Information-Theoretic Costs of Simulating Quantum Measurements

Mark M. Wilde

McGill University

Joint with
Patrick Hayden, **Francesco Buscemi**, and **Min-Hsiu Hsieh**

Quantum Information Seminar,
Perimeter Institute, Waterloo, Canada
April 18, 2012

Overview

•Review Winter's measurement compression protocol

•Introduce a new variation of the protocol

•Review classical data compression with QSI

•Introduce measurement compression with QSI

•Outline some applications of MC-QSI

POVMs

Recall:

Quantum state is a positive, unit trace operator ρ

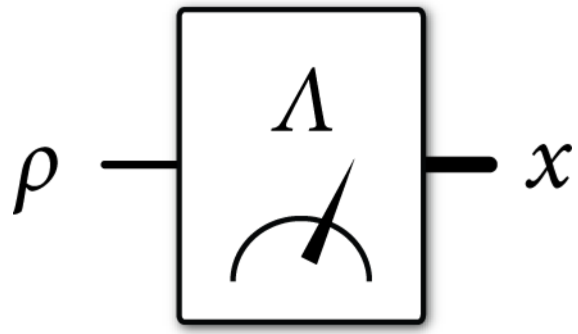
$$\rho \geq 0, \quad \mathrm{Tr}\{\rho\} = 1$$

Positive operator-valued measure is a collection $\Lambda = \{\Lambda_x\}$ such that

$$\sum_x \Lambda_x = I, \quad \forall x : \Lambda_x \geq 0$$

Probability of getting outcome x when performing Λ on ρ is

$$p_X(x) = \mathrm{Tr}\{\Lambda_x \rho\}$$

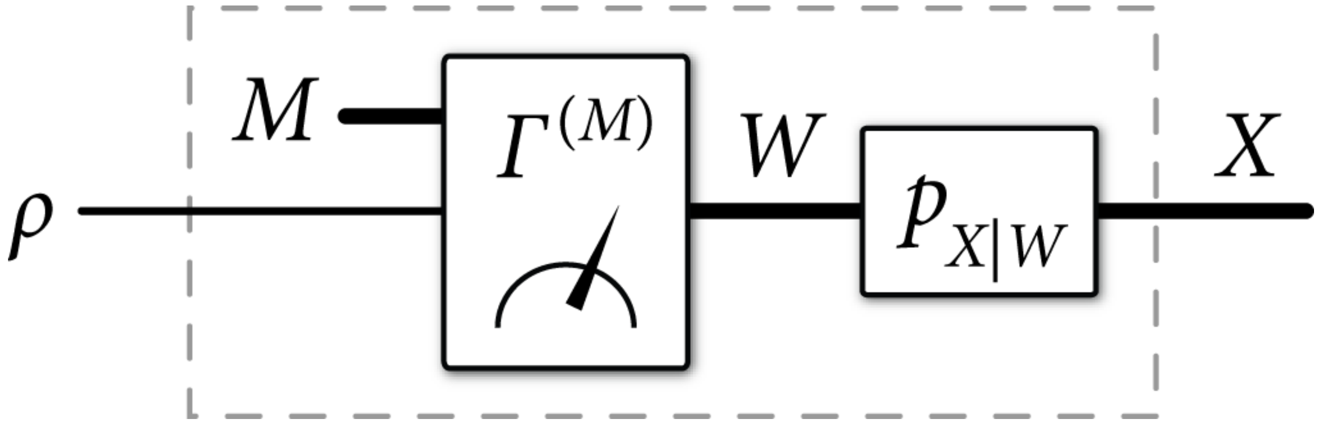


Decomposing POVMs

Just as density operators can represent **noisy quantum states**, so can POVMs represent **noisy measurements**...

Consider decomposing Λ as a **random selection** of a measurement according to M combined with a noisy post-processing $p_{X|W}(x|w)$:

$$\Lambda_x = \sum_{m,w} p_M(m)\,\Gamma_w^{(m)}\,p_{X|W}(x|w)$$



What are the communication costs of simulating quantum measurements?

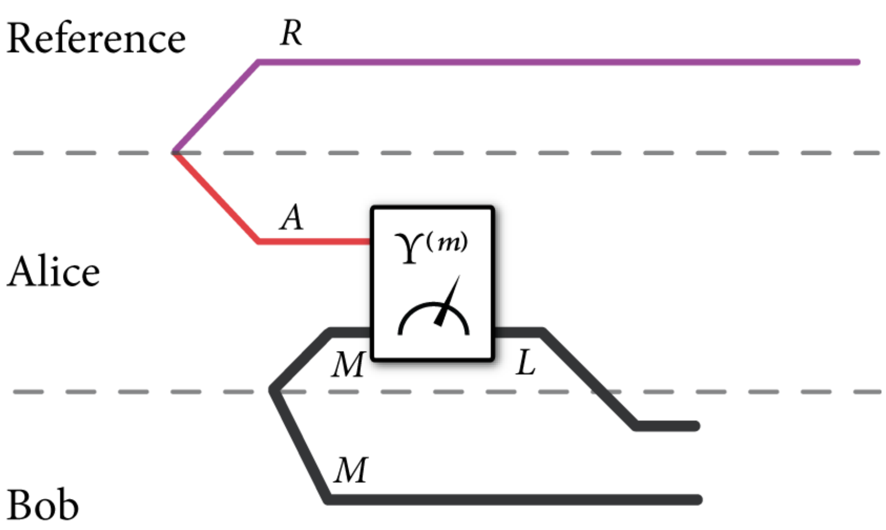
Example. Consider the following POVM:

$$\left\{ \frac{1}{2}|0\rangle\langle 0|,\ \frac{1}{2}|1\rangle\langle 1|,\ \frac{1}{2}|+\rangle\langle +|,\ \frac{1}{2}|-\rangle\langle -| \right\}$$

This measurement decomposes as a random choice of Pauli *X* or *Z*

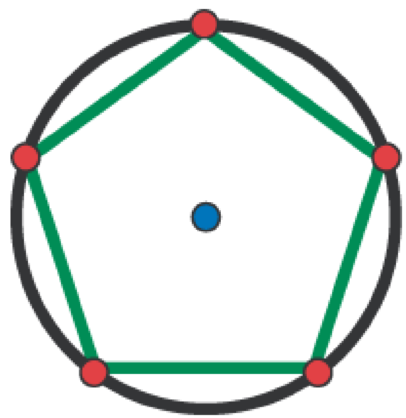
$$\left\{ \frac{1}{2}\left\{|0\rangle\langle 0|,\ |1\rangle\langle 1|\right\},\ \frac{1}{2}\left\{|+\rangle\langle +|,\ |-\rangle\langle -|\right\} \right\}$$

Protocol:

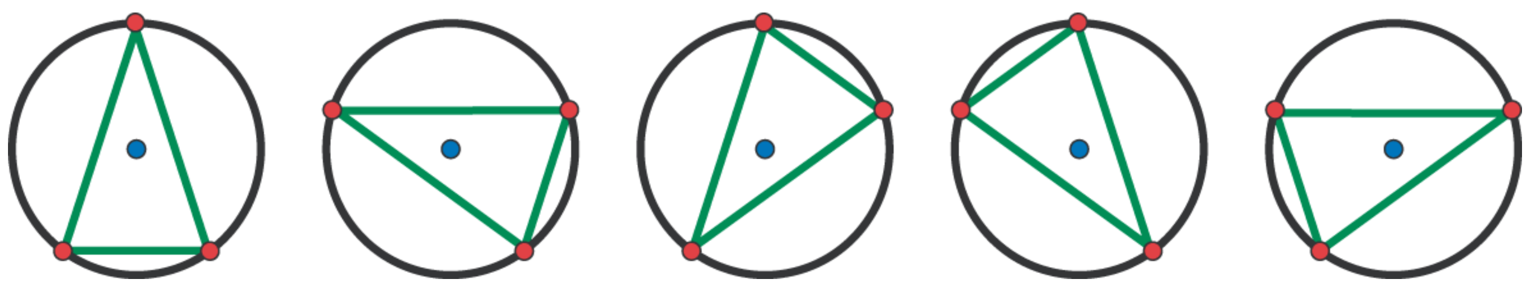


Another Example: Pentagon States

Example. Take a slice of the Bloch sphere that includes its center.
Consider 5 states that form a pentagon on the slice.
With appropriate weightings, these sum to the identity and form a POVM



Measurement decomposes as a random choice of 3-outcome measurements:



Simulate it with common randomness and classical communication

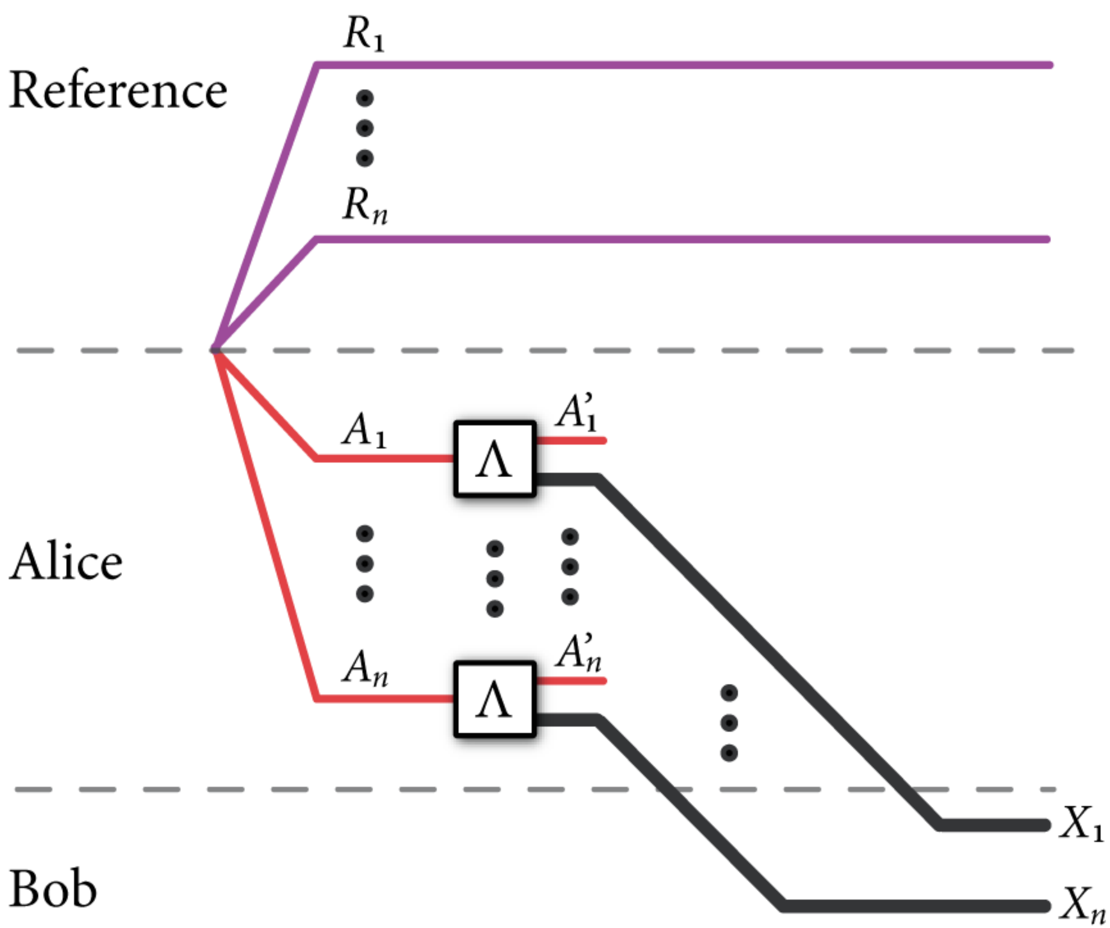
Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Measurement Compression

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Ideal Information Processing Task for Measurement Compression

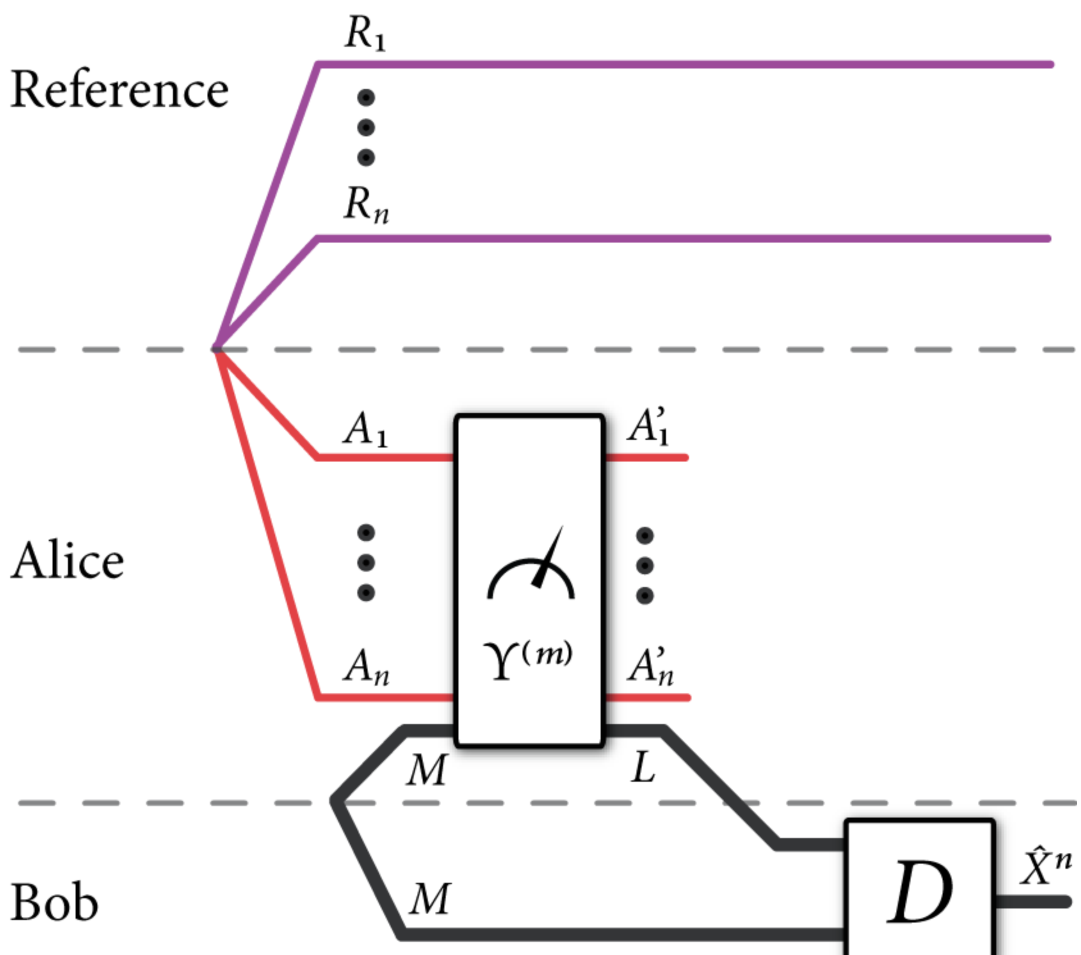
Go to the IID setting:



Andreas Winter. “Extrinsic” and “Intrinsic” Data in Quantum Measurements. arXiv:quant-ph/0109050

Actual Information Processing Task for Measurement Compression

Use common randomness, a collective measurement, and classical communication to simulate original measurement



Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Faithful Simulation

A measurement simulation is **faithful** if its action on an IID state is indistinguishable from the true measurement:

Definition 1 (Faithful simulation for purification) *A sequence of protocols provides a faithful simulation of the POVM Λ on the source ρ, if for a purification $|\phi_\rho\rangle$ of the source, the states on the reference and source systems after applying the measurement maps are ϵ-close in trace distance for all $\epsilon > 0$ and sufficiently large n:*

$$\left\| \left(\mathrm{id} \otimes \mathcal{M}_{\Lambda^{\otimes n}}\right) \left(\phi_\rho^{\otimes n}\right) - \left(\mathrm{id} \otimes \mathcal{M}_{\widetilde{\Lambda}^n}\right) \left(\phi_\rho^{\otimes n}\right) \right\|_1 \leq \epsilon. \tag{1}$$

$$\mathcal{M}_{\Lambda^{\otimes n}}(\sigma) \equiv \sum_{x^n} \mathrm{Tr}\left\{\Lambda_{x^n}\sigma\right\} |x^n\rangle\langle x^n|,$$

$$\mathcal{M}_{\widetilde{\Lambda}^n}(\sigma) \equiv \sum_{x^n} \mathrm{Tr}\left\{\widetilde{\Lambda}_{x^n}\sigma\right\} |x^n\rangle\langle x^n|.$$

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Measurement Compression Theorem

Theorem 1 (Measuremen Groenewold's information gain (1971)
and Λ a POVM to simulate on this state. A protocol for faithful simulation of the POVM is achievable with classical communication rate R and common randomness rate S if and only if the following set of inequalities hold

$$R \geq I(X;R),$$
$$R + S \geq H(X),$$

where the entropies are with respect to a state of the following form:

$$\sum_x |x\rangle\langle x|^X \otimes \mathrm{Tr}_A\{(I^R \otimes \Lambda^A)\phi^{RA}\} \tag{1}$$

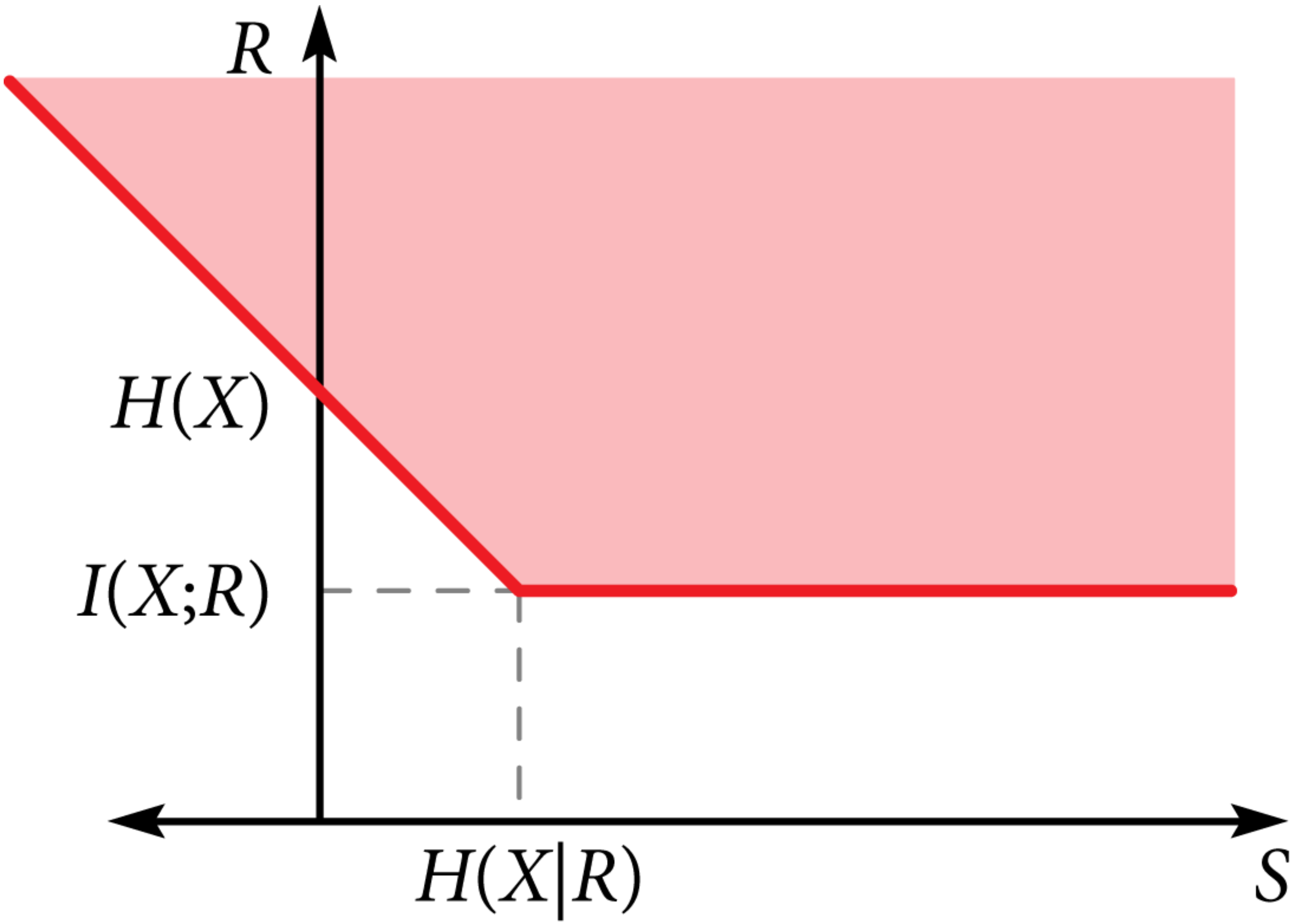
Shannon entropy

and ϕ^{RA} is some purification of the state ρ.

This holds for a "feedback" simulation in which
Alice also gets the output of the simulated measurement.

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Measurement Compression Region



Notable rate pairs correspond to measurement compression and Shannon compression (*also Shannon compression combined with c. comm. to comm. rand.*)

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Achievability

Resource inequality for measurement compression:

$$I\left(X;R\right)[c \to c] + H\left(X|R\right)[cc] \geq \left\langle \Lambda\left(\rho\right)\right\rangle$$

Consider POVM Λ and state ρ leads to the following ensemble:

$$p_X(x) = \mathrm{Tr}\{\Lambda_x \rho\}$$

$$\hat{\rho}_x = \frac{1}{p_X(x)}\sqrt{\rho}\Lambda_x\sqrt{\rho}$$

Can think that the goal is to "steer" the reference to be as above

Do this with $\sqrt{\text{measurement}}\ \ \{\rho^{-1/2}\, p_X(x)\hat{\rho}_x\, \rho^{-1/2}\}$

How to do this approximately?

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Achievability (Ctd.)

Select $|L||M|$ codewords $x^n(l,m)$ according to $p_{X^n}(x^n)$ where

$$|\mathcal{L}| \approx 2^{nI(X;R)}$$

$$|\mathcal{M}| \approx 2^{nH(X|R)}$$

$$|\mathcal{L}|\,|\mathcal{M}| \approx 2^{nH(X)}$$

Exploit the **Ahlswede-Winter Operator Chernoff bound** to guarantee that

$$\frac{1}{|\mathcal{L}|}\sum_{l} \hat{\rho}_{x^n(l,m)} \approx \rho^{\otimes n}$$

This first condition is helpful in constructing a POVM for each *m*

$$\frac{1}{|\mathcal{L}|\,|\mathcal{M}|}\left|\{l,m : x^n(l,m) = x^n\}\right| \approx p_{X^n}(x^n)$$

This second condition is helpful in proving that the **simulation is faithful**

Andreas Winter. "Extrinsic" and "Intrinsic" Data in Quantum Measurements. arXiv:quant-ph/0109050

Single-Letter Converse

Single-letter converse → the rates in the theorem are optimal

$$R \geq I(X;R)$$
$$R + S \geq H(X)$$

Happens more often in QIT when resources are **hybrid** (quantum and classical)

Main steps are just to think about the most general protocol for this task and exploit **quantum data processing inequality**

Non-feedback Measurement Compression

Wilde, Hayden, Buscemi, and Hsieh (2012).

Nonfeedback Measurement Compression

Suppose that POVM $\{\Lambda\}$ has a decomposition as

$$\Lambda_x = \sum_w p_{X|W}(x|w) M_w$$

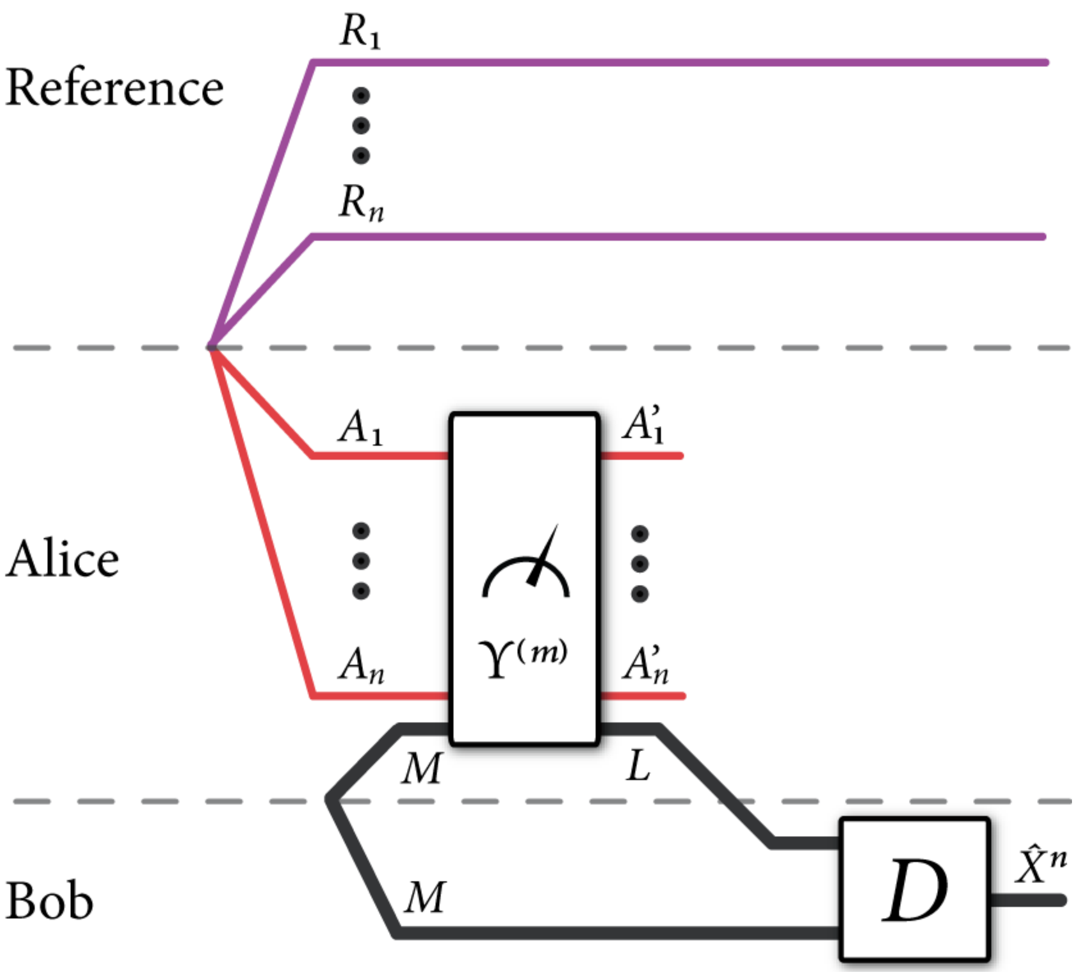
It would then be possible to simulate $\{M_w\}$ first, followed by Bob locally simulating X from W

Is there a benefit in doing so?

Wilde, Hayden, Buscemi, and Hsieh (2012).

Non-feedback Measurement Compression

Simulation is such that Alice does not require measurement output



Wilde, Hayden, Buscemi, and Hsieh (2012).

Nonfeedback Measurement Compression

Achievability follows by employing a variation of Winter's measurement compression protocol:

$$I\left(W;R\right)\left[c\rightarrow c\right]+I\left(W;X|R\right)\left[cc\right]\geq\left\langle \Lambda\left(\rho\right)\right\rangle$$

No need for as much common randomness consumption because Bob simulates $p_{X|W}(x|w)$ locally

Total rate of **common randomness consumption** is then $I(W;X|R)$ for a total classical cost of $I(W;XR)$

Single-letter converse follows from a technique similar to that of Paul Cuff (arXiv:0805.0065) adapted to the quantum case

Nonfeedback Measurement Compression

Theorem 1 (Non-feedback measurement compression theorem) *Let ρ be a source state and $\mathcal{N}$ a quantum instrument to simulate on this state:*

$$\mathcal{N}(\rho) = \sum_x \mathcal{N}_x(\rho) \otimes |x\rangle\langle x|^X .$$

A protocol for faithful simulation of the quantum instrument is achievable with classical communication rate R and common randomness rate S if and only if R and S are in the rate region given by the union of the following regions:

$$R \geq I(W;R),$$
$$R + S \geq I(W;XR),$$

where the entropies are with respect to a state of the following form:

$$\sum_{x,w} p_{X|W}(x|w)\,|w\rangle\langle w|^W \otimes |x\rangle\langle x|^X \otimes \mathrm{Tr}_A\left\{\left(I^R \otimes \mathcal{M}_w^A\right)\left(\phi_\rho^{RA}\right)\right\}, \qquad (1)$$

Total cost can be lower

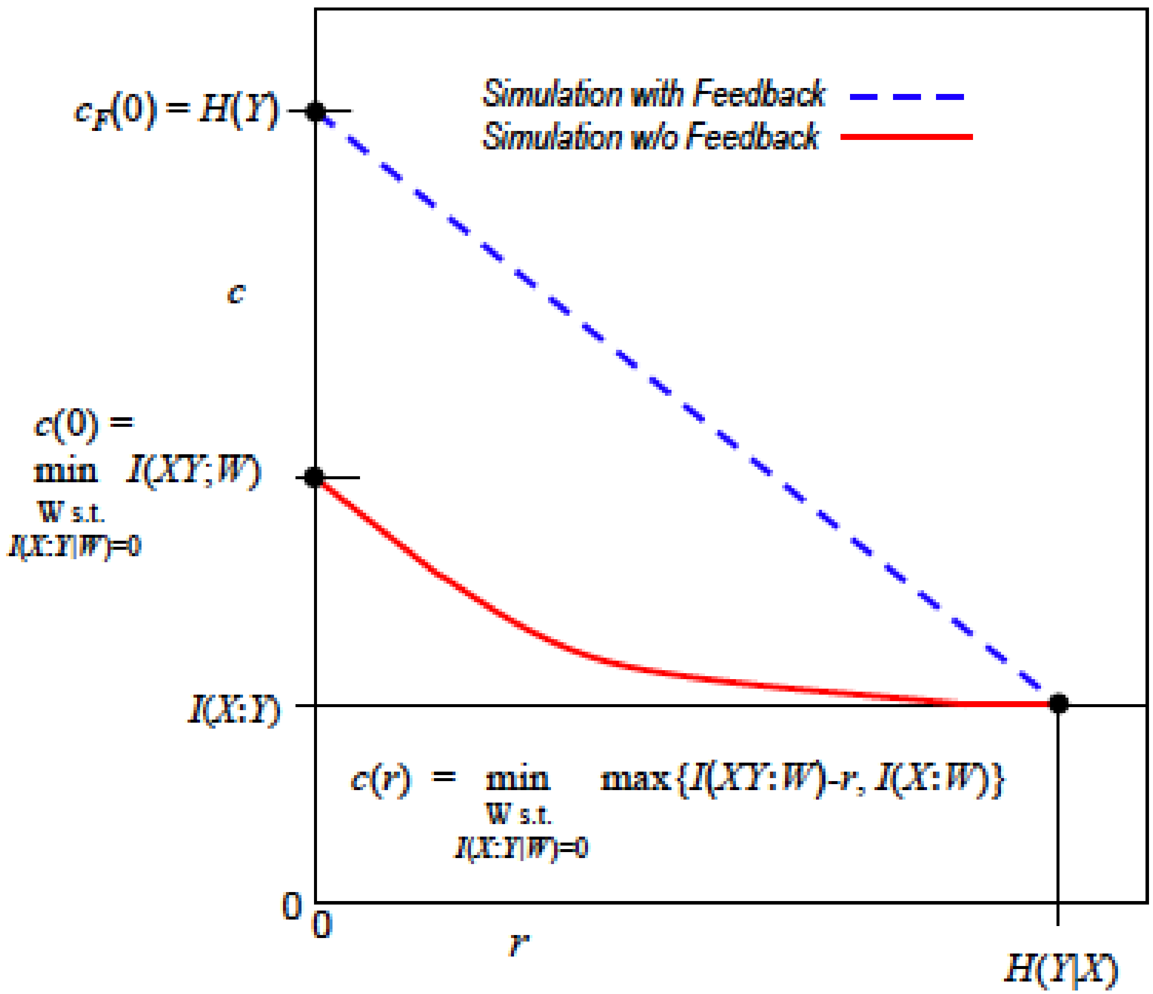
ϕ_ρ^{RA} is some purification of the state ρ, and the union is with respect to all decompositions of the original instrument $\mathcal{N}$ of the form:

$$\mathcal{N}(\rho) = \sum_{x,w} p_{X|W}(x|w)\,\mathcal{M}_w(\rho) \otimes |x\rangle\langle x|^X, \qquad (2)$$

such that $R - W - X$ is a quantum Markov chain.

Nonfeedback Measurement Compression

Example plot of trade-off improvement:



Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor and Andreas Winter. 0912.5537

Classical Data Compression with Quantum Side Information

Devetak and Winter. arXiv:quant-ph/0209029

Classical Data Compression with Quantum Side Information

Consider an ensemble of the following form:

$$\{p_X(x), \rho_x\}$$

Suppose that an **information source** generates a classical sequence x^n and quantum state ρ_{x^n}

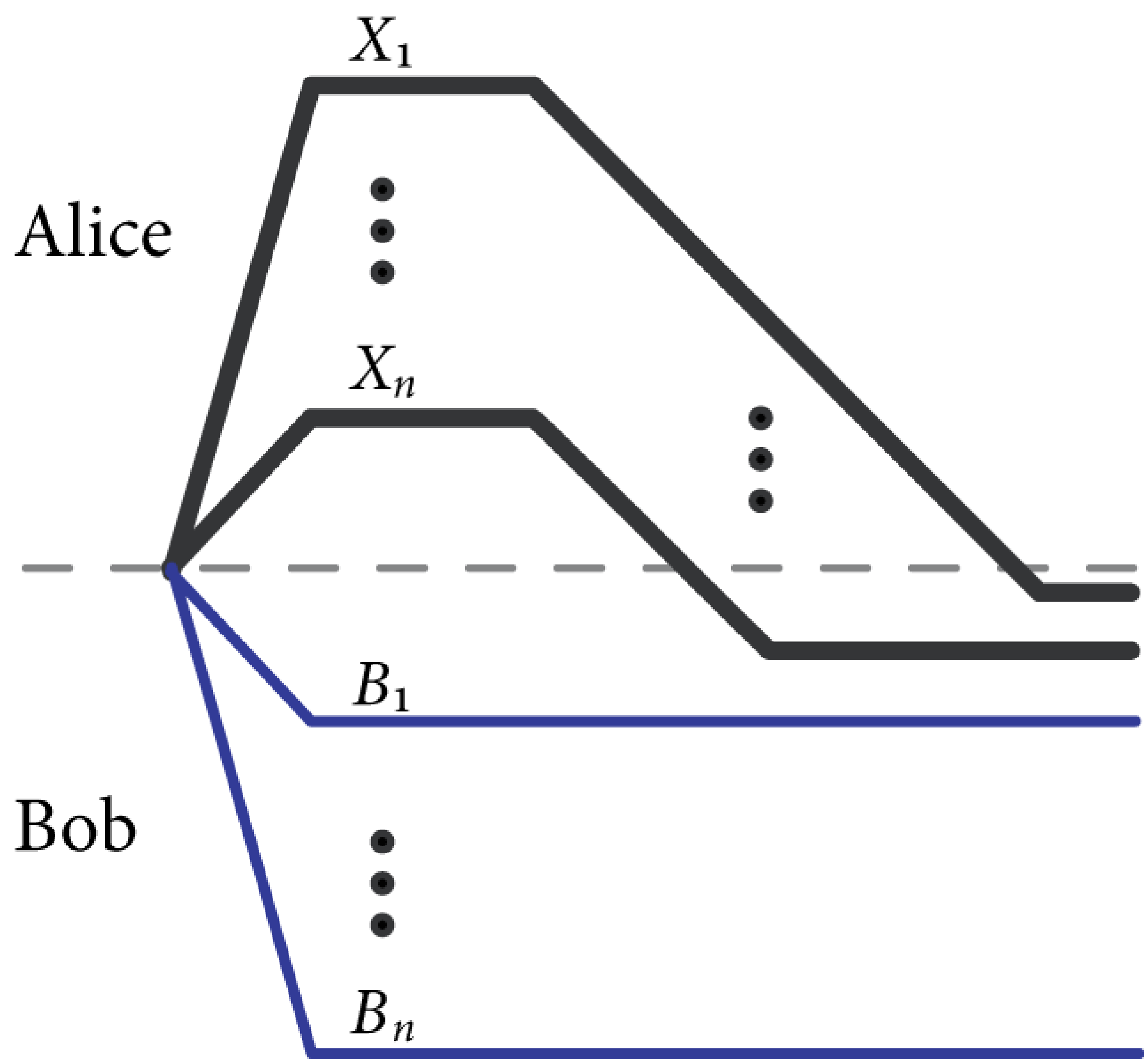
It gives the classical sequence to Alice and the quantum state to Bob

Question: *How much classical communication is needed for Bob to recover x^n?*

Could just Shannon compress x^n, but we can do better with QSI...

Devetak and Winter. arXiv:quant-ph/0209029

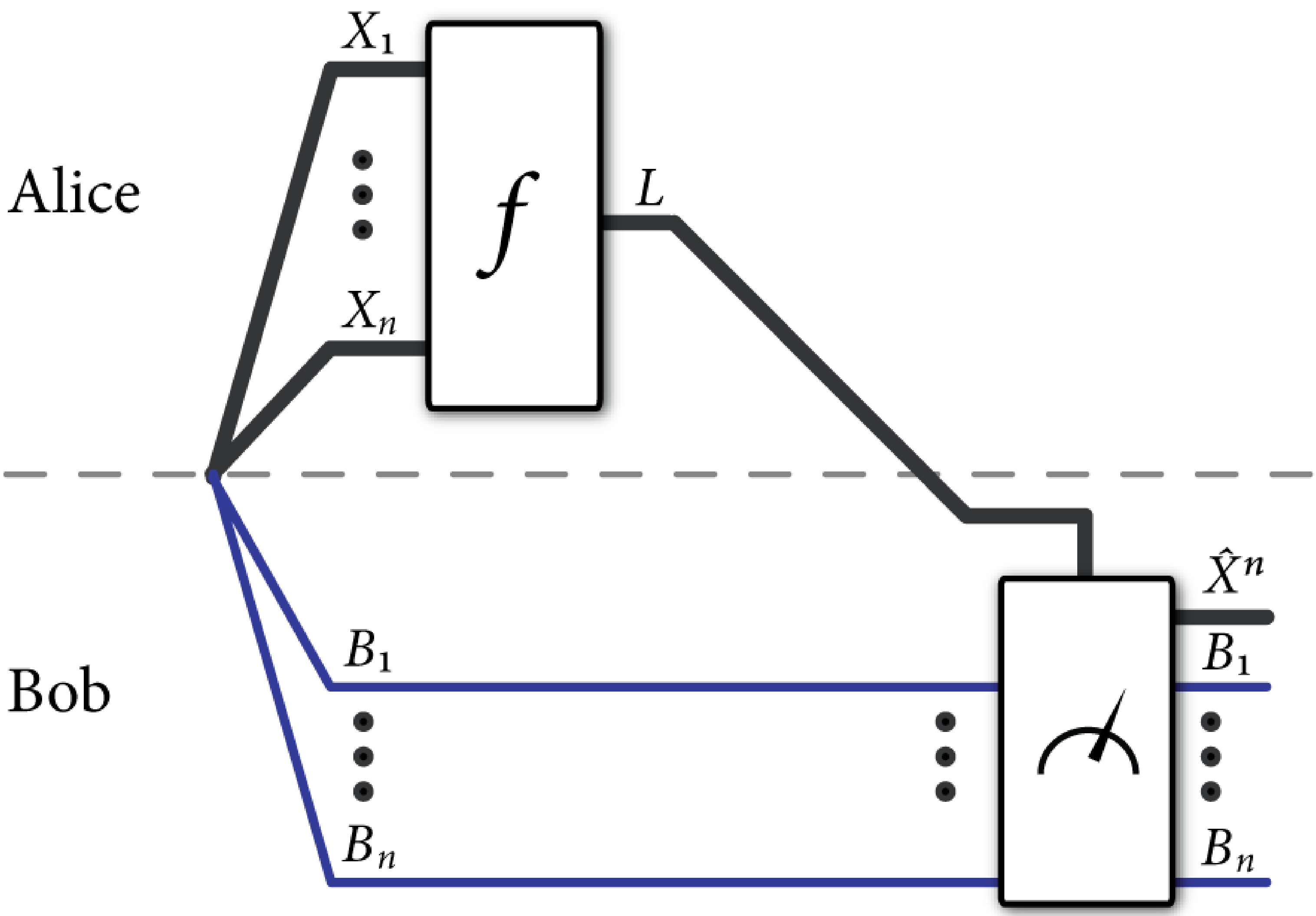
Ideal Protocol for CDC-QSI



In the ideal protocol, Alice just sends the classical sequence to Bob.

Devetak and Winter. arXiv:quant-ph/0209029

Actual Protocol for CDC-QSI



1) Alice hashes the classical sequence and sends Bob the hash

2) Bob performs a “gentle” quantum measurement conditional on the hash value to recover x^n

CDC-QSI Theorem

Theorem 1 (Classical data compression with quantum side information) *Suppose that*

$$\sum_x p_X(x) |x\rangle\langle x|^X \otimes \rho_x^B$$

is a classical-quantum state that characterizes a classical-quantum source. Then the conditional von Neumann entropy $H(X|B)$ *is the smallest possible achievable rate for classical data compression with quantum side information for this source:*

$$\inf\{R \mid R \text{ is achievable}\} = H(X|B).$$

Intuition:

There are $nH(X)$ bits needed to describe the classical sequence x^n

Bob can recover $nI(X;B)$ bits about x^n by measuring his state ρ_{x^n}

Alice needs to send the difference $n[H(X) - I(X;B)] = nH(X|B)$

Devetak and Winter. arXiv:quant-ph/0209029

Achievability

Resource inequality for CDC-QSI:

$$\langle \rho^{XB} \rangle + H(X|B)[c \to c] \geq \langle \rho^{XX_B B} \rangle$$

New proof strategy exactly like classical Slepian-Wolf protocol

Before communicating, Alice throws the typical sequences into **random bins**. After doing so, this establishes a code and our assumption is that Bob knows the assignments.

What's different: Bob receives hash from Alice, and scans over all of the quantum states consistent with the hash value. He performs sequential binary projective measurements asking, "*Does my quantum state correspond to the m^{th} sequence consistent with the hash*?"

Wilde, Hayden, Buscemi, Hsieh (2012)

Single-Letter Converse

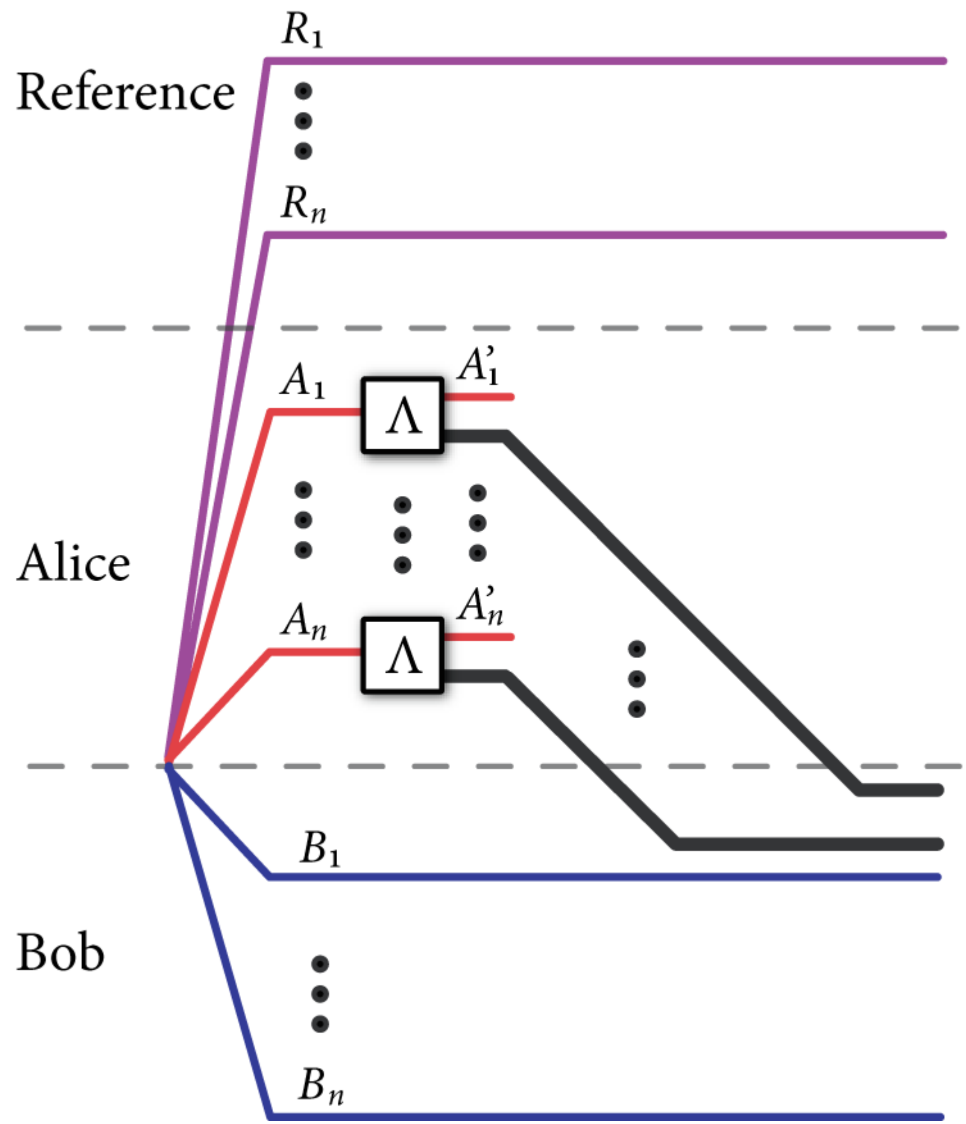
Main steps are just to think about the most general protocol for this task and exploit quantum data processing inequality

$$
\begin{aligned}
nR &\geq H(L) \\
&\geq H(L|B^n) \\
&\geq I(X^n; L|B^n) \\
&= H(X^n|B^n) - H(X^n|LB^n) \\
&\geq H(X^n|B^n)_\omega - H(X^n|\hat{X}^n)_\omega \\
&\geq H(X^n|B^n)_\sigma - n\epsilon' \\
&= nH(X|B) - n\epsilon'.
\end{aligned}
$$

Measurement Compression with Quantum Side Information

Wilde, Hayden, Buscemi, and Hsieh (2012).

Ideal MC-QSI Protocol

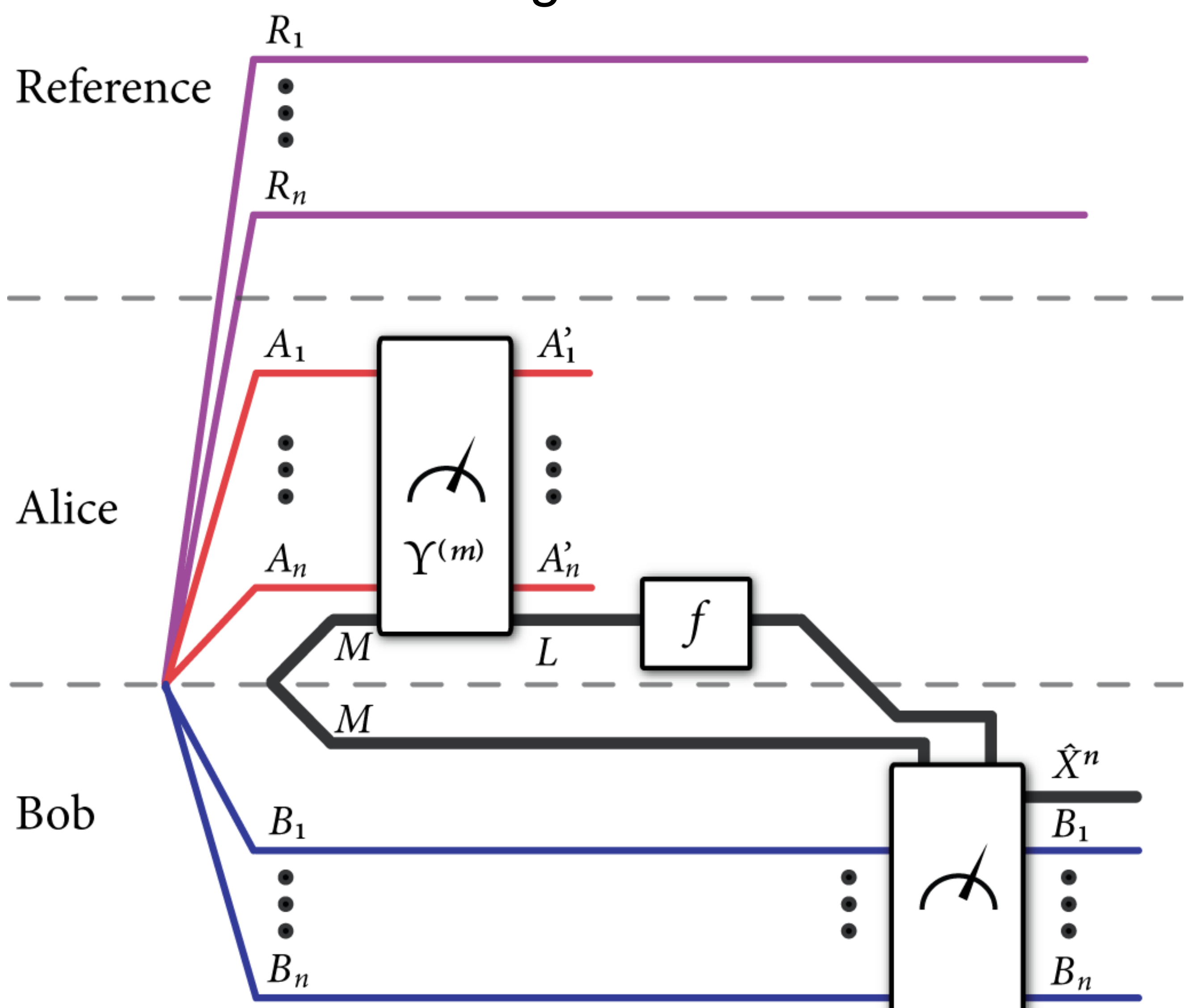


Alice and Bob share many copies of state ρ^{AB}

Goal is for Alice and Bob to simulate ideal measurement and for Bob's state not to be disturbed

Actual MC-QSI Protocol

Use common randomness, an Alice collective measurement, classical communication, and a Bob collective measurement to simulate original measurement



Wilde, Hayden, Buscemi, and Hsieh (2012).

Achievability

Resource inequality for CDC-QSI:

$$\langle \rho^{AB} \rangle + I(X;R|B)[c \to c] + H(X|RB)[cc] \geq \langle \Lambda^{A}(\rho^{AB}) \rangle$$

Proof strategy combines ideas from MC and CDC-QSI
(*though not possible to concatenate protocols with resource calculus*)

Choose an MC protocol randomly as before. Choose a hash function randomly as well. Can show there exists a choice of these that works well.

Operation: Alice performs simulation measurement, hashes the outcome, and sends it to Bob.
Bob receives hash from Alice, and scans over all of the post-measurement states consistent with the hash value.
He performs sequential binary projective measurements asking, "*Does my quantum state correspond to the m^{th} measurement outcome consistent with the hash*?"

MC-QSI Theorem

Theorem 1 (Measurement compression with QSI) *Let ρ^{AB} be a source state shared between a sender A and a receiver B, and let Λ be a POVM to simulate on the A system of this state. A protocol for faithful simulation of the POVM is achievable with classical communication rate R and common randomness rate S if and only if the following set of inequalities hold*

$$R \geq I(X;R|B),$$
$$R + S \geq H(X|B),$$

where the entropies are with respect to a state of the following form:

$$\sum_x |x\rangle\langle x|^X \otimes \mathrm{Tr}_A\left\{\left(I^R \otimes \Lambda_x^A\right)\phi^{RAB}\right\},$$

and ϕ^{RAB} is some purification of the state ρ^{AB}.

This holds for a "feedback" simulation in which Alice also gets the output of the simulated measurement.

Wilde, Hayden, Buscemi, and Hsieh (2012).

Single-Letter Converse

Single-letter converse → the rates in the theorem are optimal

Main steps are just to think about the most general protocol for this task and exploit quantum data processing inequality

Also, *we require that the protocol causes only a negligible disturbance to Bob's state*

$$R \geq I(X;R|B)$$

$$R + S \geq H(X|B)$$

This is for feedback case in which Alice gets a copy of measurement outcome

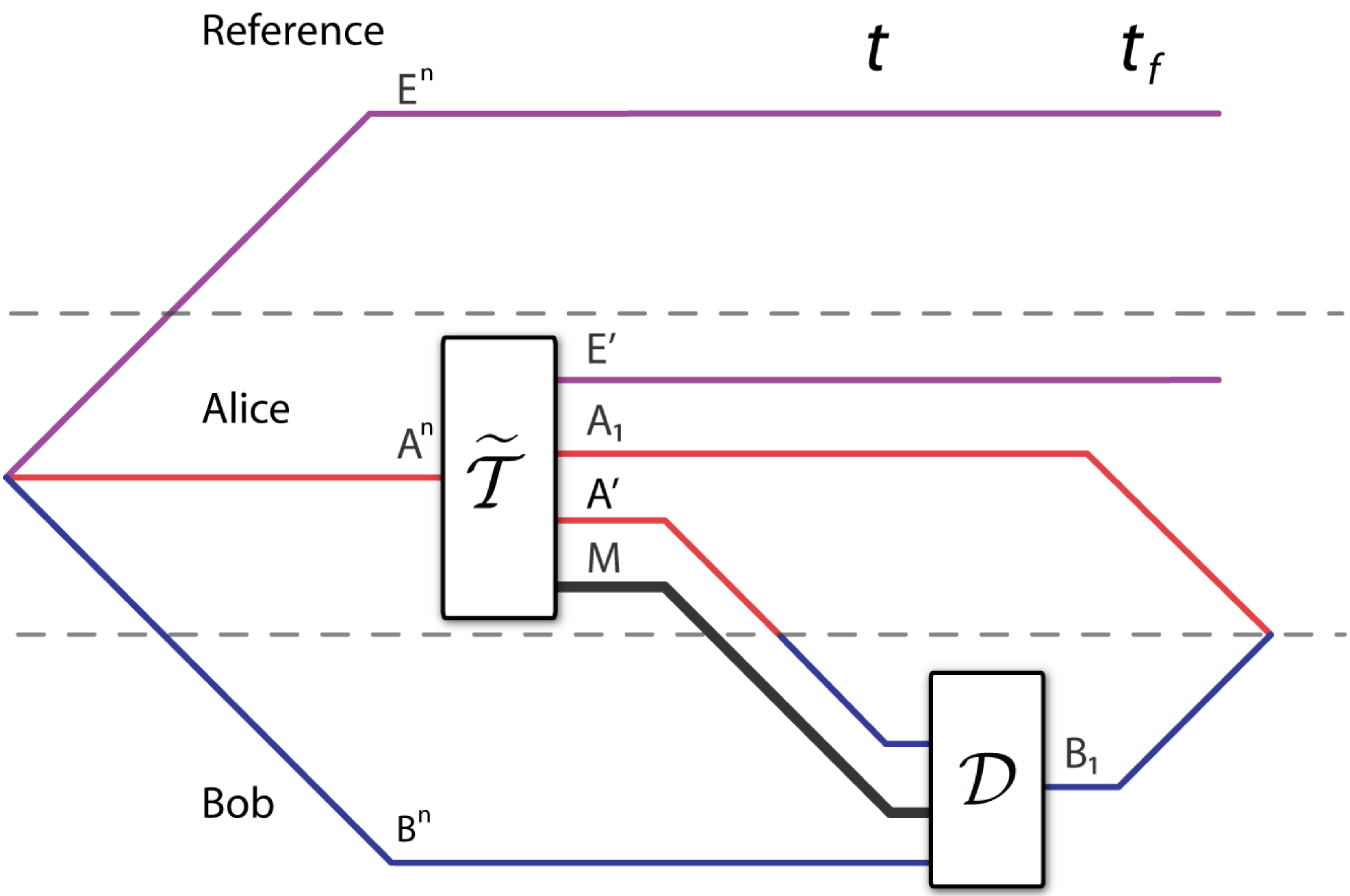
Applications of MC-QSI

1) Classically assisted state redistribution

2) Quantum reverse Shannon theorem for a quantum instrument

3) Local purity distillation

Classically assisted state redistribution



Most general protocol for entanglement distillation with the help of classical and quantum communication

Classically-assisted state redistribution

Begin with state ρ^{AB} that has purification ψ^{ABE}

Perform **MC-QSI**

Requires $I(X_B; E|B)$ rate of classical communication

Then perform **Quantum State Redistribution** conditional on classical information

$$\langle \rho^{AB} \rangle + I\left(X_B; E|B\right)_\sigma [c \to c] + \frac{1}{2} I\left(A'; E|E' X_B\right)_\sigma [q \to q] \geq \frac{1}{2}\left(I\left(A'; B|X_B\right)_\sigma - I\left(A'; E'|X_B\right)_\sigma\right)[qq]$$

Classically-assisted state redistribution

Quantum Reverse Shannon Theorem for a Quantum Instrument

We have a reverse Shannon theorem for a quantum channel

We have a reverse Shannon theorem for a POVM

What about for a quantum instrument with classical and quantum outputs?

Protocol is to perform measurement compression followed by FQRS:

$$I(X;R)[c \to c] + H(X|R)[cc] + \frac{1}{2} I(B';R|X)[q \to q] + \frac{1}{2} I(B';E|X)[qq] \geq \langle U_{\mathcal{N}}^{A \to X X_E B' E} : \rho^A \rangle.$$

Reverse Shannon theorem when QSI is available:

$$\langle \rho^{AB} \rangle + I(X;R|B)[c \to c] + H(X|RB)[cc] + \frac{1}{2} I(B';R|BX)[q \to q] + \frac{1}{2}\left(I(B';E|X) - I(B';B|X)\right)[qq] \geq \langle U_{\mathcal{N}}^{A \to X X_E B' E} : \rho^{AB} \rangle$$

Local Purity Distillation

Paradigm: Alice and Bob share a state
Their goal is to distill local pure states
using classical communication and local unitaries

By using MC-QSI, we have the following improvement to Krovi-Devetak 0705.4089

Theorem 1 *The 1-way distillable local purity of the state* ρ^{AB} *is given by* $\kappa_{\rightarrow} = \kappa^*_{\rightarrow}$, *where*

$$\kappa^*_{\rightarrow}\left(\rho^{AB}, R\right) = \kappa\left(\rho^{A}\right) + \kappa\left(\rho^{B}\right) + P_{\rightarrow}\left(\rho^{AB}, R\right).$$

In the above, we have the definitions

$$\kappa\left(\omega^C\right) \equiv \log d_C \cdots$$

Lower classical comm. cost

$$P_{\rightarrow}\left(\rho^{AB}, R\right) \equiv \lim_{k\rightarrow\infty} \frac{1}{k} P^{(1)}\left(\left(\rho^{AB}\right)^{\otimes k}, kR\right)$$

and

$$P^{(1)}\left(\rho^{AB}, R\right) \equiv \max_{\Lambda} \left\{ I\left(Y;B\right)_{\sigma} : I\left(Y;E|B\right) \leq R \right\},$$

$$\sigma^{YBE} \equiv \left(\mathcal{M}_{\Lambda} \otimes I^{BE}\right)\left(\psi^{ABE}\right),$$

where ψ^{ABE} *is a purification of* ρ^{AB}, $\mathcal{M}_{\Lambda}$ *is a measurement map corresponding to the POVM* Λ, *and the maximization is over all POVMs mapping Alice's system* A *to a classical system* Y.

Conclusion and Current Work

Measurement compression gives a powerful
operational way for understanding quantum measurement

We have extended Winter's original protocol in two ways:

1) **Nonfeedback measurement compression**
2) **Measurement compression with QSI**

In progress:

Figuring out nonfeedback measurement compression w/ QSI

Good open question:

Prove measurement compression theorem so that protocol
does not depend on structure of input state