Imperfectly Shared Randomness in Communication

Madhu Sudan
Harvard

Joint work with Clément Canonne (Columbia), Venkatesan Guruswami (CMU) and Raghu Meka (UCLA).
Classical theory of communication

Shannon (1948)

- Clean architecture for reliable communication.
- But does Bob really need all of $x$?
The model (with shared randomness)

\[ f : (x, y) \mapsto \Sigma \]

\[ R = $$$ \]

\[ CC(f) = \# \text{bits exchanged by best protocol} \]

\[ f(x, y) \text{ w.p. } 2/3 \]
Communication Complexity - Motivation

- **Standard: Lower bounds**
  - Circuit complexity, Streaming, Data Structures, extended formulations ...

- **This talk:**
  - Communication complexity as model for communication
  - Food for thought: Shannon vs. Yao? Which is the right model.
  - Typical (human-human/computer-computer) communication involves large context and brief communication.
  - Contexts imperfectly shared.
This talk

- Example problems with low communication complexity.

- New form of uncertainty and overcoming it.
Aside: Easy CC Problems

- **Equality testing:**
  \[ EQ(x, y) = 1 \iff x = y; \quad CC(EQ) = O(1) \]

- **Hamming distance:**
  \[ H_k(x, y) = 1 \iff \Delta(x, y) \leq k; \quad CC(H_k) = O(k \log k) \quad [\text{Huang et al.}] \]

- **Small set intersection:**
  \[ \cap_k (x, y) = 1 \iff \text{wt}(x), \text{wt}(y) \leq k \\& \exists i \in S . t . x_i = y_i \; 1. \]
  \[ CC(\cap_k) = O(k) \quad [\text{Håstad Wigderson}] \]

- **Gap (Real) Inner Product:**
  \[ x, y \in \mathbb{R}^n; |x|_2, |y|_2 = 1; \]
  \[ GIP_\epsilon(x, y) = 1 \text{ if } \langle x, y \rangle \geq \epsilon; \quad CC(GIP_\epsilon) \]

**Summary from**

[Ghazi, Kamath, S.’16]
Uncertainty in Communication

- Overarching question: Are there communication mechanisms that can overcome uncertainty?

- What is uncertainty?

- This talk: Alice, Bob don’t share randomness perfectly; only approximately.
Rest of this talk

- **Model:** Imperfectly Shared Randomness

- **Positive results:** Coping with imperfectly shared randomness.

- **Negative results:** Analyzing weakness of imperfectly shared randomness.
Model: **Imperfectly Shared Randomness**

- Alice ← $r$; and Bob ← $s$ where 

  $(r, s) = \text{i.i.d. sequence of correlated pairs } (r_i, s_i)_i$;
  
  $r_i, s_i \in \{-1, +1\}; \mathbb{E}[r_i] = \mathbb{E}[s_i] = 0; \mathbb{E}[r_is_i] = \rho \geq 0$.

- Notation:
  - $isr_\rho(f) = \text{cc of } f \text{ with } \rho\text{-correlated bits}$.
  - $cc(f): \text{Perfectly Shared Randomness cc.} = isr_1(f)$
  - $priv(f): \text{cc with PRIVate randomness} = isr_0(f)$

- Starting point: for Boolean functions $f$

  - $cc(f) \leq isr_\rho(f) \leq priv(f) \leq cc(f) + \log n$
  - What if $cc(f) \ll \log n$? E.g. $cc(f) = O(1)$
Distill Perfect Randomness from ISR?

- Agreement Distillation:
  - Alice $\leftarrow r$; Bob $\leftarrow s$; $(r, s)$ $\rho$-corr. unbiased bits
  - Outputs: Alice $\rightarrow u$; Bob $\rightarrow v$; $H_\infty(u), H_\infty(v) \geq k$
  - Communication = $c$ bits;
  - What is max. prob. $\tau$ of agreement ($u = v$)?

- Well-studied in the literature!
  - [Ahlswede-Csiszar ‘70s]:
    \[ \tau \rightarrow 1 \Rightarrow c = \Omega(k) \text{ (one-way)} \]
  - [Bogdanov-Mossel ‘2000s]: $c = 0 \Rightarrow \tau \leq \exp(-k)$
  - [Our work]: $\tau = \exp(-k + O(c))$ (two-way)

- Summary: Can’t distill randomness!
Results

- Model first studied by [Bavarian, Gavinsky, Ito’14] ("Independently and earlier").
  - Their focus: Simultaneous Communication; general models of correlation.
  - They show \( \text{isr}(\text{Equality}) = O(1) \) (among other things)

- Our Results:
  - Generally: \( cc(f) \leq k \Rightarrow \text{isr}(f) \leq 2^k \)
  - Converse: \( \exists f \text{ with } cc(f) \leq k \text{ and } \text{isr}(f) \geq 2^k \)
Equality Testing (our proof)

- Key idea: Think inner products.
  - Encode \( x \mapsto X = E(x); y \mapsto Y = E(y); X, Y \in \{-1, +1\}^N \)
    - \( x = y \Rightarrow \langle X, Y \rangle = N \)
    - \( x \neq y \Rightarrow \langle X, Y \rangle \leq N/2 \)

- Estimating inner products:
  - Building on sketching protocols ...
  - Alice: Picks Gaussians \( G_1, \ldots, G_t \in \mathbb{R}^N \),
  - Sends \( i \in [t] \) maximizing \( \langle G_i, X \rangle \) to Bob.
  - Bob: Accepts iff \( \langle G'_i, Y \rangle \geq 0 \)
  - Analysis: \( O_\rho(1) \) bits suffice if \( G \approx_\rho G' \)

Gaussian Protocol
General One-Way Communication

- **Idea:** All communication \( \leq \) Inner Products
- (For now: Assume one-way-cc(\( f \)) \( \leq k \))
  - For each random string \( R \)
    - Alice’s message = \( i_R \in [2^k] \)
    - Bob’s output = \( f_R(i_R) \) where \( f_R : [2^k] \rightarrow \{0,1\} \)
    - W.p. \( \geq \frac{2}{3} \) over \( R \), \( f_R(i_R) \) is the right answer.
General One-Way Communication

- **For each random string** $R$
  - Alice’s message = $i_R \in [2^k]$
  - Bob’s output = $f_R(i_R)$ where $f_R : [2^k] \rightarrow \{0,1\}$
  - W.p. $\geq \frac{2}{3}$, $f_R(i_R)$ is the right answer.

- **Vector representation:**
  - $i_R \mapsto x_R \in \{0,1\}^{2^k}$ (unit coordinate vector)
  - $f_R \mapsto y_R \in \{0,1\}^{2^k}$ (truth table of $f_R$).
  - $f_R(i_R) = \langle x_R, y_R \rangle$; Acc. Prob. $\propto \langle X, Y \rangle$; $X = (x_R)_R$; $Y = (y_R)_R$
  - Gaussian protocol estimates inner products of unit vectors to within $\pm \epsilon$ with $O_\rho \left( \frac{1}{\epsilon^2} \right)$ communication.
Two-way communication

- Still decided by inner products.

- Simple lemma:
  - $\exists K_A^k, K_B^k \subseteq \mathbb{R}^{2^k}$ convex, that describe private coin k-bit comm. strategies for Alice, Bob s.t. accept prob. of $\pi_A \in K_A^k, \pi_B \in K_B^k$ equals $\langle \pi_A, \pi_B \rangle$

- Putting things together:

  **Theorem:** $cc(f) \leq k \Rightarrow isr(f) \leq O_\rho(2^k)$
Main Technical Result: Matching lower bound

Theorem: There exists a (promise) problem $f$ s.t.

- $cc(f) \leq k$
- $isr_{\rho}(f) \geq \exp(k)$

The Problem:

- Gap Sparse Inner Product (G-Sparse-IP).
- Alice gets \textbf{sparse} $x \in \{0,1\}^n$; $\text{wt}(x) \approx 2^{-k} \cdot n$
- Bob gets $y \in \{0,1\}^n$
- Promise: $\langle x, y \rangle \geq (.9)2^{-k} \cdot n$ or $\langle x, y \rangle \leq (.6)2^{-k} \cdot n$
- Decide which.
Protocol for G-Sparse-IP

- Note: Gaussian protocol takes $O(2^k)$ bits.
  - Need to get exponentially better.
- Idea: $x_i \neq 0 \Rightarrow y_i$ correlated with answer.
- Use (perfectly) shared randomness to find random index $i$ s.t. $x_i \neq 0$.
- Shared randomness: $i_1, i_2, i_3, \ldots$ uniform over $[n]$.
- Alice → Bob: smallest index $j$ s.t. $x_{ij} \neq 0$.
- Bob: Accept if $y_{ij} = 1$
- Expect $j \approx 2^k$; $cc \leq k$.

G-Sparse-IP:

$x, y \in \{0, 1\}^n; \text{wt}(x) \approx 2^{-k} \cdot n$

Decide $\langle x, y \rangle \geq (.9) 2^{-k} \cdot n$
or $\langle x, y \rangle \leq (.6) 2^{-k} \cdot n$?
Lower Bound Idea

- **Catch**: \( \forall \text{Dist.}, \exists \text{Det. Protocol w. comm.} \leq k. \)
  - Need to fix strategy first, construct dist. later.

- **Main Idea**:
  - Protocol can look like G-Sparse-Inner-Product
    - But implies players can agree on common index to focus on ...
  - Agreement is hard
  - Protocol can ignore sparsity
    - Requires \( 2^k \) bits
  - Protocol can look like anything!
    - Invariance Principle [MOO, Mossel ... ]
Invariance Principle [MOO’08]

- **Informally:**
  - Analysis of prob. processes with bits often hard.
  - Analysis of related processes with Gaussian variables easy.
  - “Invariance Principle” – under sufficiently general conditions ... prob. of events “invariant” when switching from bits to Gaussian

**Theorem:** For every convex $K_1, K_2 \subseteq [-1,1]^\ell$

\[ \exists \text{ transformations } T_1, T_2 \text{ s.t.} \]

if $f: \{0,1\}^n \rightarrow K_1$ and $g: \{0,1\}^n \rightarrow K_2$

have no common influential variable, then

$F = T_1f: \mathbb{R}^n \rightarrow K_1$ and $G = T_2g: \mathbb{R}^n \rightarrow K_2$ satisfy

$\mathbb{E}_{x,y}[\langle f(x), g(y) \rangle] \approx \mathbb{E}_{X,Y}[\langle F(X), G(Y) \rangle]$
Summarizing

- $k$ bits of comm. with perfect sharing
  $\rightarrow 2^k$ bits with imperfect sharing.
- This is tight
- Invariance principle for communication
  - Agreement distillation
  - Low-influence strategies

G-Sparse-IP:
$x, y \in \{0, 1\}^n \land wt(x) \approx 2^{-k} \cdot n$
Decide $\langle x, y \rangle \geq (.9) \ 2^{-k} \cdot n$
or $\langle x, y \rangle \leq (.6) \ 2^{-k} \cdot n$?
Conclusions

- Imperfect agreement of context important.
  - Dealing with new layer of uncertainty.
  - Notion of scale (context LARGE)

- Many open directions+questions:
  - Imperfectly shared randomness:
    - One-sided error?
    - Does interaction ever help?
    - How much randomness?
    - More general forms of correlation?
Thank You!