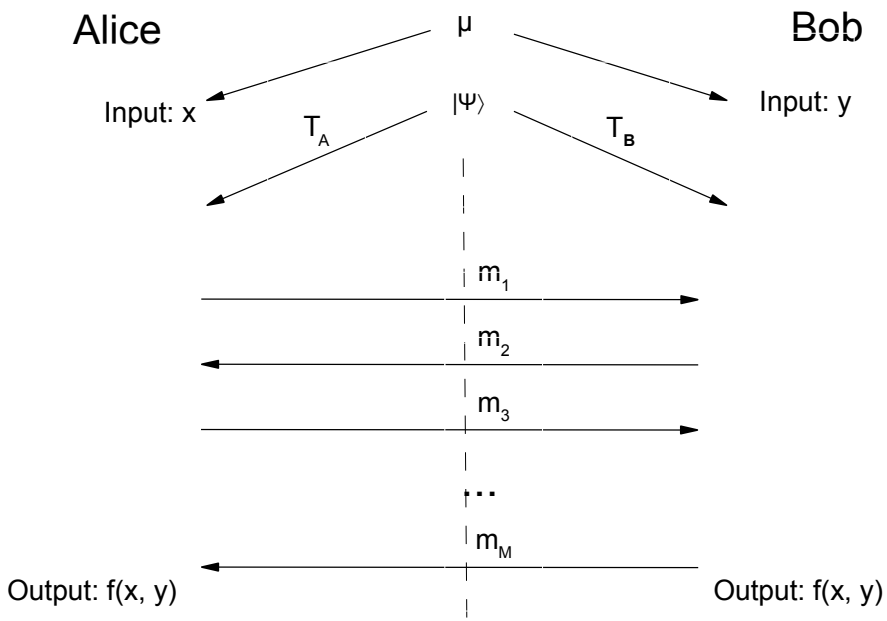
Quantum Information Complexity

Dave Touchette
University of Waterloo, Perimeter Institute, Université de Montréal

Beyond iid in information theory,
BIRS, Banff, 2015

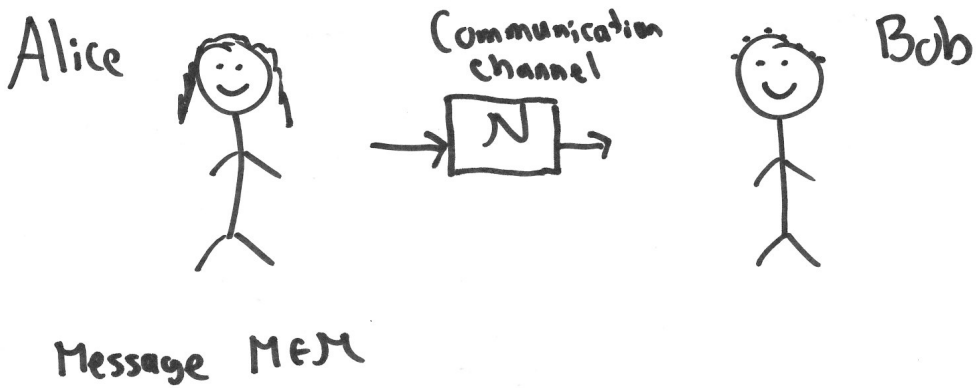
Interactive Quantum Communication

- Communication complexity setting:



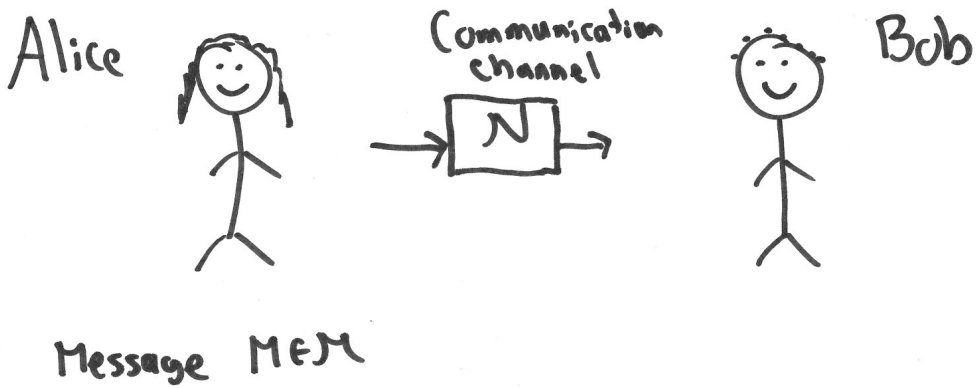
- Information-theoretic view: quantum information complexity
  - How much quantum **information** to compute f on μ
- Information content of interactive quantum protocols?

Unidirectional Classical Communication



- Separate into 2 prominent communication problems
  - Compress messages with "low information content"
  - Transmit messages "noiselessly" over noisy channels

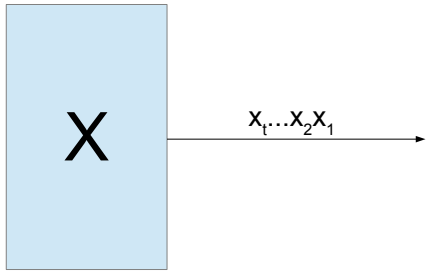
Unidirectional Classical Communication



- Separate into 2 prominent communication problems
  - **Compress** messages with "low information content"
  - Transmit messages "noiselessly" over noisy channels

Information Theory

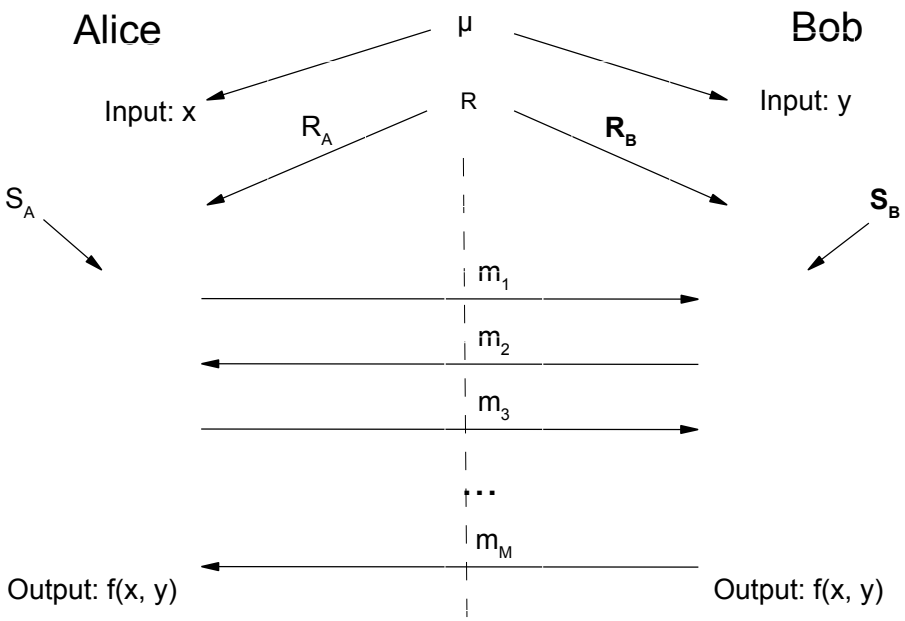
- How to quantify information?
- Shannon's entropy!
- Source X of distribution p_X has entropy $H(X) = -\sum_x p_X(x) \log(p_X(x))$ bits
- Operational significance: optimal asymptotic rate of compression for i.i.d. copies of source X:



- One-shot, average length: Huffman encoding $\leq H(X) + 1$
- Derived quantities: conditional entropy $H(X|Y)$, mutual information $I(X : Y)$, conditional mutual information $I(X : Y|Z)$ ...

Interactive Classical Communication

- Communication complexity of tasks, e.g. bipartite functions



- $m_1 = f_1(x, r, s_A), m_2 = f_2(y, m_1, r, s_B), m_3 = f_3(x, m_1, m_2, r, s_B), \cdots$
- Protocol transcript $\Pi(x, y, r, s) = m_1 m_2 \cdots m_M$
- Classical protocols: Π memorizes whole history
- $CC(f, \mu, \epsilon) = \min_\Pi CC(\Pi)$
- $CC(\Pi) = |m_1| + |m_2| + \cdots + |m_M|$

Coding for Interactive Protocols

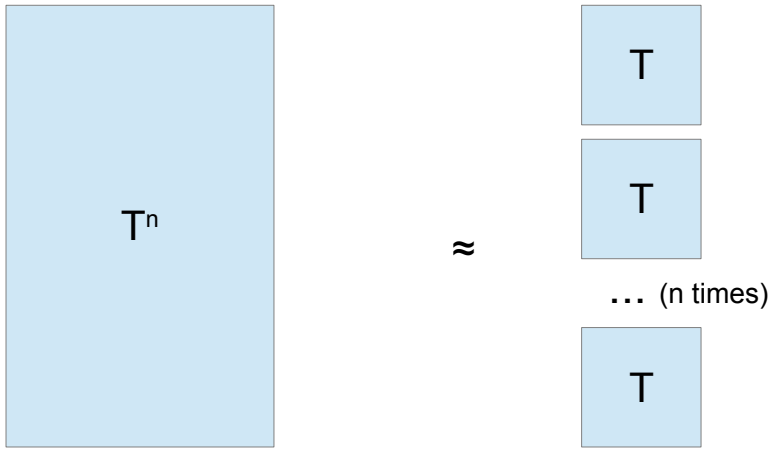
- Protocol compression
  - Can we compress protocols that "do not convey much information"
    - ★ For many copies run in parallel?
    - ★ For a single copy?
  - What is the amount of information conveyed by a protocol?
    - ★ Total amount of information at end of protocol?
    - ★ Optimal asymptotic compression rate?

Protocol Compression: Classical Information Complexity

- Information complexity: $IC(f, \mu, \epsilon) = \inf_{\Pi} IC(\Pi, \mu)$
- Information cost: $IC(\Pi, \mu) = I(X : \Pi | Y) + I(Y : \Pi | X)$
  - Amount of information each party learns about the other's input from the final transcript
- Important properties:
  - Additivity: $IC(T_1 \otimes T_2) = IC(T_1) + IC(T_2)$
  - Lower bounds communication: $IC(T) \leq CC(T)$
  - Operational interpretation: $IC(T) = ACC(T) = \lim_{n \to \infty} \frac{1}{n} CC(T^{\otimes n})$ [BR11]
  - Direct sum on composite functions, e.g. $DISJ_n$ from AND
  - Convexity, Concavity, Continuity, etc.

Applications of Classical IC I

- Direct sum: $CC((f,\epsilon)^{\otimes n}) \geq \Omega(n \cdot CC(f,\epsilon))$? [BBCR10, BR11, ...]
- Remember $IC(f,\epsilon) = \lim_{n\to\infty} \frac{1}{n} CC\left((f,\epsilon)^{\otimes n}\right)$
  - Direct sum related to one-shot compression down to IC

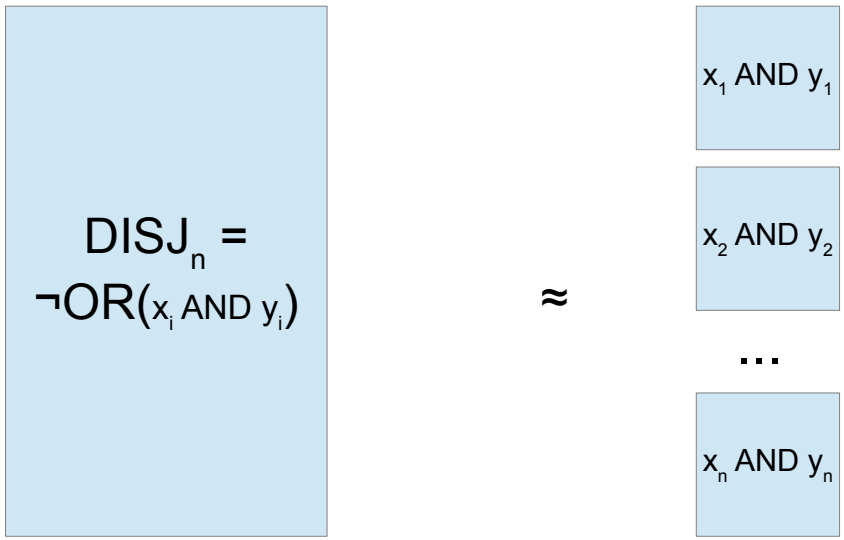


Applications of Classical IC I

- Direct sum: $CC((f,\epsilon)^{\otimes n}) \geq \Omega(n \cdot CC(f,\epsilon))$? [BBCR10, BR11, ...]
- Remember $IC(f,\epsilon) = \lim_{n\to\infty} \frac{1}{n} CC\left((f,\epsilon)^{\otimes n}\right)$
  - Direct sum related to one-shot compression down to IC
- BBCR10 : can compress to $\tilde{O}(\sqrt{CC \cdot IC})$
  - on product distributions: compress down to $\tilde{O}(IC)$
  - must compress simultaneously multiple rounds of low information
- BR11 : can compress to $O(IC + r)$ for r rounds
  - One-shot, average length version of S-W
  - Interactive protocol
  - $H(X|Y)+$ lower order terms
  - $I(X : M|Y) + \cdots$, for message M generated from X

Applications of Classical IC II

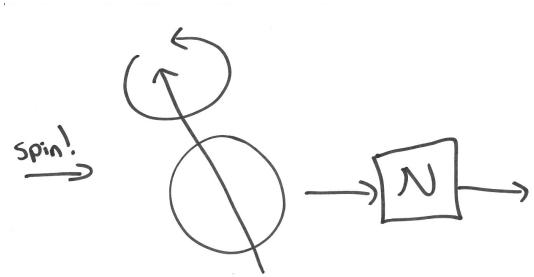
- Exact communication complexity bound!! [BGPW13]
  - E.g. $CC(DISJ_n) = 0.4827 \cdot n \pm o(n)$
- $IC_0(Disj_n) = n \cdot IC_0(AND)$
- $IC_0^r(AND) = 0.4827 + \theta(\frac{1}{r^2})$
  - $IC_0(AND) = \lim_{r \to \infty} IC_0^r(AND)$
  - Infinite rounds necessary to attain IC
  - Infimum over protocol necessary



Quantum Information Complexity ?

- Can we define a sensible notion of quantum information complexity?
- Can we obtain similar applications for it?

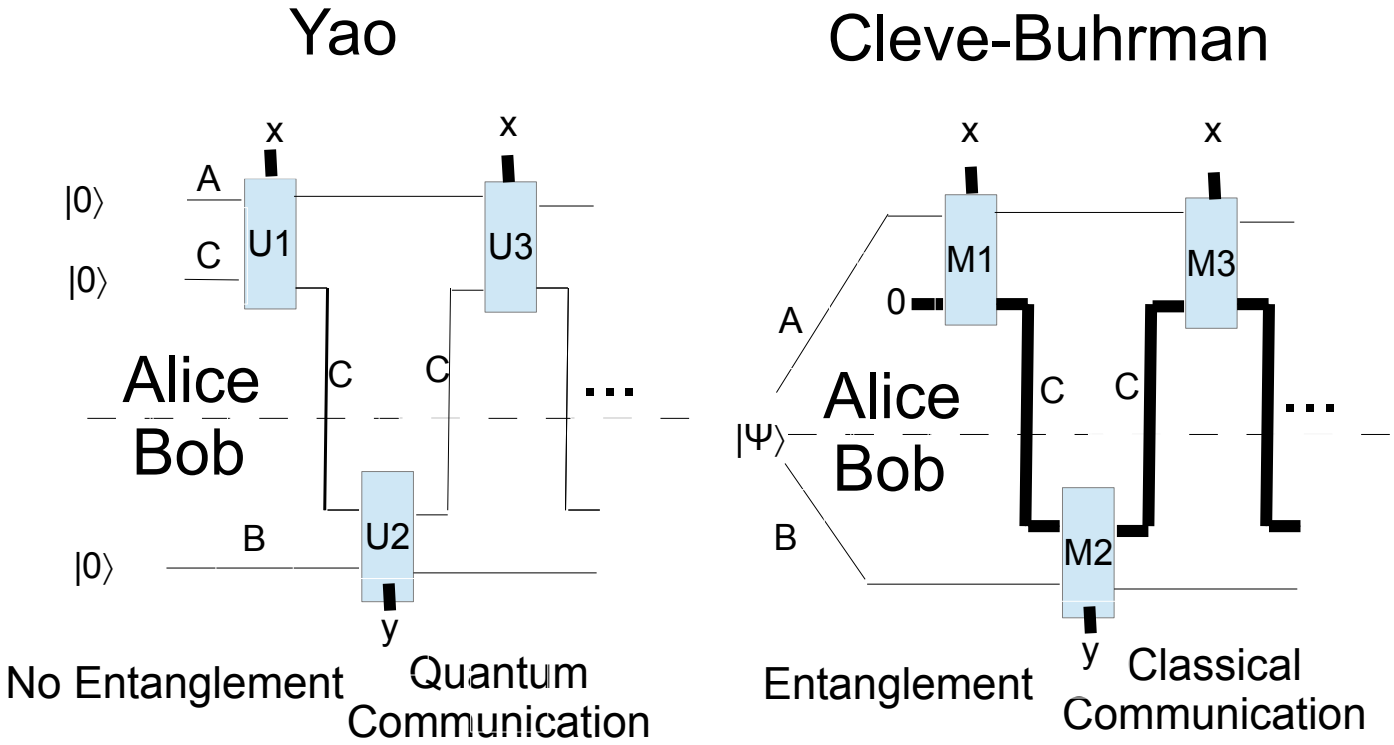
Quantum Information Theory



- von Neumann's quantum entropy: $H(A)_\rho = -Tr(\rho^A \log \rho^A) = H(\lambda_i)$ for $\rho_A = \sum_i \lambda_i |i\rangle\langle i|$
- Characterizes optimal rate for quantum source compression
- Derived quantities defined in formal analogy to classical quantities
- Conditional entropy can be negative!

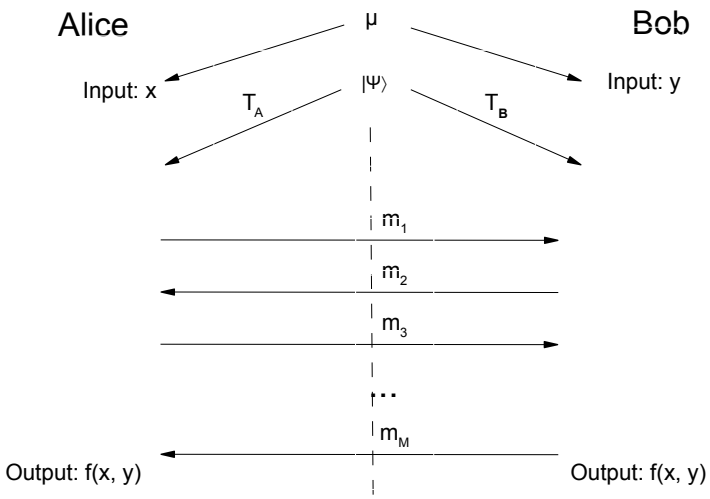
Quantum Communication Complexity

- 2 Models for computing classical $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$



- Hybrid: arbitrary pre-shared entanglement ψ, quantum messages m_i
- Exponential separations in communication complexity
  - Classical vs. quantum
  - N-rounds vs. N+1-rounds

Interactive Quantum Communication and QIC



- Recall classically: $IC(\Pi, \mu) = I(X : \Pi|Y) + I(Y : \Pi|X)$
  - $\Pi = m_1 m_2 \cdots m_M$
- Potential definition for quantum information cost: $QIC(\Pi, \mu) = I(X : m_1 m_2 \cdots m_M|Y) + I(Y : m_1 m_2 \cdots m_M|X)$? No!!

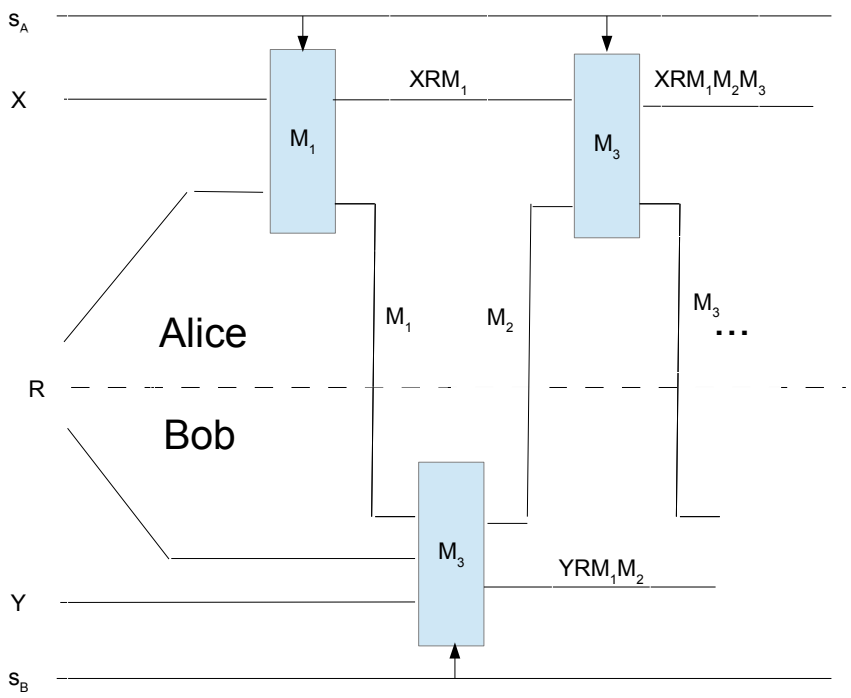
Problems

- Bad $QIC(\Pi, \mu) = I(X : m_1 m_2 \cdots m_M | Y) + I(Y : m_1 \cdots | X)$
- Many problems
- Yao model:
  - No-cloning theorem : cannot copy m_i, no transcript
  - Can only evaluate information quantities on registers defined at same moment in time
  - Not even well-defined!
- Cleve-Buhrman model:
  - m_i's could be completely uncorrelated to inputs
  - e.g. teleportation at each time step
  - Corresponding quantum information complexity is trivial

Potential Solutions

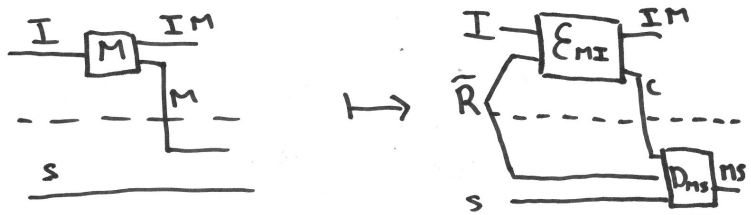
- 1) Keep as much information as possible, and measure final correlations, as in classical information cost
  - Problem : Reversible protocols, no garbage, only additional information is the function output
  - Corresponding quantum information complexity is trivial
- 2) Measure correlations at each step [JRS03, JN14]
  - $\sum_{iodd} I(X : m_i B_{i-1}|Y) + \sum_{ieven} I(Y : m_i A_{i-1}|X)$
  - Problem: for M messages and total communication C, could be $\Omega(M \cdot C)$
  - We want $QIC \leq QCC$, independent of M,
    - ⋆ i.e. direct lower bound on communication

Approach: Reinterpret Classical Information Cost



- Shannon task: simulate noiseless channel over noisy channel
- Reverse Shannon task: simulate noisy channel over noiseless channel

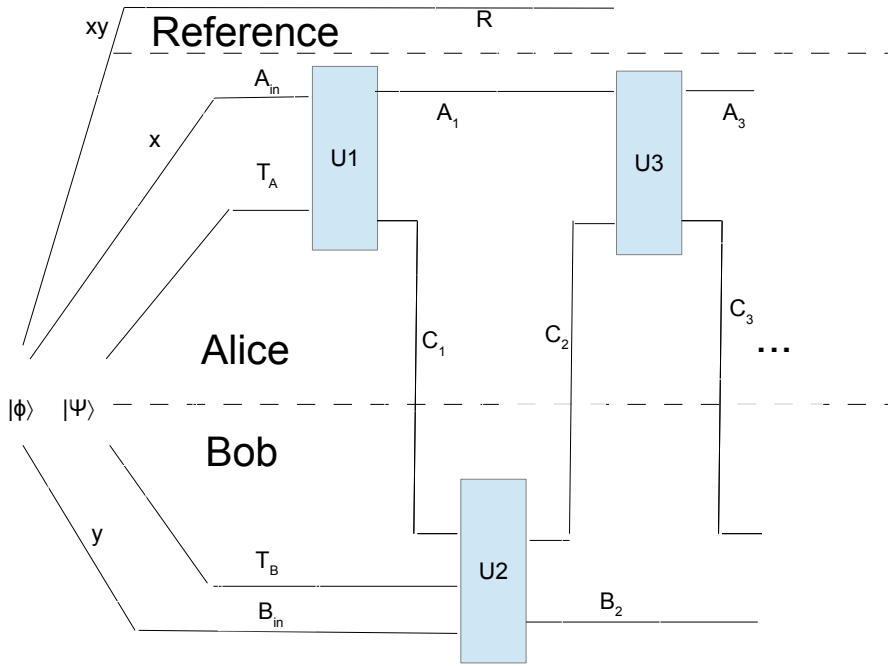
Channel simulations



- channel $M|I$ for input I, output/message M, side information S
- Known asymptotic cost : $\lim_{n\to\infty} \frac{1}{n} \log |C_n| = I(I : M|S)$
- Sum of asymptotic channel simulation costs: good operational measure of information
- Rewrite $IC(\Pi, \mu) = I(XR^A : M_1|YR^B) + I(YM_1R^B : M_2|XR^AM_1) + I(XM_1M_2R^A : M_3|YR^BM_1M_2)\cdots$
- Provides new proof of $IC = ACC$, and extends to $IC^r = ACC^r$

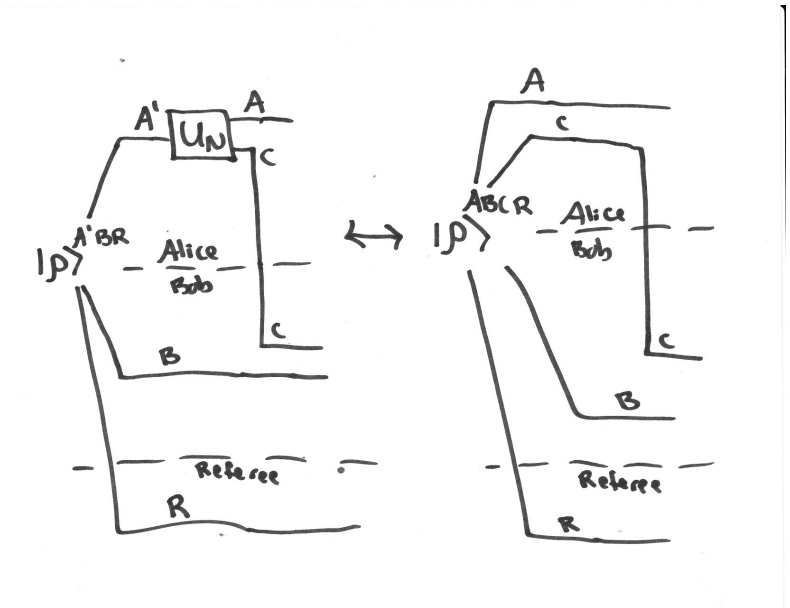
Intuition for Quantum Information Complexity

- Take channel simulation view for quantum protocol
- Purify everything
  - Can apply to fully quantum, bipartite inputs and tasks



- Quantum channel simulation with feedback and side information
- Equivalent to quantum state redistribution

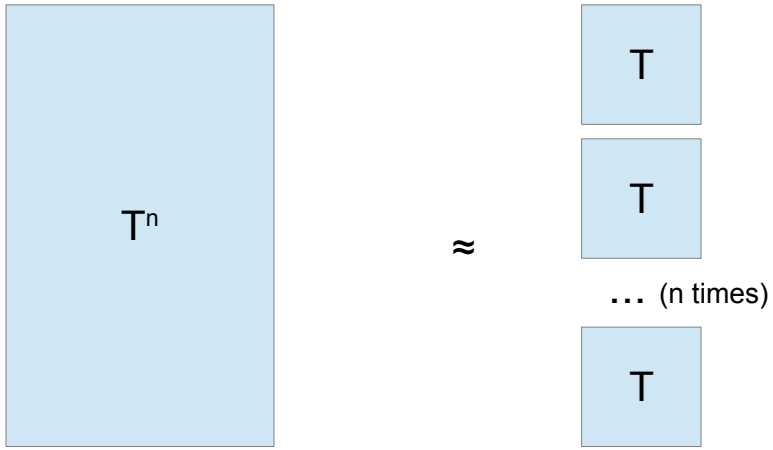
Definition of Quantum Information Complexity



- Asymptotic communication cost is $I(R : C|B)$ for R holding purification of input A / side information B, and output/message C
  - In QSR, strong converse holds with free feedback [BCT14]
- $QIC(\Pi, \mu) = I(R : C_1|B_0) + I(R : C_2|A_1) + I(R : C_3|B_1) + \cdots$
- $QIC(T) = AQCC(T) = \lim_{n\to\infty} \frac{1}{n} QCC(T^{\otimes n})$
- Satisfies all other desirable properties for an information complexity
- Single-shot protocol compression leads to first general multi-round direct sum result for quantum communication complexity

Direct Sum for Quantum Communication I

- Direct sum: $QCC((f,\epsilon)^{\otimes n}) \geq \Omega(n \cdot QCC(f,\epsilon))$
  - $QIC(f,\epsilon) = \lim_{n\to\infty} \frac{1}{n} QCC((f,\epsilon)^{\otimes n})$: direct sum related to compression down to QIC

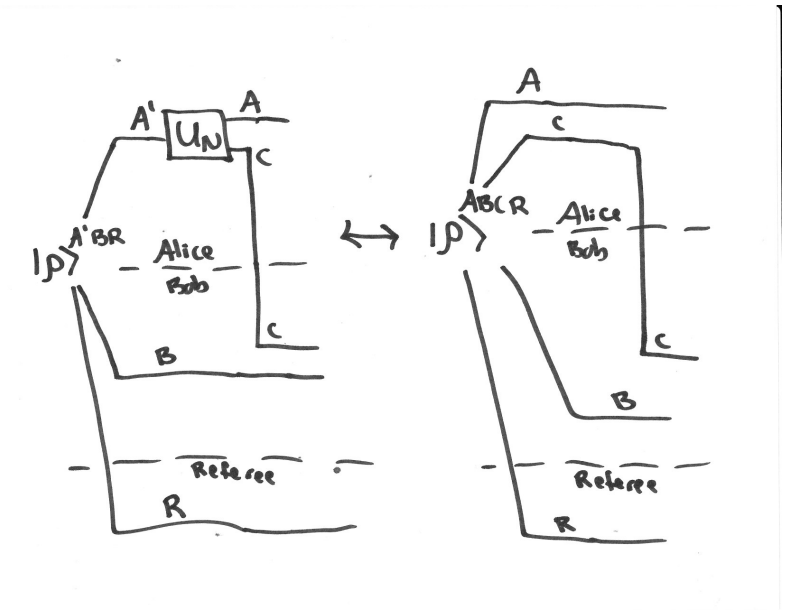


Direct Sum for Quantum Communication I

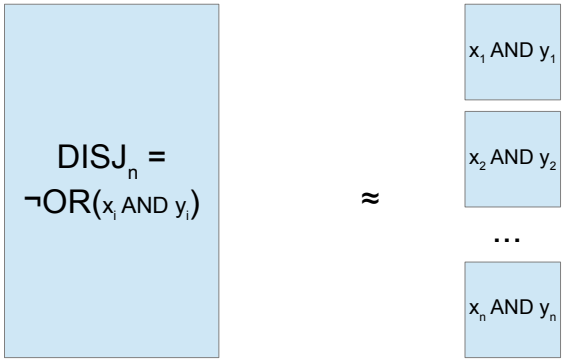
- Direct sum: $QCC((f,\epsilon)^{\otimes n}) \geq \Omega(n \cdot QCC(f,\epsilon))$
  - $QIC(f,\epsilon) = \lim_{n\to\infty} \frac{1}{n} QCC((f,\epsilon)^{\otimes n})$: direct sum related to compression down to QIC
- We know: $QCC^r(f,\mu,\epsilon) \leq O(r^2 \cdot QIC(f,\mu,\epsilon) + r)$
  - Compare with classical: $CC^{7r}(f,\mu,\epsilon) \leq O(IC^r(f,\mu,\epsilon) + r)$
  - Can we improve on quantum compression?

Direct Sum for Quantum Communication II

- Unbounded round?
- How to simultaneously compress many rounds with low information quantum messages?
- Open Q: QSR with no communication for $I(C : R|B) \leq \epsilon$



QCC lower bound?



- $Disj_n$: can we obtain exact QCC?
- $QIC_0(Disj_n) = nQIC_0(AND)$ holds
- But $QCC(Disj_n) = \theta(\sqrt{n})$!
  - Protocol achieving $O(\sqrt{n})$ is highly interactive
  - For a single message: $\Omega(n)$
- Bounded round $QCC^r(Disj_n)$: $O(\frac{n}{r})$ [AA03], $\Omega(\frac{n}{r^2})$ [JRS03]
- First step with QIC: conjecture $QCC^r(Disj_n) \geq \Omega(\frac{n}{r})$
  - Conjecture: $QIC_0^r(AND) \geq \Omega(\frac{1}{r})$

Bounded Round Disjointness

- Near-optimal bound $\tilde{\Theta}(\frac{n}{r})$ for n bits and r-round protocols
- Joint work with Mark Braverman, Ankit Garg, Young Kun Ko and Jieming Mao
- Indirect approach to prove $QIC_0^r(AND) \in \tilde{\Omega}(1/r)$
  - Reduce back to $Disj_n$!!
  - Continuity in input distribution: dependance on r not present for classical IC
- Possible direct approach: through CQMI lower bound
  - New lower bounds: [FR14] and generalization might be useful
  - Can we remove polylog factor?

Conclusion: Summary

- Definition of QIC
- Operational interpretation
- Properties
  - Difference in continuity in input
- Multi-round direct sum
- Bounded round disjointness

Research Directions

- Improved Direct sum
- No communication QSR sampling / simultaneous multi round compression
- Concrete quantum communication complexity lower bound
  - Tighter (exact?) disjointness
- etc.