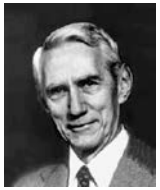
Imperfectly Shared Randomness in Communication

Madhu Sudan
Harvard

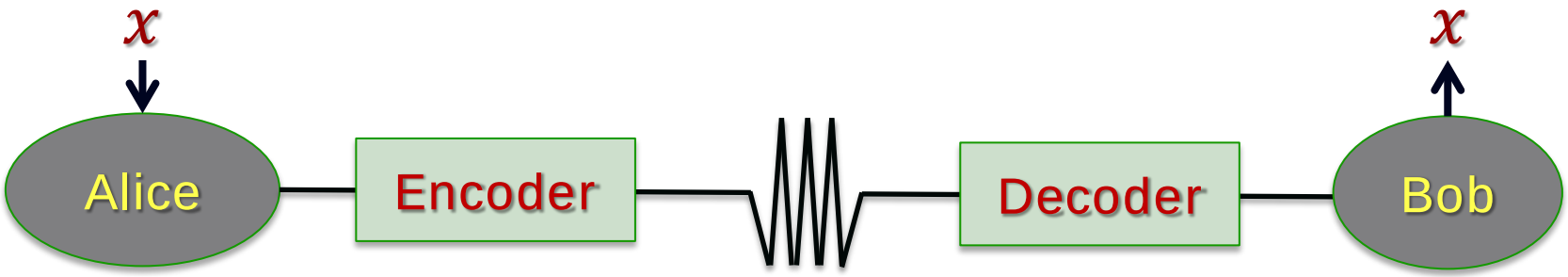
Joint work with Clément Canonne (Columbia), Venkatesan Guruswami (CMU) and Raghu Meka (UCLA).

Classical theory of communication



Shannon (1948)

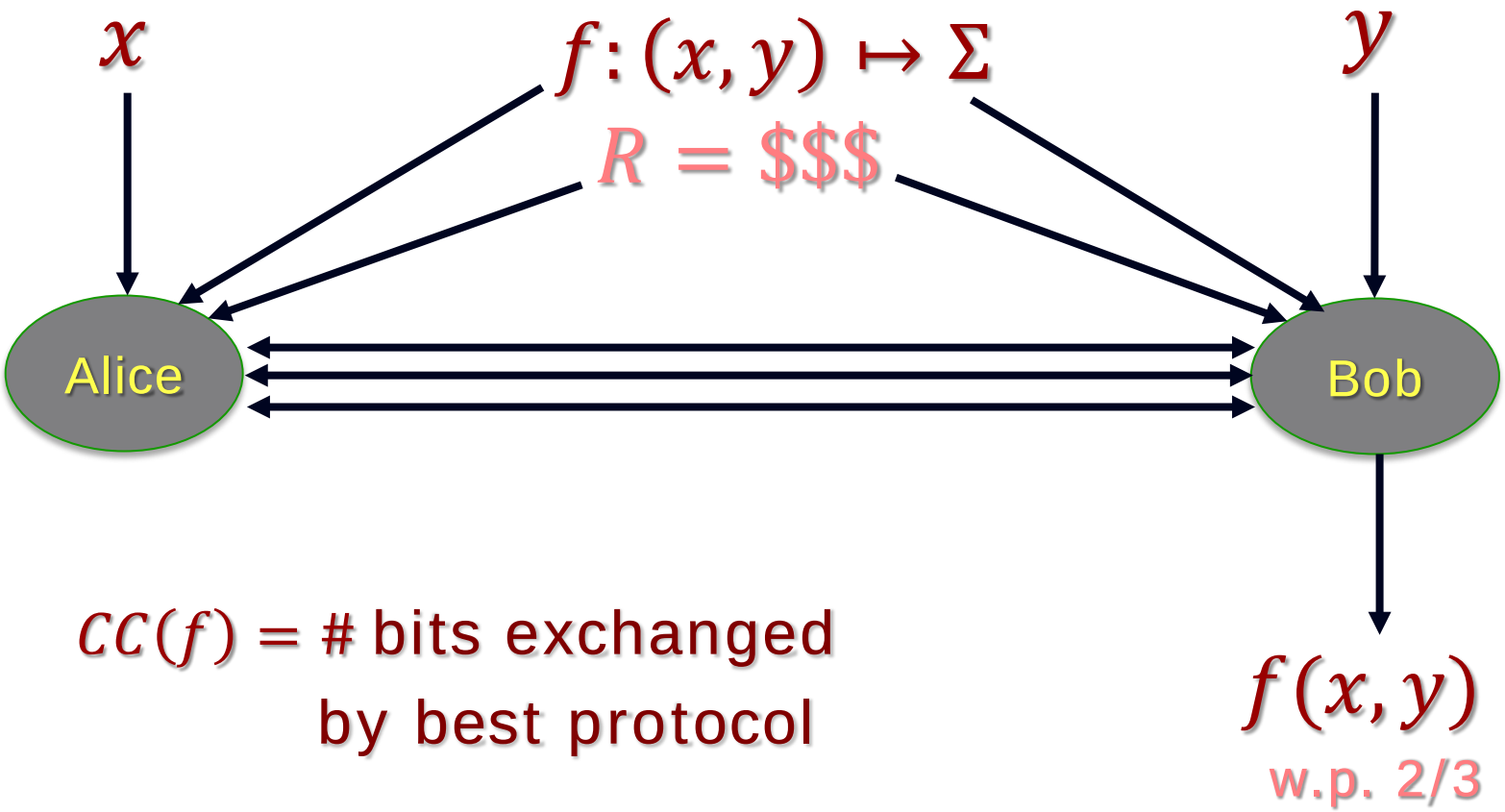
- Clean architecture for reliable communication.



- Remarkable mathematical discoveries: Prob. Method, Entropy, (Mutual) Information, Compression schemes, Error-correcting codes.
- But does Bob really need all of x?

[Yao'80] Communication Complexity

The model (with shared randomness)



$CC(f) = \#$ bits exchanged by best protocol

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:
  - $EQ(x, y) = 1 \Leftrightarrow x = y$; C
- Hamming distance:
  - $H_k(x, y) = 1 \Leftrightarrow \Delta(x, y) \leq k$;
- Small set intersection:
  - $\cap_k (x, y) = 1 \Leftrightarrow$ wt(x), wt$(y$
  - $CC(\cap_k) = O(k)$ [Håstad Wi
- Gap (Real) Inner Produ
  - $x, y \in \mathbb{R}^n; |x|_2, |y|_2 = 1$;
  - $GIP_{c,s}(x, y) = 1$ if $\langle x, y \rangle \geq \epsilon$;

Protocol:

Fix ECC $E: \{0,1\}^n \to \{0,1\}^N$

$poly(k)$ Proto

Use common

to hash $[n] \to$

$x = (x_1, \ldots, x_n)$
$y = (y_1, \ldots, y_n)$
$\langle x, y \rangle \triangleq \sum_i x_i y_i$

Main Insight:

If $G \leftarrow N(0,1)^n$, then

$\mathbb{E}[\langle G, x \rangle \cdot \langle G, y \rangle] = \langle x, y \rangle$

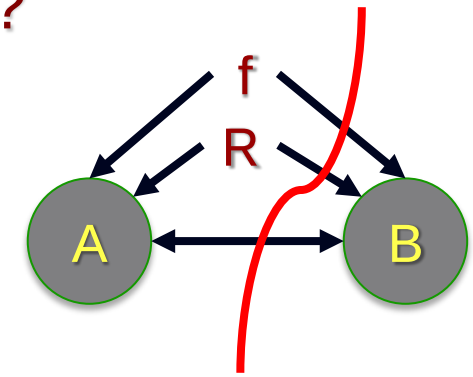
Summary from

[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 $\leftarrow r$; and Bob $\leftarrow s$ where
  (r, s) = i.i.d. sequence of correlated pairs $(r_i, s_i)_i$;
  $r_i, s_i \in \{-1, +1\}; \mathbb{E}[r_i] = \mathbb{E}[s_i] = 0; \mathbb{E}[r_i s_i] = \rho \geq 0$.
- Notation:
  - $isr_\rho(f)$ = cc of f with ρ-correlated bits.
  - $cc(f)$: Perfectly Shared Randomness cc. $= isr_1(f)$
  - $priv(f)$: 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. $cc(f) = O(1)$

$\rho \leq \tau \Rightarrow$
$isr_\rho(f) \geq isr_\tau(f)$

Distill Perfect Randomness from ISR?

- Agreement Distillation:
  - Alice $\leftarrow r$; Bob $\leftarrow s$; (r,s) ρ-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. τ 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 $isr(\text{Equality}) = O(1)$ (among other things)

- Our Results:
  - Generally: $cc(f) \leq k \Rightarrow isr(f) \leq 2^k$
  - Converse: $\exists f$ with $cc(f) \leq k$ & $isr(f) \geq 2^k$

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 $f_R: [2^k] \to \{0,1\}$
    - 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 $f_R: [2^k] \to \{0,1\}$
  - 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 <u>sparse</u> $x \in \{0,1\}^n$; $\mathrm{wt}(x) \approx 2^{-k} \cdot n$
  - 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.

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

psr 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. $x_{i_j} \neq 0$.
- Bob: Accept if $y_{i_j} = 1$
- Expect $j \approx 2^k$; $cc \leq k$.

G-Sparse-IP:
$x, y \in \{0,1\}^n; wt(x) \approx 2^{-k} \cdot n$
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: $\forall$ Dist., $\exists$ 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 ...]

x

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 $K_1, K_2 \subseteq [-1,1]^\ell$

$\exists$ transformations T_1, T_2 s.t.

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

have no common influential variable, then

$F = T_1 f: \mathbb{R}^n \to K_1$ and $G = T_2 g: \mathbb{R}^n \to K_2$ satisfy

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

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