Interactive Quantum Information Theory

Dave Touchette
Institute for Quantum Computing and C&O,
University of Waterloo,
Perimeter Institute for Theoretical Physics
(Starting 09/19: CS Dept., Université de Sherbrooke)

Spring 2018 INTRIQ meeting
16 Mai 2018
Shannon’s Information Theory

A Mathematical Theory of Communication [Shannon ’48]

- Compress messages with “low information content”
- Transmit messages over noisy channels
Compression

Enc

Dec
Transmission over Noisy Channels

- Want good communication rates
Quantum Information Theory

- Compression: compress quantum messages, qubit
- Transmission of messages over noisy quantum channels: classical and quantum messages, ...
Interactive Communication

- Direct link to distributed computing, but also connexion to data structures, streaming algorithms, approximation algorithms, circuits, etc.

- What about a theory of information for interactive communication? for interactive quantum communication?
Outline

1. Interactive Communication Protocols
2. Information Cost and Compression for Interactive Quantum Communication
3. Noisy Interactive Quantum Communication
4. Specific Problem: Practical Quantum Appointment Scheduling
Outline

1. Interactive Communication Protocols
2. Information Cost and Compression for Interactive Quantum Communication
3. Noisy Interactive Quantum Communication
4. Specific Problem: Practical Quantum Appointment Scheduling
Interactive Classical Communication

- Communication complexity of bipartite functions

Definition of Protocol $\Pi$:

- $f_1, f_2, f_3, \ldots, f_M, R_A, R_B$

Length of $C_i = \#$ bits of $C_i = |C_i|$

Cost of $\Pi = CC(\Pi) = \sum_i |C_i|$

Cost of $f = CC(f) = \min_{\Pi} CC(\Pi)$
Different models of CC

- Private, Shared Randomness: $n \rightarrow O(\log n) \rightarrow O(1)$
  - e.g.: $EQ_n(x, y) = [x = y]$, $x, y \in \{0, 1\}^n$
- Interaction: $\Omega(n) \rightarrow O(\log n)$
  - e.g.: $GT_n(x, y) = [x \geq y]$
- Quantum: $\Omega(n^{1/3}) \rightarrow O(\log n)$
- Information vs. communication: $\Omega(\log n) \rightarrow O(\log \log n)$
Different models of CC

- Private, Shared Randomness: \( n \to O(\log n) \to O(1) \)
  - e.g.: \( EQ_n(x, y) = [x = ? y], x, y \in \{0, 1\}^n \)
- Interaction: \( \Omega(n) \to O(\log n) \)
  - e.g.: \( GT_n(x, y) = [x \geq y] \)
- Quantum: \( \Omega(n^{1/3}) \to O(\log n) \)
- Information vs. communication: \( \Omega(\log n) \to O(\log \log n) \)
Information vs. Communication

- $\log_2(24) \approx 4.584$ bits

Alice's input: Anita

Bob's input: Herman
Outline

1. Interactive Communication Protocols
2. Information Cost and Compression for Interactive Quantum Communication
3. Noisy Interactive Quantum Communication
4. Specific Problem: Practical Quantum Appointment Scheduling
Information Theory

- How to quantify classical information?
- Shannon information $I$!
- Conditional Mutual Information:
  \[ I(X : M|Y) = I(X : YM) - I(X : Y) \]
What is the amount of information conveyed by a protocol?

- Total amount of *information leaked* at end of protocol?
  - Cryptographic motivation

- Sum of information content of each transmitted message?
- Optimal asymptotic compression rate?

Long sequence of work in classical setting [CSWY01, BJKS02, JRS0*, BBCR10, MMN10, BR11, Bra12, KLLRX13, BGPW14, BRYW14, ...]

- Classically, these three notions all agree
Classical Information Complexity

- Information cost of $\Pi$ on $XY \sim \mu = IC(\Pi, \mu)$
  - Info Alice learns about Bob’s input
  - + "Bob" "Alice’s"
  - $= I(Y : C_1C_2\cdots C_M|XR_A)$
  - $+ I(X : C_1C_2\cdots C_M|YR_B)$
- Information cost of $f = IC(f) = \inf_{\Pi} \max_{\mu} IC(\Pi, \mu)$

touchette.dave@gmail.com
Properties of Classical Information Complexity

- $T = (f, \mu, \epsilon)$: Task of computing $f$ with average error $\epsilon$ w.r.t. $\mu$
- $T_1 \otimes T_2$: Product task
- **Additivity**: $IC(T_1 \otimes T_2) = IC(T_1) + IC(T_2)$
- Lower bounds communication: $IC(T) \leq CC(T)$
- Operational interpretation: $IC(T) = ACC(T) = \lim_{n \to \infty} \frac{1}{n} CC(T \otimes^n)$
  [Braverman, Rao 2011]
- Continuity, convexity in error $\epsilon$, concavity in $\mu$, etc.
Quantum Information Complexity (QIC)

- Still computes classical function: \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \)
- Quantum protocol: QIC
- In terms of von Neumann information
- Account only for new information per message
- Satisfies all Properties listed for classical IC [T14]
Developing Framework

- Obtain Lower Bounds
  - on Communication
  - e.g. Disjointness [BGKMT15, CKL17]
  - on Concrete Models of Computation
  - e.g. Augmented Index and Streaming Algorithm for DYCK(2) [NT17]

- Study Structural Question
  - Is "batch" computation more efficient: Direct Sum
  - Counterexample to strong conjecture [ATYY17]
  - Partial Compression Results [DT15]
  - Further Compression: $2^{QIC}$ one-way, Interactive Compression?
  - Smaller input-size vs. communication trade-off?

- Study Fundamental Questions
  - Accounts for Back-Flow of Information [LT17]
  - Variable Length Compression [AGHY16]
  - Limit of Compression [AJK15]
  - Privacy [KLLR15]

- ...
Outline

1. Interactive Communication Protocols
2. Information Cost and Compression for Interactive Quantum Communication
3. **Noisy Interactive Quantum Communication**
4. Specific Problem: Practical Quantum Appointment Scheduling
Noisy Interactive Communication

- Simulate interactive protocols designed to be run over noiseless channel over noisy channels at high communication rate

\[
R_A, R_B \\
X, Y
\]
\[
C_1 = f_1(X, R_A) \\
C_2 = f_2(Y, R_B, C_1) \\
\vdots \\
C_M = f_M(Y, R_B, C_{<M})
\]

Output: \( f(x, y) \)
Noisy Interactive Communication

- Simulate interactive protocols designed to be run over noiseless channel over noisy channels at high communication rate

Output: $f(x, y)$
Difficulties for Interactive Coding

- Major obstacles for such highly interactive protocols over noisy channels?
- Standard Error Correcting Codes are inapplicable, in both classical and quantum setting

- Standard ECC with interaction: Single corrupted block derails protocol
- Need coding strategy acting collectively on multiple messages
- Classical solutions for different models: [Sch92, Sch93, BR11, BK12, FGOS12, BN13, BKN14, GMS11, GMS14, GH14, BE17, GHS14, EGH15, HV17, ABY17, ...]
Quantum Solutions

- New, uniquely quantum difficulty: No-Cloning Theorem
  - Joint quantum state evolves with protocol, but no copies can be made
  - Any logical quantum data leaked to environment cannot be recovered
- Get positive communication rate for noisy channel with one-way quantum capacity, can tolerate maximal adversarial error rate up to 1/2 [BNTTU14]
- More recently, $Q_{int} \geq 1 - O(\sqrt{\varepsilon})$ for low adversarial noise $\varepsilon$ [LNSTYY18]
  - Better than bound for plain classical model!
  - Is this optimal? Many other interesting research directions ...
- Assumes ideal local quantum computers... What about shorter term goals? Can we still get provable quantum advantage for practical quantum protocols?
Outline

1. Interactive Communication Protocols
2. Information Cost and Compression for Interactive Quantum Communication
3. Noisy Interactive Quantum Communication
4. Specific Problem: Practical Quantum Appointment Scheduling
Practical quantum communication protocol for appointment scheduling
- Joint work with Lovitz and Lütkenhaus, PRA’18
- Quantum advantage in terms of IC
- Robust to noise
Appointment Scheduling

- View $x, y \subseteq \{1, 2, \ldots, n\}$, calendar on $n$ dates
- Appointment Scheduling: output $i \in x \cap y$, or $\emptyset$ if $x \cap y = \emptyset$
- Rewrite in terms of $x, y \in \{0, 1\}^n$: Find $i$ s.t. $x_i = y_i = 1$, i.e. $\text{AND}(x_i, y_i) = 1$
- Classical: $IC \in \Omega(n)$
- Quantum advantage: $QIC \in \tilde{O}(\sqrt{n})$ [BCW98, HW02, AA03, Razb03]
- Need interaction: for $r$ messages/rounds, can achieve $\tilde{\Theta}(n/r)$ [JRS03, BGKMT15]
- Can we do with "simple" Quantum Subroutine?
- Yes! Uses 2-mode coherent states interactively, beamsplitter, + classical processing, inspired by [AL14, BGKMT15, JRS03]
Restricted Model of Interactive Quantum Communication

- Classical pre-, mid- and post- processing with limited information leakage
  - Must Carefully Handle Private ”Randomness” [CKL17]
  - Account for ”Quantum Honest-but-Curious” parties [CvDNT98]
- ”Simple” Quantum Subroutines
- Quantum Advantage for IC?

Output: f(x,y)
Quantum Fingerprinting with Coherent States

- Recently:
  - Protocol [AL14] and Implementation [XAWWPFSLL15] of Quantum Fingerprinting [BCWdW01]
  - Using Coherent States $|\alpha\rangle = \exp(-\frac{|\alpha|^2}{2}) \sum_{k=1}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle$
  - Interact through Beamsplitter
  - On $|\pm\alpha\rangle$, Detectors D0 clicks with probability $1 - \exp(-|\alpha|^2)$
    - On $\alpha = 0$, Clicks with Probability 0 (in Ideal Setting)
  - Different Model of Communication: no Direct Interaction, Simultaneous Message to Referee

```
Alice

X

Bob

Y

Referee: X = Y ?
```

touchette.dave@gmail.com
Interactive Quantum Information Theory
Quantum Subroutine $\widetilde{\Pi}_A$ for AND

- Back to Direct Interaction, Appointment Scheduling
- First, Focus on Solving AND
- Protocol $\widetilde{\Pi}_A$ on inputs $a, b \in \{0, 1\}$:

  - Loop $r$ times
  - Exchange output "0", "1", or "Inconclusive"

```
Loop $r$ times
Exchange output "0", "1", or "Inconclusive"
```

```
$\widetilde{\Pi}_A$ on inputs $a, b \in \{0, 1\}$:

- $a = 0$: $Id$
- $a = 1$: BS$_r$
- $b = 0$: Inject
- $b = 1$: $Id$

Splitting ratio: $\approx \frac{1}{r}$
```

Output: $|\alpha\rangle|0\rangle$ or $|0\rangle|\alpha\rangle$
Recursive call of $\tilde{\Pi}_A$ for $\text{AND}$

- If $\mu_\epsilon(1, 1) = \epsilon$, $QIC(\tilde{\Pi}_A, \mu_\epsilon) \approx h(\frac{1}{r}) + r h(\epsilon)$
- With Probability $\exp(-|\alpha|^2)$, $\tilde{\Pi}_A$ returns ”Inconclusive”
- **Protocol** $\Pi_A$ on inputs $a, b \in \{0, 1\}$:
  1. Run Protocol $\tilde{\Pi}_A$.
  2. If $\tilde{\Pi}_A$ returns “0”, return output “0”.
  3. If $\tilde{\Pi}_A$ returns “1”, Alice and Bob exchange $a$ and $b$ and return $\text{AND}(a, b)$ as output.
  4. If $\tilde{\Pi}_A$ returns “Inconclusive,” restart $\Pi_A$.
- If $\mu_\epsilon(1, 1) = \epsilon$, $QIC(\Pi_A, \mu_\epsilon) \approx \frac{1}{1-\exp(-|\alpha|^2)}[h(\frac{1}{r}) + r h(\epsilon)]$
Solving Appointment Scheduling

- **Protocol** $\Pi_D$ on inputs $x, y \in \{0, 1\}^n$:
  1. Using shared randomness, publicly sample $s$ dates with replacement. Denote this date set by $S$.
  2. Alice sends $x_i$ to Bob for each $i \in S$.
  3. If Bob find any $i \in S$ with $x_i = y_i = 1$, he sends the smallest such $i$ to Alice, and both output this $i$. Else, they continue.
  4. Run date-wise the $\Pi_A$ protocol for all dates outside of $S$.
  5. If they find any $i$ such that $\text{AND}(x_i, y_i) = 1$, both output the smallest such $i$.
  6. If they do not find any such $i$, output “∅”.

- In Ideal Setting, Zero-Error Protocol
- Can Obtain Quantum Advantage:
  Quantum $QIC \in \tilde{O}(n^{2/3})$ vs. Classical $IC \in \Omega(n)$
Quantum Advantage for Appointment Scheduling: Ideal

- Theoretical Bounds, Idealized Setting, in More Details:
- Classical Lower Bound: $IC \geq 0.48n$ [BGPW13]
- Quantum Upper Bound:
  
  
  $$QIC(\Pi_D) \leq s + \log s + 1 + \frac{n}{1-\exp(-|\alpha|^2)} \max \left\{ \frac{2(2r+3)}{n}, h\left(\frac{1}{2}(1 - F(r, \alpha))\right) + 2(2r + 3)h\left(\frac{2\ln n}{s} + \frac{1}{n}\right) \right\}$$

  - in which $F(r, \alpha) = \exp\left[-r|\alpha|^2 \left[1 - \cos\left(\frac{\pi}{2r}\right)\right]\right]$

- Obtain $QIC \in \tilde{O}\left(\frac{n}{r}\right)$ with $r \leq n^{1/3}$, $s \approx \frac{n}{r}$, $\alpha$ Constant
$\text{QIC} \in \tilde{O}(n^{2/3})$ vs. $I_C \in \Omega(n)$ Trade-Off

Theoretical Bounds, Idealized Setting, $\tilde{O}(n^{2/3})$ vs. $\Omega(n)$ Trade-Off
Quantum Subroutine $\tilde{\Pi}_A'$ for AND with Errors

- Want to Account for Experimental Errors
- Dark Counts: Even for zero amplitude, Detectors D0 still Clicks with Probability $p_{dark} > 0$
- Transmission and Coupling Loss $\eta < 1$ per Message:
  $|\gamma\rangle|\delta\rangle \rightarrow |\sqrt{\eta}\gamma\rangle|\sqrt{\eta}\delta\rangle \rightarrow 2r \ times \ |\eta^r\gamma\rangle|\eta^r\delta\rangle$
- Detector efficiency: further loss $\eta_{det}$ in detector,
  $|\gamma_f\rangle|\delta_f\rangle \rightarrow |\sqrt{\eta_{det}}\gamma_f\rangle|\sqrt{\eta_{det}}\delta_f\rangle$

```
touchette.dave@gmail.com
```

Interactive Quantum Information Theory
Quantum Bound in Non-Ideal Setting

- Theoretical Bounds, Non-Ideal setting, accounting for dark counts and losses
- Quantum Upper Bound:
  \[ QIC(\Pi_D) \leq s + \log s + 1 + \frac{2n}{1-p} p_{dark} \]
  \[ + \frac{n}{1-p} \max \left[ \frac{2(2r+3)}{n}, \right. \]
  \[ h\left(\frac{1}{2}(1 - F(r, \alpha_{out}, \eta))\right) \]
  \[ +2(2r + 3)h\left(\frac{2\ln n}{s} + \frac{1}{n}\right) \]

  - in which
    \[ F(r, \alpha_{out}, \eta) = \exp \left[ -\frac{(1-\eta^2)}{(1-\eta^2)} \left( \frac{1}{\eta} \right)^{2r} |\alpha_{out}|^2 \left[ 1 - \cos \left( \frac{\pi}{2r} \right) \right] \right] \]
    and \( p \) is probability of "Inconclusive":
    \[ p = \exp(-\eta_{det}|\alpha_{out}|^2) (1 - p_{dark})^2 \]
    \[ + (1 - \exp(-\eta_{det}|\alpha_{out}|^2) + \exp(-\eta_{det}|\alpha_{out}|^2) p_{dark}) p_{dark} \]

  - Trade-off for \( r \) between \( \left( \frac{1}{\eta} \right)^{2r} \) vs. \( \approx \frac{1}{r^2} \)
"one-sided" error $\leq p_{dark}$, might only err on output $\emptyset$
Quantum Advantage as $\eta \to 1$

- Protocol Designed s.t. Loss Factor $\eta$ is Most Limiting
- Small Transmission Distance fine here, Coupling is Probably most Challenging
- With $\eta \approx 1 - \frac{1}{r}$, can still get $QIC \in \tilde{O}(\frac{n}{r})$ for $r \leq n^{1/3}$ by slightly adapting protocol

![Graph showing QIC/n vs. $\eta$](image-url)
Outlook

▶ Summary:
  ▶ QIC: New framework to study interactive quantum communication
  ▶ Noisy interactive quantum protocols: can maintain quantum communication advantage over noisy channels
  ▶ Development of Practical Protocols with Quantum Advantage for Appointment Scheduling
  ▶ Robust to Experimental Errors

▶ Research Directions:
  ▶ Further Applications of Quantum Information Complexity
  ▶ Further Developments of Noisy Interactive Quantum Communication
  ▶ Further Developments of Practical Protocols
  ▶ Experimental Implementations of Quantum Advantage!

▶ Thank you!

touchette.dave@gmail.com