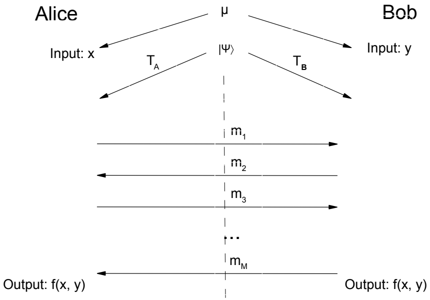
Quantum Information Complexity and Direct Sum

Dave Touchette
Université de Montréal

QIP 2015, Sydney, Australia

Interactive Quantum Communication

- Communication complexity setting:

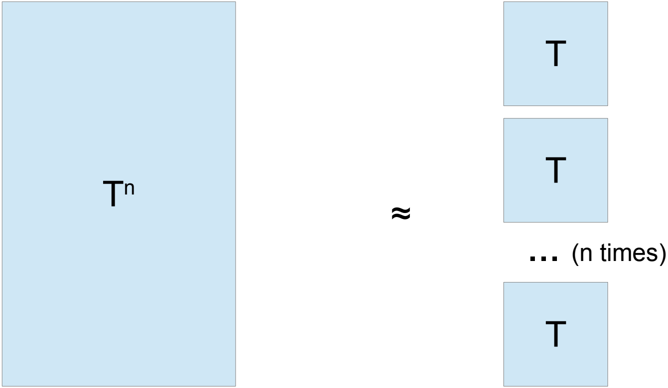


- Information-theoretic view: quantum information complexity
  - How much quantum **information** to compute f on μ

Results

- Definition of quantum information complexity of task $T = (f, \mu, \epsilon)$
- Interpretation as amortized communication
  - $QIC(T) = AQCC(T) := \lim_{n\to\infty} \frac{1}{n} QCC(T^{\otimes n})$
- Properties
  - Lower bounds communication: $QIC(T) \leq QCC(T)$
    - ★ No dependance on # of messages M
  - Additivity: $QIC(T_1 \otimes T_2) = QIC(T_1) + QIC(T_2)$
- Application to direct sum for quantum communication
  - Protocol compression builds on one-shot state redistribution of [BCT14]
  - M-rounds: $QCC^M((f, \epsilon)^{\otimes n}) \in \Omega(n(\frac{\delta}{M})^2 QCC^M(f, \epsilon + \delta) - M)$
- Potential application to communication lower bound
  - Direct sum on composite functions
  - E.g.: reduction from QIC of $DISJ_n$ to QIC of AND
  - Conjecture for $DISJ_n$: $QCC^M(DISJ_n) \in \Theta(\frac{n}{M} + M)$
  - Known bounds: $O(\frac{n}{M} + M), \Omega(\frac{n}{M^2} + M)$ [AA03, JRS03]

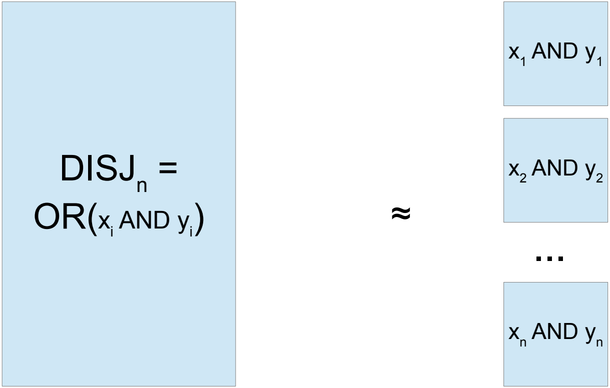
Direct Sum



Results

- Definition of quantum information complexity of task $T = (f, \mu, \epsilon)$
- Interpretation as amortized communication: $QIC(T) = AQCC(T)$
- Properties
  - Lower bounds communication: $QIC(T) \leq QCC(T)$
    - No dependance on # of messages M
  - Additivity: $QIC(T_1 \otimes T_2) = QIC(T_1) + QIC(T_2)$
- Application to direct sum for quantum communication
  - Protocol compression builds on one-shot state redistribution of [BCT14]
  - M-rounds: $QCC^M((f, \epsilon)^{\otimes n}) \in \Omega(n(\frac{\delta}{M})^2 QCC^M(f, \epsilon + \delta) - M)$
- Potential application to communication lower bound
  - Direct sum on composite functions
  - E.g.: reduction from QIC of $DISJ_n$ to QIC of AND
  - Conjecture for $DISJ_n$: $QCC^M(DISJ_n) \in \Theta(\frac{n}{M} + M)$
  - Known bounds: $O(\frac{n}{M} + M), \Omega(\frac{n}{M^2} + M)$ [AA03, JRS03]

Disjointness Decomposition



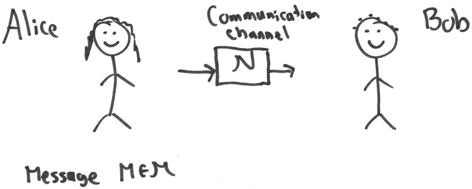
Results

- Definition of quantum information complexity of task $T = (f, \mu, \epsilon)$
- Interpretation as amortized communication: $QIC(T) = AQCC(T)$
- Properties
  - Lower bounds communication: $QIC(T) \leq QCC(T)$
    - No dependance on # of messages M
  - Additivity: $QIC(T_1 \otimes T_2) = QIC(T_1) + QIC(T_2)$
- Application to direct sum for quantum communication
  - Protocol compression builds on one-shot state redistribution of [BCT14]
  - M-rounds: $QCC^M((f, \epsilon)^{\otimes n}) \in \Omega(n(\frac{\delta}{M})^2 QCC^M(f, \epsilon + \delta) - M)$
- Potential application to communication lower bound
  - Direct sum on composite functions
  - E.g.: reduction from QIC of $DISJ_n$ to QIC of AND
  - Conjecture for $DISJ_n$: $QCC^M(DISJ_n) \in \Omega(\frac{n}{M} + M)$
  - Known bounds: $O(\frac{n}{M} + M), \Omega(\frac{n}{M^2} + M)$ [AA03, JRS03]

Results

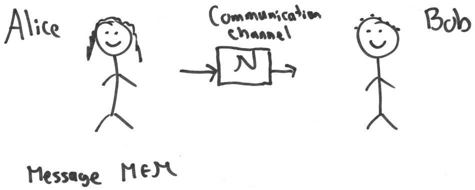
- **Definition** of quantum information complexity of task $T = (f, \mu, \epsilon)$
- Interpretation as amortized communication: $QIC(T) = AQCC(T)$
- Properties
  - Lower bounds communication: $QIC(T) \leq QCC(T)$
    - No dependance on # of messages M
  - Additivity: $QIC(T_1 \otimes T_2) = QIC(T_1) + QIC(T_2)$
- Application to direct sum for quantum communication
  - Protocol compression builds on one-shot state redistribution of [BCT14]
  - M-rounds: $QCC^M((f,\epsilon)^{\otimes n}) \in \Omega(n(\frac{\delta}{M})^2 QCC^M(f, \epsilon + \delta) - M)$
- Potential application to communication lower bound
  - Direct sum on composite functions
  - E.g.: reduction from QIC of $DISJ_n$ to QIC of AND
  - Conjecture for $DISJ_n$: $QCC^M(DISJ_n) \in \Theta(\frac{n}{M} + M)$
  - Known bounds: $O(\frac{n}{M} + M), \Omega(\frac{n}{M^2} + M)$ [AA03, JRS03]

Unidirectional Classical Communication



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

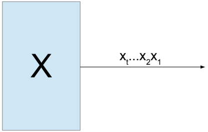
Unidirectional Classical Communication



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

Information Theory

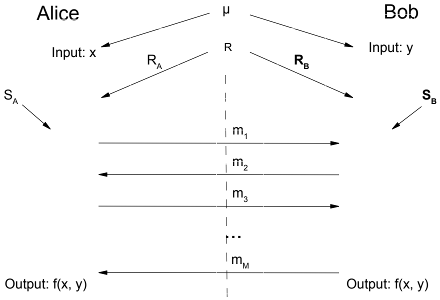
- How to quantify information?
- Shannon's entropy!
- Source X of distribution p_X has entropy $H(X) = -\sum_x p_X(x) \log(p_X(x))$ bits
- Operational significance: optimal asymptotic rate of compression for i.i.d. copies of source X



- Derived quantities: conditional entropy $H(X|Y)$, mutual information $I(X:Y)$...
- Mutual information characterizes a noisy channel's capacity
  - Also the optimal channel simulation rate

Interactive Classical Communication

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



- Protocol transcript $\Pi(x, y, r, s) = m_1 m_2 \cdots m_M$
- Can memorize whole history

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?
    - Optimal asymptotic compression rate?

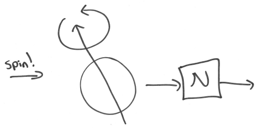
Protocol Compression: Information Complexity

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

Applications of Classical Information Complexity

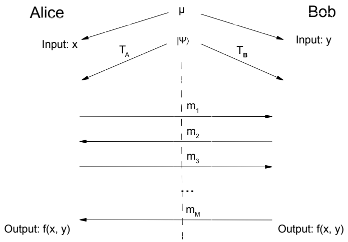
- Direct sum: $CC((f,\epsilon)^{\otimes n}) \approx nCC((f,\epsilon))$
- Direct product: $suc(f^n, \mu^n, o(Cn)) < suc(f, \mu, C)^{\Omega(n)}$
- Exact communication complexity bound!!
  - E.g. $CC(DISJ_n) = 0.4827 \cdot n \pm o(n)$
- Etc.

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!
- Mutual information characterizes a channel's entanglement-assisted capacity and optimal simulation rate

Interactive Quantum Communication and QIC



- Yao: no pre-shared entanglement ψ, quantum messages m_i
- Cleve-Buhrman: arbitrary pre-shared entanglement ψ, classical messages m_i
- Hybrid: arbitrary pre-shared entanglement ψ, quantum messages m_i
- 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!!

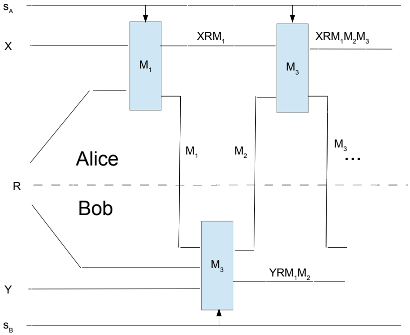
Problems

- 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

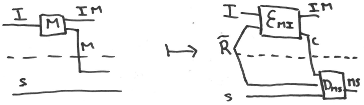
- 1) Keep as much information as possible, and measure final correlations, as in classical information cost
  - Problem : Reversible protocols: no garbage, only additional information is the output
  - Corresponding quantum information complexity is trivial
- 2) Measure correlations at each step [JRS03, 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 $QIC \in O(QCC)$, 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

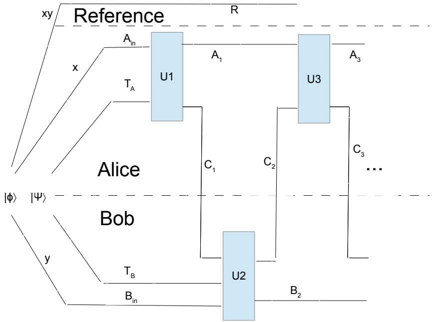
Channel simulations



- channel $M|I$ for input I, output/message M, side information S
- Known asymptotic cost : $\limsup_{n\to\infty} \frac{1}{n} \log |C_n| = I(I : M|S)$
- 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 it to bounded rounds

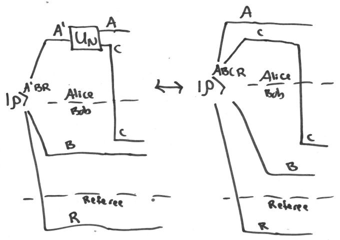
Intuition for Quantum Information Complexity

- Take channel simulation view for quantum protocol
- Purify everything



- 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
- $QIC(\Pi, \mu) = I(R : C_1|B_0) + I(R : C_2|A_1) + I(R : C_3|B_1) + \cdots$
- $QIC(T) = AQCC(T) = \limsup_{n\to\infty} \frac{1}{n} QCC_n(T^{\otimes n})$
- Satisfies all other desirable properties for an information complexity
- First general multi-round direct sum result for quantum communication complexity

Conclusion: Results

- Definition of QIC with desirable properties of classical IC
- Operational interpretation: QIC (T) = AQCC (T)
- Application to direct sum theorem for bounded round quantum communication complexity

Research Directions: Quantum Information Complexity

- Communication complexity lower bound
  - Bounded-round disjointness function and others [Building on JRS03]
- Prior-free quantum information complexity
- General upper bound on quantum communication complexity
- General lower bound on quantum information complexity
- Exponential separations between QIC and QCC
- Improved Direct sum
- Direct products, even for single round