DIO, MIO...	Q. transport, metrology...
Magic state	Stabilizer states (stabilizer polytope)	Stabilizer ops, stabilizer-preserving ops...	Q. computation, classical simulation costs...
Asymmetry	Symmetric states (wrt some symm. group)	Symmetry-preserving ops...	Q. reference frames, metrology...
Discord-type correlation	Classical-quantum states	π-commuting ops, commutativity-preserving ops...	DQC1, heat transfer...
Non-Gaussianity	Gaussian states	Gaussian ops...	Q. (optical) computation...

This talk

A general, unified quantitative theory of one-shot resource trading.

Not specific to any particular resource or any particular task

Only one or finite instances of resource are in play

Conversion from/to some “currency” states

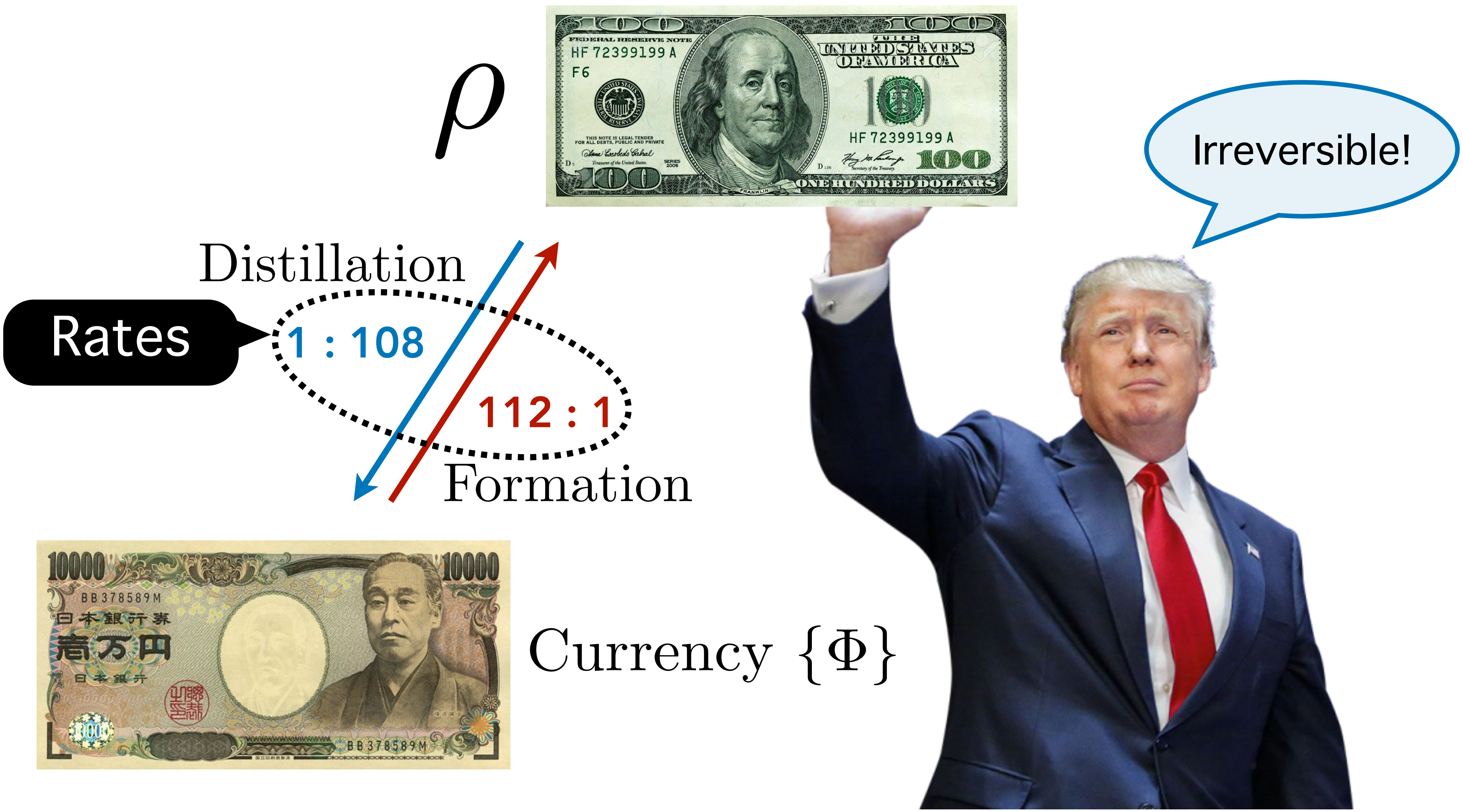
...And also, some explicit applications to the magic state theory, which plays key roles in many key developments on quantum computation.

General resource theory

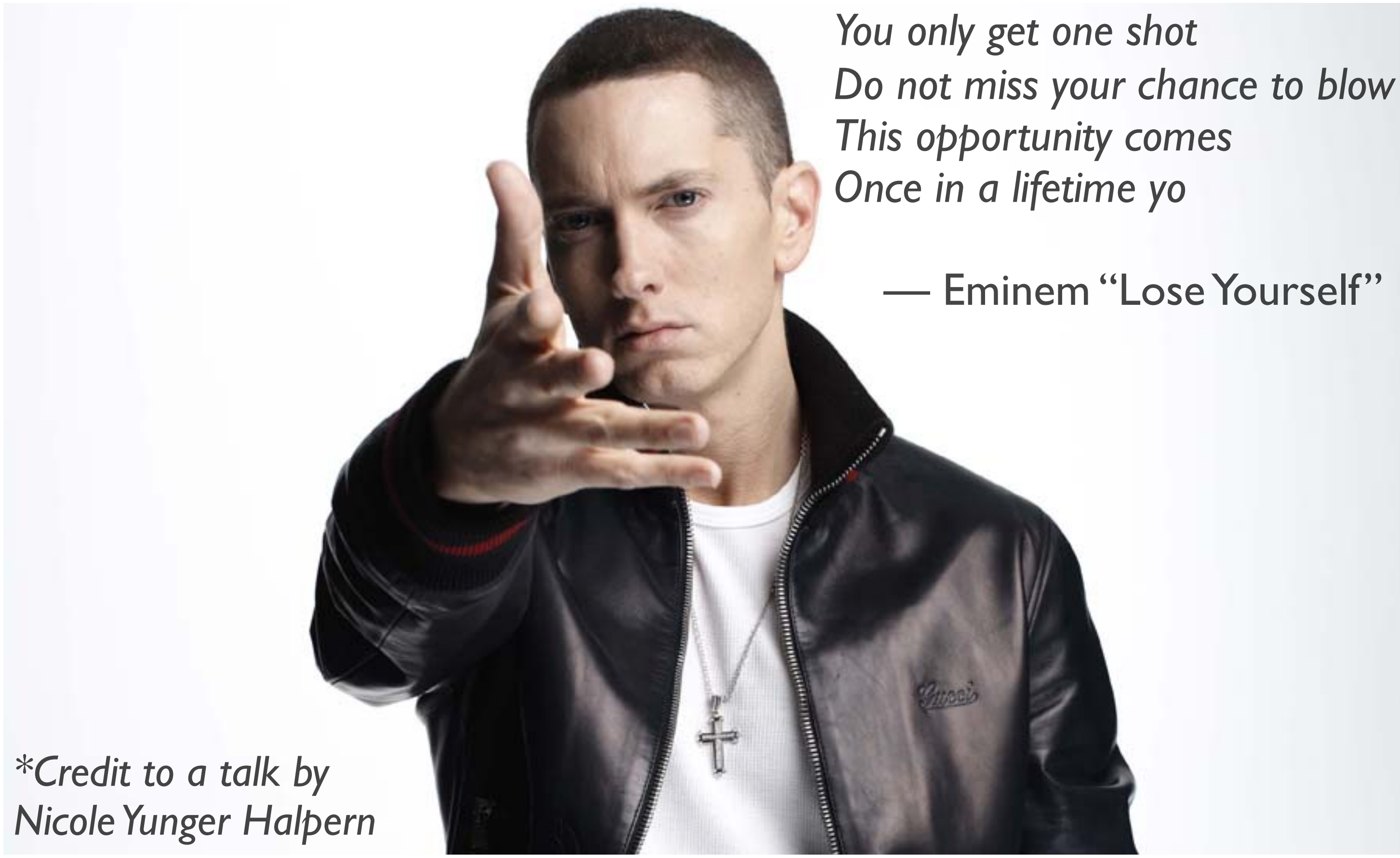
Different resource theories could share lots of common structures...

→ Let's invent all-purpose resource theory juicers!

Resource trading



One-shot



- Realistic scenario: i) Only finite instances of resource are available; ii) Certain extent of error/inaccuracy is allowed.
- Contrast: "asymptotic", i.e. infinite i.i.d. instances (a conventional setting of information theory—think about e.g. entropies, channel capacities; in resource theory: asymptotic reversibility [Brandao/Gour, PRL '15]).

Resource destroying (RD) map

Original theory: [ZWL/Hu/Lloyd, PRL '17]

$\mathcal{F}$: the set of free states.

Definition (Resource destroying map)

λ (a map from states to states) is an RD map if it has the following properties:

1. Resource destroying: $\forall \rho \notin \mathcal{F}, \lambda(\rho) \in \mathcal{F}$
2. Non-resource fixing: $\forall \sigma \in \mathcal{F}, \lambda(\sigma) = \sigma$

Remark: The basic definition is highly flexible. RD maps do not even need to be linear.

Resource destroying (RD) map

The following type of RD map is particularly important:

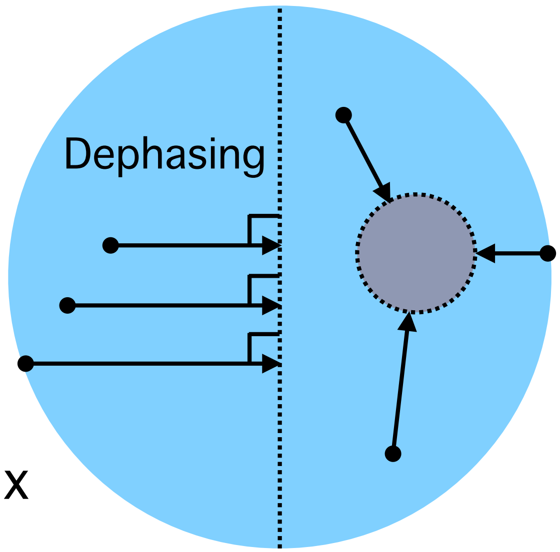
Definition (Exact RD map)

Exact RD map $\tilde{\lambda}$ satisfies: $D(\rho \| \tilde{\lambda}(\rho)) = \min_{\sigma \in \mathcal{F}} D(\rho \| \sigma), \forall \rho.$

I.e. "picks out" the closest free state*.

Examples:

- Coherence: Full dephasing
- Asymmetry: Uniform twirling
- Non-Gaussianity: Outputs Gaussian with the same mean displacement and covariance matrix



Resource destroying (RD) map

RD map theory induces unified definitions of different types of free operations. Here we consider the following two:

Definition (Resource non-generating operations)

$$\mathscr{F}_{\mathrm{NG}} := \{\mathcal{E} \,|\, \lambda \circ \mathcal{E} \circ \lambda = \mathcal{E} \circ \lambda\}$$

CPTP map

$$\lambda\left(\mathcal{E}\left(\lambda(\rho)\right)\right) = \mathcal{E}\left(\lambda(\rho)\right), \forall \rho$$

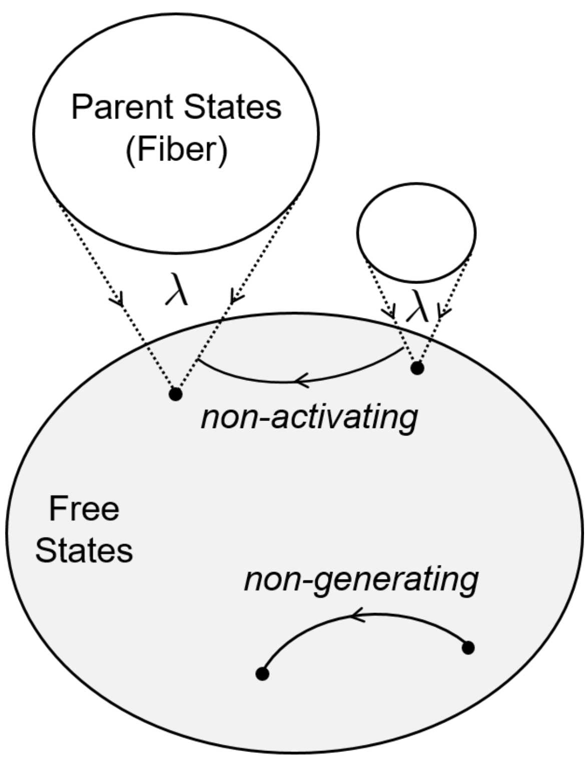
- Maximum set of free operations: any other operation would create resource and thus trivialize the theory.
- Invariant under the variation of RD map.

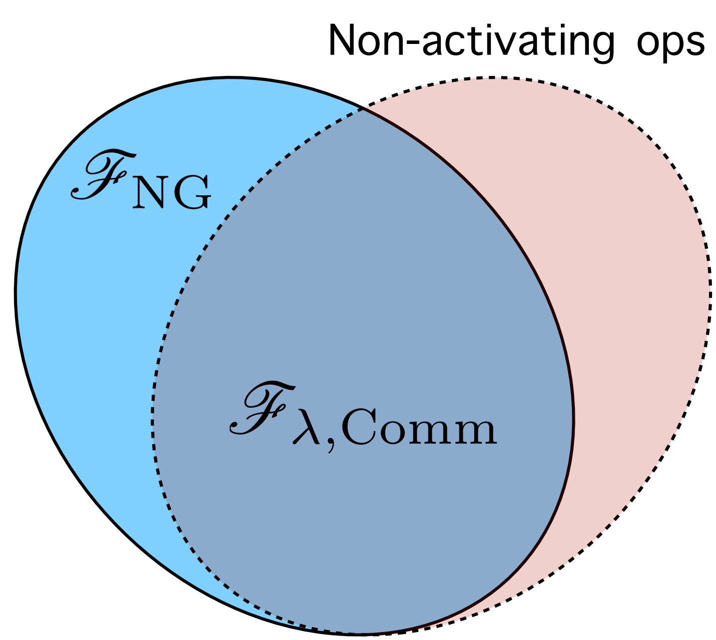
Resource destroying (RD) map

Definition (Commuting operations)

$$\mathscr{F}_{\lambda,\mathrm{Comm}} = \{\mathcal{E} \mid \lambda \circ \mathcal{E} = \mathcal{E} \circ \lambda\}$$

Examples: DIO (coherence), twirling-covariant (asymmetry), π-commuting (discord)...





Divergences between q. states

Let's first define some "distance" measures between quantum states (density operators) ρ and σ.

Definition (Uhlmann fidelity)

$$f(\rho,\sigma) := \left(\mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2 = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$$

Measuring "similarity" of the two states.

Just overlap^2 for pure states: $f(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|^2$

"Purified distance": $P(\rho,\sigma) := \sqrt{1 - f(\rho,\sigma)}$

Divergences between q. states

Definition (Max-relative entropy)

$$D_{\max}(\rho\|\sigma) := \log \min\{\lambda : \rho \leq \lambda\sigma\}$$

$\lambda\sigma - \rho$ is positive semidefinite

Well-defined when $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$

Definition (Min-relative entropy)

$$D_{\min}(\rho\|\sigma) := -\log \mathrm{Tr}\left\{\Pi_\rho \sigma\right\}$$

Π is the projector onto the support

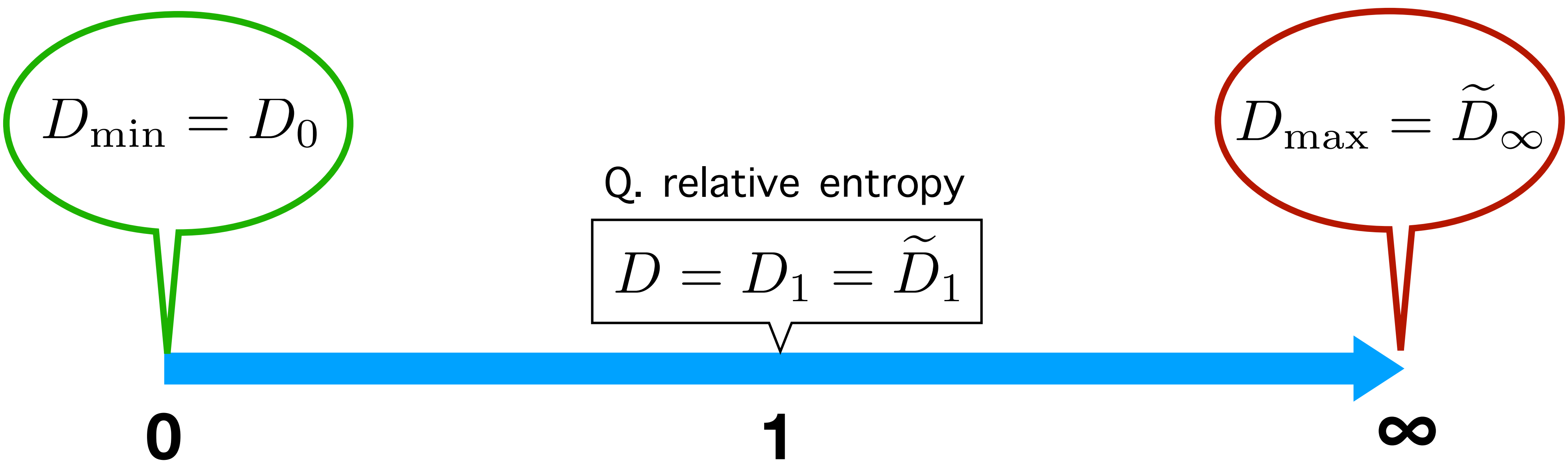
Well-defined when $\mathrm{supp}(\rho) \cap \mathrm{supp}(\sigma) \neq \emptyset$

Equivalent to $-\log f(\rho, \sigma)$ when ρ is pure

Divergences between q. states

Spectrum of quantum Renyi divergences:

D_α : Non-sandwiched q. Renyi-α div.
$\widetilde{D}_\alpha$: Sandwiched q. Renyi-α div.



Smoothing

Invoke "smoothing" technique to "stabilize" the measures (smoothed variants will account for error tolerance).
Idea: optimize over the "ε-vicinity".

Define the ε-ball in the state space as $\mathcal{B}^\epsilon(\rho) := \{\rho' : f(\rho', \rho) \geq 1 - \epsilon\}$

Definition (Smooth max/min-relative entropy)

$$D^\epsilon_{\max(\min)}(\rho\|\sigma) := \min_{\rho' \in \mathcal{B}^\epsilon(\rho)}(\max)\; D_{\max(\min)}(\rho'\|\sigma)$$

Also consider the "operator-smoothing" of min-relative entropy:

Definition (Hypothesis testing relative entropy)

$$D^\epsilon_H(\rho\|\sigma) := \max_{0 \leq P \leq I, \mathrm{Tr}\{P\rho\} \geq 1-\epsilon} (-\log \mathrm{Tr}\{P\sigma\})$$

Resource monotones

Resource measures based on the above divergences
(Idea: minimize distance to free states)

Definition (Divergence-based resource measures)

$$\mathfrak{D}_{\max(\min)}(\rho) := \min_{\sigma\in\mathcal{F}} D_{\max(\min)}(\rho\|\sigma) \qquad \mathfrak{f}(\rho) := \max_{\sigma\in\mathcal{F}} f(\rho,\sigma)$$

Monotone under any free operation, due to the "data processing" inequalities of the above distance measures.

$$\delta(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \le \delta(\rho,\sigma)$$

Useful smooth versions, by plugging in smooth divergences:

Definition (Smooth ~)

$$\mathfrak{D}^{\epsilon}_{\max}(\rho) := \min_{\sigma\in\mathcal{F}} D^{\epsilon}_{\max}(\rho\|\sigma), \quad \mathfrak{D}^{\epsilon}_{H}(\rho) := \min_{\sigma\in\mathcal{F}} D^{\epsilon}_{H}(\rho\|\sigma)$$

Resource monotones

Another important type of monotone (~noise needed to turn the resource state into a free one)

Definition (Free robustness/log-robustness)

$$R(\rho) := \min\{s \geq 0 : \exists \sigma \in \mathcal{F}, \frac{1}{1+s}\rho + \frac{s}{1+s}\sigma \in \mathcal{F}\},$$
$$LR(\rho) := \log(1 + R(\rho)).$$

Here if any σ is allowed (so-called "generalized robustness"), then the corresponding LR is equivalent to the D_max monotone. Equality on pure states implies existence of root states (bipartite vs. multipartite entanglement)

Definition (Smooth ~)

$$LR^{\epsilon}(\rho) := \min_{\rho' \in \mathcal{B}^{\epsilon}(\rho)} LR(\rho')$$

Finite free robustness implies: F is non-affine, no linear RD map

Resource monotones

- Some other general operational meanings are known for the D_max monotone: catalytic erasure [Anshu/Hsieh/Jain, PRL ’18] (smooth), subchannel discrimination [Takagi/Regula/Bu/ZWL/Adesso, PRL ’19] (exact).

- Little general knowledge about the other measures so far.

- *The D_min monotone exhibits peculiar features: (even the state-smoothed version) could be zero for non-free states (i.e. does not satisfy the “faithfulness” condition)… (Implications for distillation)

Resource monotones

RD-map-induced measures:

Definition (λ-induced measures)

$$\mathfrak{D}_{\max(\min),\lambda}(\rho) := D_{\max(\min)}(\rho\|\lambda(\rho)).$$

Monotone under all commuting operations [ZWL/Hu/Lloyd, PRL '17].

Smooth versions similarly defined:

Definition (Smooth λ-induced measures)

$$\mathfrak{D}^{\epsilon}_{\max,\lambda}(\rho) := D^{\epsilon}_{\max}(\rho\|\lambda(\rho)), \quad \mathfrak{D}^{\epsilon}_{H,\lambda}(\rho) := D^{\epsilon}_{H}(\rho\|\lambda(\rho)),$$

Note: No optimization over free states; Easy to compute for nice λ.

Resource currencies

A family of reference states that serve as a "standard currency"

$$\{\phi_d \in \mathcal{D}(\mathcal{H}_d)\}, \quad d \in \mathbb{D} \subseteq \mathbb{Z}_+$$

One for each dimension

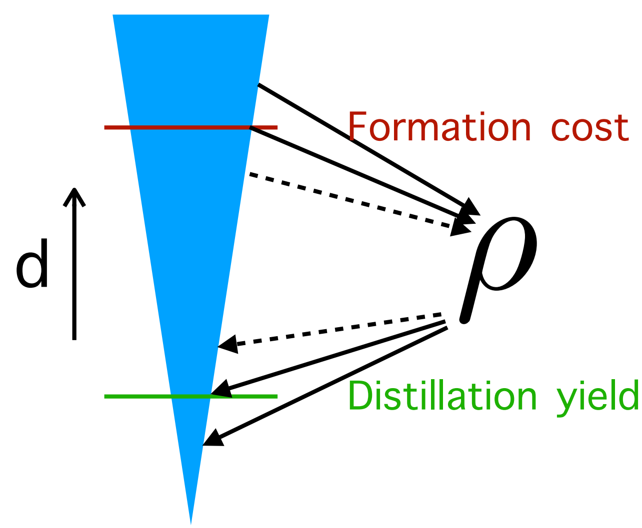
Valid dimensions

E.g. for multi-qubit theories

$$\mathbb{D} = \{2^n\}, n = 1, 2, 3...$$

Usually want to consider pure states,
"uniform" and "standard" in some sense

E.g. Bell pairs (ebits) as units
Uniform superposition/most coherent states



Modification coefficients

Definition (Modification coefficients)

$$
\begin{aligned}
m_f(\phi_d) &:= -\log \mathfrak{f}(\phi_d)/\log d,\\
m_{\max(\min)}(\phi_d) &:= \mathfrak{D}_{\max(\min)}(\phi_d)/\log d,\\
m_{LR}(\phi_d) &:= LR(\phi_d)/\log d.
\end{aligned}
$$

Similarly for the λ-induced measures.

"Normalized" parameters that encode "distance" to F

Let's look at some important resource currencies:

- Bipartite entanglement: Bell pairs (ebit units) $\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes n}$

  Additivity

  Or more generally $\frac{1}{d^{1/4}}\sum_{j=1}^{\sqrt{d}} |j\rangle|j\rangle$ $m_f = m_{\min} = m_{\max} = m_{LR} = 1/2, \forall d$

- Coherence: $\frac{1}{\sqrt{d}}\sum_{j=1}^{d} |d\rangle$ $m_f = m_{\min} = m_{\max} = 1, \forall d$

  Golden state collapse theorem (in a minute)

- *Magic: T-states $T^{\otimes t}$ $m_f = m_{\min} = m_{\max} \approx 0.23, \forall d$

  "Clifford magic" states

  m_LR is dependent on t

A few useful properties

Now we formulate a few simple properties of theories that will serve as sufficient (in many cases not necessary) conditions for different results:

- Condition (CH): F is formed by a convex hull of pure (free) states.

  *Very generic. Holds for basically all known convex theories except q. thermodynamics, where F is only the thermal/Gibbs state.

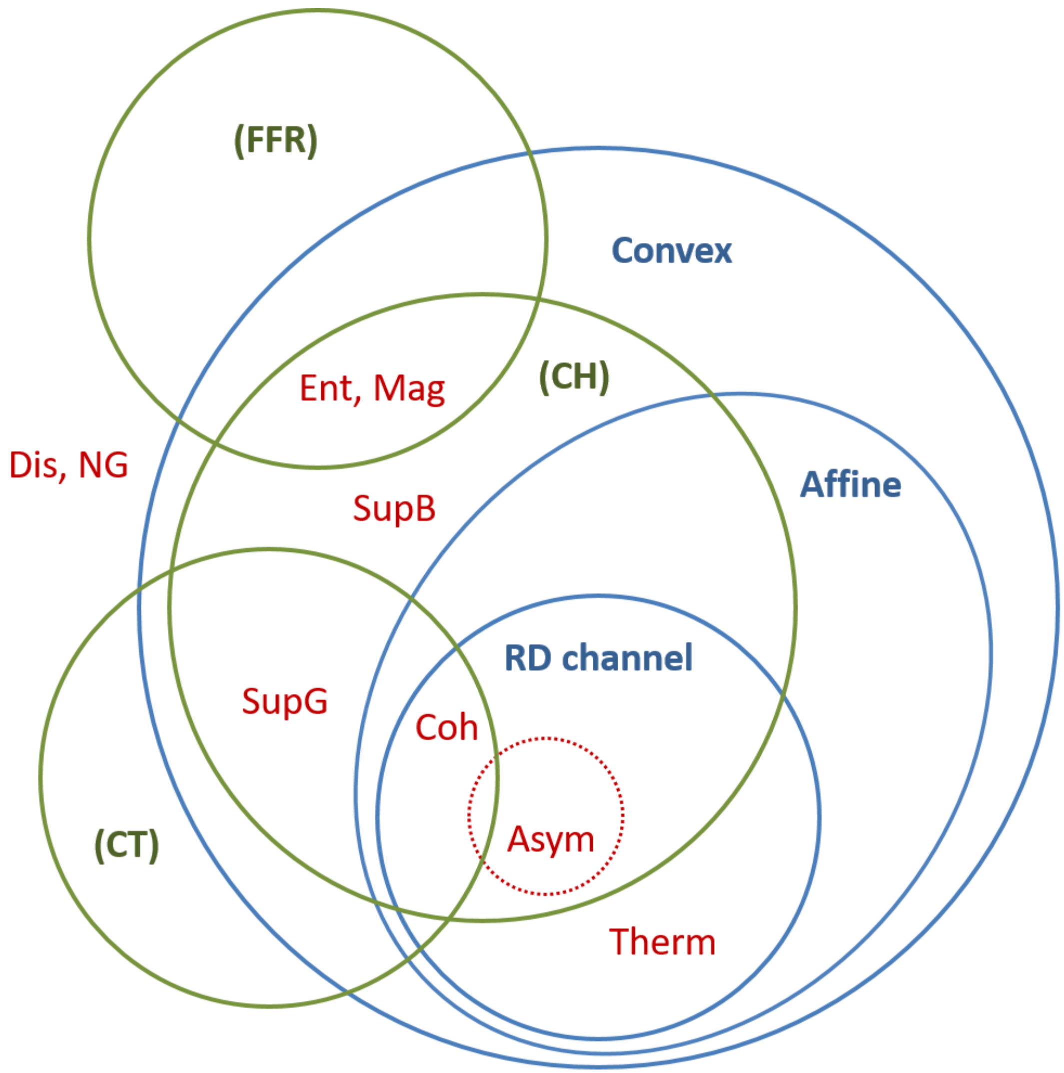
- Condition (CT) (for a chosen pure currency): Constant overlap with all free states.

  *This one is rather strong. Holds for coherence, thermodynamics (trivially), some superposition theories (see paper); not for entanglement, magic states etc.

- Condition (FFR): All states have finite free robustness.

  *Free robustness measures have drawn considerable interest recently. We show that this implies: i) F is a non-affine set; ii) RD map cannot be linear.

Zoo of Resource theories



Ent: Entanglement
Coh: Coherence
Mag: Magic states
Asym: Asymmetry
Therm: Thermodynamics
Dis: Discord
NG: Non-Gaussianity
SupB: Superposition (App. B)
SupG: Superposition (App. G)

A user guide for our all-purpose juicer (v1.0)

Collapse of modification coefficients

We prove an important and highly generic result about "max-resource" states:

Theorem (Collapse theorems)

Assume (CH). For any d, there exists a pure state $\hat{\Phi}_d$ s.t.

$$m_f(\hat{\Phi}_d) = m_{\min}(\hat{\Phi}_d) = m_{\max}(\hat{\Phi}_d) := g_d$$

"Golden state"

and achieve the maximum of each simultaneously.

"Golden coefficient"

Further consider exact RD map $\tilde{\lambda}$:

$$m_{f,\tilde{\lambda}}(\hat{\Phi}_d) = m_{\min,\tilde{\lambda}}(\hat{\Phi}_d) = m_{\max,\tilde{\lambda}}(\hat{\Phi}_d) = g_d$$

Equivalently, all the corresponding monotones (including Renyi) attain the same maximum value at this pure state.

Collapse of modification coefficients

Remarks:

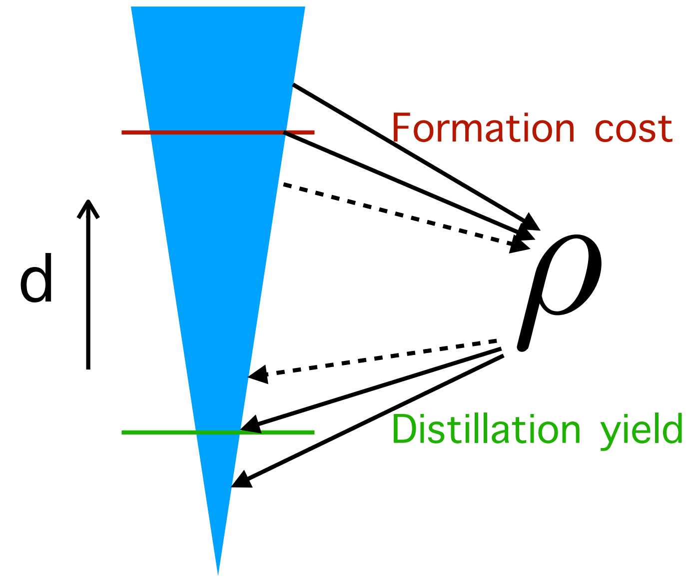
- The above results are highly nontrivial, considering that
  - The divergences and corresponding monotones generally behave very differently, so the collapse phenomenon is very special;
  - The divergences do not induce the same ordering (counterexample provided), so i) the max values are simultaneously attained; ii) exact RD map induces the closest free state for all measures, are both very special.

  $\rightarrow$Bad things just don't happen for golden states and exact RD maps!

- For (CH) theories, the result guarantees a complete family of pure max-resource states! As currency: most sensible conceptually; collapse theorems lead to tight bounds.
- Even (CH) is not necessary! Results also hold for q. thermodynamics.

Formation cost

"Minimum size" of reference state needed to approximate the state, by an operation from a certain set of free operations (with a certain type of constraint).



Definition (One-shot ε-formation cost under $\mathscr{F}$)

$$\Omega^{\epsilon}_{C,\mathscr{F}}(\rho \leftarrow \{\phi_d\}) := \log \min\{d \in \mathbb{D} : \exists \mathcal{E} \in \mathscr{F}, \mathcal{E}(\phi_d) \in \mathcal{B}^{\epsilon}(\rho)\}$$

Formation cost

Lower bound (fundamental limit/optimality). Unified form:

Theorem (Optimality)

Let $d_0 = \min\{d \in \mathbb{D} : \mathfrak{R}(\phi_d) \geq \mathfrak{R}^\epsilon(\rho)\}$

$$\Omega^\epsilon_{C,\mathscr{F}}(\rho \leftarrow \{\phi_d\}) \geq \frac{\mathfrak{R}^\epsilon(\rho)}{m(\phi_{d_0})}$$

- $\mathscr{F} = \mathscr{F}_{\mathrm{NG}}, \mathfrak{R} = \mathfrak{D}_{\max}, m = m_{\max}$
- $\mathscr{F} = \mathscr{F}_{\mathrm{NG}}, \mathfrak{R} = LR, m = m_{LR}$ (FFR)
- $\mathscr{F} = \mathscr{F}_{\lambda,\mathrm{Comm}}, \mathfrak{R} = \mathfrak{D}_{\max,\lambda}, m = m_{\max,\lambda}$

Consequences of monotonicity (for divergences, due to data processing inequalities) under free operations

Formation cost

Upper bound (achievability)

Theorem (Achievability)

Consider pure currency $\{\Phi_d\}$

Let $\quad d_0' = \min\{d \in \mathbb{D} : -\log \mathfrak{f}(\Phi_d) \geq \mathfrak{R}^\epsilon(\rho)\}$

$$\Omega^\epsilon_{C,\mathscr{F}}(\rho \leftarrow \{\Phi_d\}) < \frac{\mathfrak{R}^\epsilon(\rho)}{m_f(\Phi_{d_0'^\downarrow})} + \log \frac{d_0'}{d_0'^\downarrow}$$

Any smaller d.
Say, d_0-1 if all d are valid

- $\mathscr{F} = \mathscr{F}_{\mathrm{NG}}, \mathfrak{R} = \mathfrak{D}_{\max}$ (CT)
- $\mathscr{F} = \mathscr{F}_{\mathrm{NG}}, \mathfrak{R} = LR$ Convex F, (FFR)
- $\mathscr{F} = \mathscr{F}_{\lambda,\mathrm{Comm}}, \mathfrak{R} = \mathfrak{D}_{\max,\lambda}$ (CT)

Proofs by constructing a free cptp map achieving the desired approximation.

- Bounds on formation cost in terms of modified smooth max-relative entropy monotone and free log-robustness monotone

Formation cost

By using the collapse theorems, we can get the following almost matching/tight bounds (in such case the general-form free maps can almost achieve the lower bounds):

Corollary (Collapsed bounds)

Consider golden states $\{\hat{\Phi}_d\}$, assume (CH), (CT)

Let $d_0 = \min\{d \in \mathbb{D} : g_d \log d \geq \mathfrak{R}^\epsilon(\rho)\}$

$$\frac{\mathfrak{R}^\epsilon(\rho)}{g_{d_0}} \leq \Omega^\epsilon_{C,\mathscr{F}}(\rho \leftarrow \{\hat{\Phi}_d\}) < \frac{\mathfrak{R}^\epsilon(\rho)}{g_{d_0^\downarrow}} + \log \frac{d_0}{d_0^\downarrow}$$

- $\mathscr{F} = \mathscr{F}_{\mathrm{NG}}, \; \mathfrak{R} = \mathfrak{D}_{\max}$
- $\mathscr{F} = \mathscr{F}_{\tilde{\lambda},\mathrm{Comm}}, \; \mathfrak{R} = \mathfrak{D}_{\max,\tilde{\lambda}}$ For exact RD map $\tilde{\lambda}$

E.g. coherence: MIO/DIO, g=1, $\frac{1}{\sqrt{d}}\sum_{j=1}^{d}|d\rangle$

More on max-resource

Definition (Root state)

Can be mapped to any state of the same dimension by a free map.

The strongest notion of max-resource: max value for any monotone

In general, sufficient but not necessary condition for golden state.
Unclear when the root state can exist.

Our formation map implies the following partial result:

Corollary

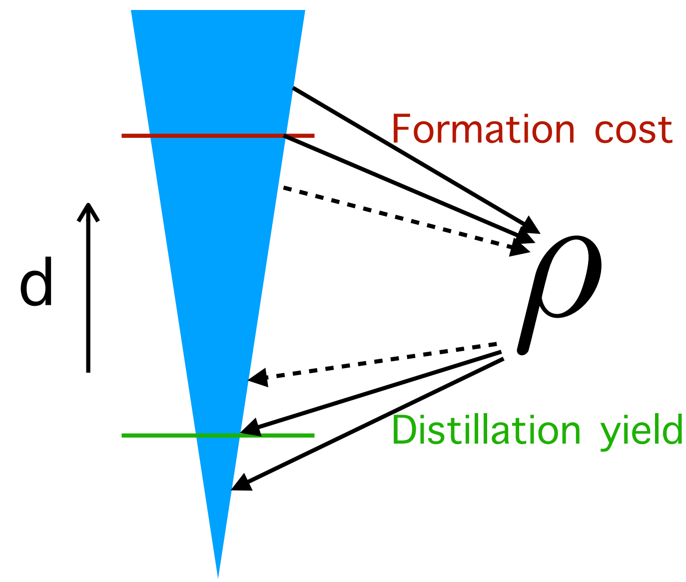
Free robustness
=
Generalized robustness

Golden state = root state if either is true:
i) (CT) ii) (FFR) and $m_{\max} = m_{LR}$ for all pure states

E.g. bipartite entanglement. In contrast, multipartite: no root state, so the free and generalized robustnesses are inequivalent

Distillation yield

A reverse direction: "Maximum size" of target reference state that can be approximately obtained, by an operation from a certain set of free operations (with a certain type of constraint).



Definition (One-shot ε-distillation yield under $\mathscr{F}$)

$$\Omega^{\epsilon}_{D,\mathscr{F}}(\rho \to \{\phi_d\}) := \log \max\{d \in \mathbb{D} : \exists \mathcal{E} \in \mathscr{F}, \mathcal{E}(\rho) \in \mathcal{B}^{\epsilon}(\phi_d)\}.$$

Also considered a stronger variant where error-tolerance is on the input state

Distillation yield

Consider resource non-generating operations first

Theorem (Optimality)

Consider pure currency $\{\Phi_d\}$

Let $d_0 = \max\{d \in \mathbb{D} : -\log \mathfrak{f}(\Phi_d) \leq \mathfrak{D}_H^\epsilon(\rho)\}$

$$\Omega^\epsilon_{D,\mathscr{F}_{\mathrm{NG}}}(\rho \to \{\Phi_d\}) \leq \frac{\mathfrak{D}_H^\epsilon(\rho)}{m_f(\Phi_{d_0})}$$

Theorem (Achievability)

Assume (FFR). Let $d_0 = \max\{d \in \mathbb{D} : LR(\phi_d) \leq \mathfrak{D}_H^\epsilon(\rho)\}$

$$\Omega^\epsilon_{D,\mathscr{F}_{\mathrm{NG}}}(\rho \to \{\phi_d\}) > \frac{\mathfrak{D}_H^\epsilon(\rho)}{m_{LR}(\phi_{d_0^\uparrow})} - \log \frac{d_0^\uparrow}{d_0}$$

Any larger d.
Say, d_0+1 if all d
are valid

For general convex theories we have another more complicated lower bound given by a distillation map based on the "isotropic state" technique

Distillation yield

Commuting operations.

Theorem (Optimality)

Consider pure currency $\{\Phi_d\}$ and RD channel (linear cptp map) Λ

Let $\quad d_0 = \max\{d \in \mathbb{D} : \mathfrak{f}_\Lambda(\Phi_d) \geq 2^{-\mathfrak{D}^{\epsilon}_{H,\Lambda}(\rho)} - 2\sqrt{\epsilon}\}$

$$\Omega^{\epsilon}_{D,\mathscr{F}_{\Lambda,\mathrm{Comm}}}(\rho \to \{\Phi_d\}) \leq \frac{-\log(2^{-\mathfrak{D}^{\epsilon}_{H,\Lambda}(\rho)} - 2\sqrt{\epsilon})}{m_{f,\Lambda}(\Phi_{d_0})}.$$

For now we only find general achievability bounds for a special notion of commuting operations based on the “isotropic” method in this formalism.

- Bounds on distillation yield (error on the target) in terms of modified hypothesis testing relative entropy

Distillation yield

A few more remarks:

- Input-error-tolerance model: A larger collection of bounds based on similar techniques can be obtained; The state-smoothing of min-relative entropy monotones (more stringent) emerge.

- More results using the maximal overlap formalism [Bu/ZWL/Regula/Takagi, in preparation], e.g. characterizations of distillation for non-(FFR) theories.

- By using the collapse theorems and a few asymptotic equipartition properties (e.g. Stein's lemma for hypothesis testing), we can obtain new asymptotic (infinite i.i.d. limit) reversibility results for non-maximal free operations.

No-go theorems for distillation

[Fang/ZWL, in preparation]

Distilling "good"/pure resource states from "bad"/noisy ones is a very useful type of protocol in QI: Entanglement/Bell pair distillation for q. communication; Magic state distillation for fault-tolerant q. computation…

Here we provide a set of very general no-go theorems, which indicate that the possibility of improving distillation is subject to strong limitations. The results are obtained through properties of min and hypothesis testing relative entropies, which were connected to distillation just now.

No-go theorems for distillation

We say a resource state has free component if it takes the form $\rho = p\sigma + (1-p)\omega$ for some free state σ, p > 0.

Very generic. Every mixed state has free component as long as there exists some full-rank free state (e.g. the maximally mixed state).

Theorem (Deterministic distillation)

It is impossible to transform any resource state with free component to any pure target state with any deterministic map with arbitrarily small error.

We find a threshold error related to the minimum eigenvalue of the resource state and its overlap with the target state, s.t. any error below this threshold is not achievable.

No-go theorems for distillation

We further establish no-go for the more general probabilistic distillation setting, which is also important in practice.

Theorem (Probabilistic distillation)

E.g. depolarizing noise

It is impossible to distill any full-rank resource state to any target state such that $m_{min}>0$ with zero-error, even probabilistically.

Pretty much always hold

There is a trade-off between accuracy and success probability.

E.g. Conventional magic state distillation protocols (to turn noisy magic states into useful ones such as T-states, fundamental to fault-tolerant schemes, Clifford-magic models etc.): encode noisy states in error correcting code, syndrome measurement, decode upon certain outcomes.

Then our results says it's impossible to devise any procedure that produces perfect T-gates; also to achieve high accuracy one needs to use large codes or iterate for many times (which exponentially reduces success probability)

Main take-home messages

- The optimal rates of approximate resource formation tasks can generally be characterized by smooth max-relative entropy monotones and the smooth free log-robustness, while those for distillation can generally be characterized by hypothesis testing relative entropy monotones. (Unified operational interpretations of these resource measures)

- Give up on your dream for ideal resource distillation/purification: (in pretty much any case you might care about,) highly accurate distillation is impossible, and perfect distillation is impossible even probabilistically.

- Golden states (a notion of max-resource) are super nice resource currencies.

Magic state quantum computation

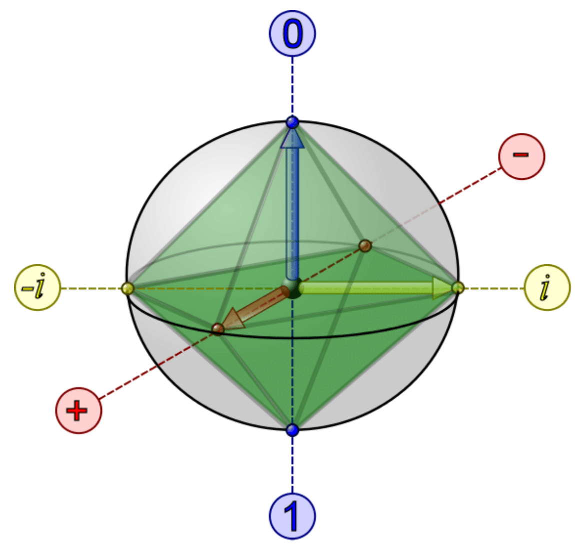
Clifford group: Preserves Pauli group $\{U : UPU^\dagger \in P_n, \forall P \in P_n\}$

Generated by {H, CNOT, S}

Phase shift $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Stabilizer states: Generated by Clifford group on trivial states

Magic states: Outside the convex hull (stabilizer polytope)



Stabilizer states and circuits are "useless" for q. computation: can be efficiently simulated classically [Gottesman-Knill Theorem] (Parity-L)

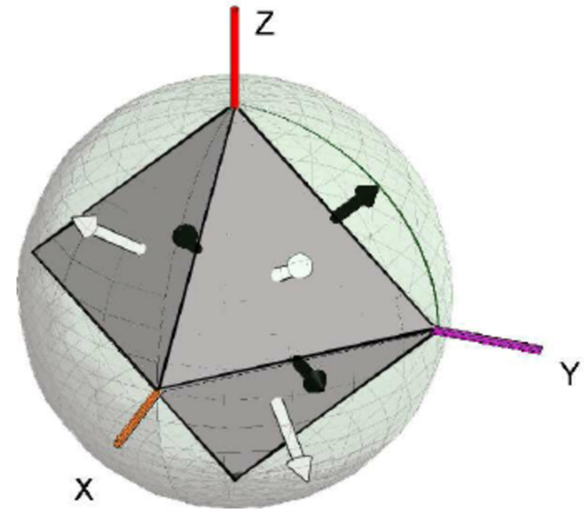
Magic states promote it to quantum universality (BQP)!

Magic state quantum computation

Commonly considered magic state: T-state and tensor products

$$|T\rangle = T|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$$

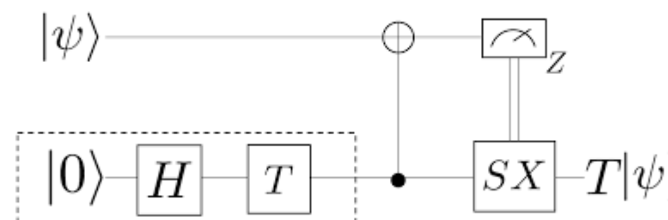
$$|T\rangle\langle T| = \frac{1}{2}\left(I + \frac{X+Y}{\sqrt{2}}\right)$$



Important resource for fault-tolerant q. computation scheme [Bravyi/Kitaev, PRA ’05...]:

Magic state distillation to prepare T-states $\longrightarrow$ State injection gadget to implement T-gates

$\Rightarrow$ Clifford circuits (fault-tolerant) + T-states



Magic state quantum computation

Therefore, T is a precious resource for quantum computation.

The number of T-gates/states (T-count) is an important figure of merit

Example: Of great interest recently—Complexity/cost of classical simulation in terms of T-count t

- Upper bound: Can do better than brute-force… Classical simulation algorithms s.t. the performance is determined by certain magic measures: Stabilizer rank ($\sim 2^{0.48t}$, pure states) [Bravyi/Gosset, PRL '16]; Free robustness ($\sim 2^{0.74t}$, all states) [Howard/Campbell, PRL '17, Heinrich/Gross, Quantum '18]
- Lower bound: Cannot be $2^{o(t)}$, conditioned on some reasonable conjectures [Morimae/Tamaki, 1901.01637]

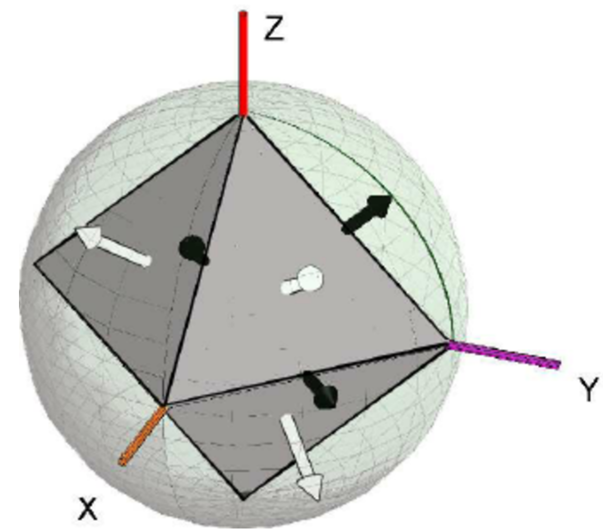
Magic state quantum computation

T-state is not golden (most powerful) state even for single qubit

Golden qubit state:

$$|G\rangle = \cos\phi|0\rangle + e^{i\pi/4}\sin\phi|1\rangle, \quad \cos(2\phi) = \frac{1}{\sqrt{3}}$$

$$|G\rangle\langle G| = \frac{1}{2}\left(I + \frac{X+Y+Z}{\sqrt{3}}\right)$$



A slightly different goal: Reduce the size of resource magic state for your quantum computation, by using more powerful magic states

[ZWL/Takagi, in preparation]

Magic state quantum computation

For illustration, some toy results by the one-shot theory:

□ Reduce qubit-count by using less G-states to get more T-states (say, then use the T-gadget). How well can we do it?

Calculate magic monotones/modification coefficients:

$$m_{\max,\min}(G^{\otimes n}) = \log(3-\sqrt{3}) \approx 0.34, \quad \mathfrak{D}_{\max,\min}(G^{\otimes n}) \approx 0.34n$$

$$m_{\max,\min}(T^{\otimes n}) = \log(4-2\sqrt{2}) \approx 0.23, \quad \mathfrak{D}_{\max,\min}(T^{\otimes n}) \approx 0.23n$$

Additivity of "Clifford-magic" states; Collapse due to convex duality [Bravyi et al]

$$LR(T^{\otimes n}) = 0.272, 0.458, 0.687, 0.950...$$

Not additive

- Perfect 2G $\longrightarrow$ 3T is impossible (max/max optimality bound)
- 3G $\longrightarrow$ 4T can be achieved by a stabilizer-preserving map with small error (D_H/LR distillation bound)

[ZWL/Takagi, in preparation]

Magic state quantum computation

□ Gate synthesis

E.g. Suppose you want to synthesize a Toffoli or CCZ gate. How many resource qubits are necessary?

$$m_{\max}(CCZ) = \log_2 \frac{2}{9} \approx 0.277$$

$$m_{\max}(G^{\otimes m}) = \log_2(3-\sqrt{3}) \approx 0.34$$

$$\xRightarrow{\text{Formation bounds}} \quad \Omega^0_{C,\mathscr{F}_{\mathrm{NG}}}(CCZ \leftarrow \{G^{\otimes m}\}) > 2.44$$

$\Rightarrow$ at least 3 for small error

Similarly we can use the one-shot results to get bounds on more general magic state manipulation (analyze T-count for gates/computation, noisy computation…). A more complete SDP formulation and probabilistic theory [in preparation]

[ZWL/Takagi, in preparation]

Toffoli + Hadamard model

- Another classical/quantum dichotomy: Toffoli (CCNOT) gates handle classical (diagonal) logic, but need quantum coherent superposition (created by e.g. Hadamard gate) to achieve quantum computation.   H-count!

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- Also a conditional exponential-time classical simulation theorem shown in [Morimae/Tamaki, 1901.01637]

- Here a “gadget” that turns resource states into H-gates is unknown; Existence seems to be in tension with certain complexity theory beliefs (Tomoyuki), so the state resource theory is not directly useful; Need the channel theory (a unified framework see [ZWL/Winter, 1904.04201])

A toy result: m T-gates require at least $m/\sqrt{2}$ H-gates

Outlook

- Bounds for other sets of free operations, such as non-generating/commuting operations with selective measurements
- More achievability bounds for distillation (some new results under the overlap formalism [Bu/ZWL/Regula/Takagi, in preparation])
- Necessary and sufficient conditions for arbitrary one-to-one conversion; Complete monotone
- Complete the one-shot channel theory ([ZWL/Winter, 1904.04201] mostly concerns the optimality side)
- Develop new juicers! (New general theories)
- Try your favorite fruit! (Apply the general framework to specific theories you care about)

Holographic “quantum” complexity?

- The conventional notion of complexity and the widely studied Nielsen's geometric approach is not fully rigorous (which is an intrinsic difficulty of the holographic complexity conjectures)...

- But we have rigorous tools to analyze “a certain type of” complexity, such as the number of “non-classical”/entangling gates, from resource theory.

- Helpful for more precise understandings of certain aspects of holographic complexity?

Thanks for your attention!

General framework paper: 1904.05840

An upcoming paper on separation of OTOC and entanglement in scrambling [Harrow/Kong/ZWL/Mehraban/Shor]

Most magical quantum states

Interesting case is not "stable"

Theorem (Typical stabilizer rank)

Set of n-qubit states with stabilizer rank $<2^n$ is of measure zero.

I.e. A typical/random pure state has maximum stabilizer rank 2^n

Idea: The non-maximal rank states form lower-dimensional manifolds in the parameter space, and there's only a finite number of such manifolds, which cannot cover the full manifold.

A corollary (Tomoyuki): Cannot improve brute-force simulation by the stabilizer rank method for almost any noisy/random input

If the conjecture is true, another intriguing no-go consequence: The most magical state cannot be transformed to almost any other state by Clifford circuits…

[ZWL/Takagi/Kong, in preparation]