MADHU SUDAN

IMPERFECTLY SHARED RANDOMNESS IN COMMUNICATION

20161116

- Classical theory of communication

→ Shannon 1948

- Clean architecture for reliable communication

→ prob. method

→ entropy

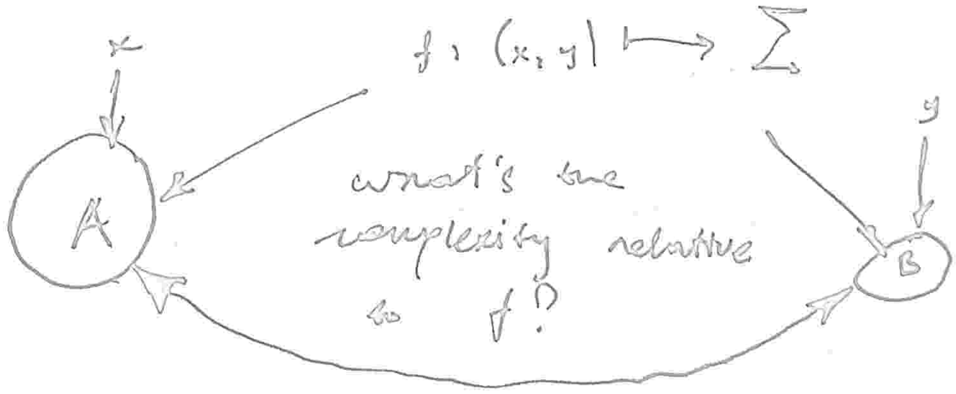
→ mutual information

→ compression schemes

→ error-correcting codes

But does Bob really need x?

- [Yao 80] Communication complexity with shared randomness



CC(f) = # bits exchanged by the best protocol

- How many bits are necessary to compute $f(x,y)$?

→ Lower bounds for boolean functions, circuit complexity, streaming, etc.

→ Communication complexity as a model for communication. Shannon vs Yao?

STUDENTS DO NOT COME BLANK.

EX HOW MUCH SHOULD BE SAID IN THE LECTURE FOR MAX. BENEFIT?

COMM. COMPLEXITY IS ALSO MOTIVATED BY HUMAN/HUMAN/COMPUTER/COMPUTER COMMUNICATION WITH LARGE CONTEXT AND BRIEF COMMUNICATION.

ALSO BY THE SITUATIONS ARE
- CONTEXTS ARE IMPERFECTLY SHARED.

GOALS:

EXAMPLE PROBLEMS WITH LOW COMMUNICATION COMPLEXITY.

EASY CC PROBLEMS:

- EQUALITY TESTING

$$EQ(x,y)=1 \iff x=y; \quad CC(EQ)=O(1)\ !$$

PROTOCOL:

FIX ERROR CORRECTING CODE.

$$E:\{0,1\}^n \longrightarrow \{0,1\}^N;$$

SHARED RANDOMNESS: $i \leftarrow [N]$;

EXCHANGE $E(x)_i$, $E(y)_i$

ACCEPT IFF $E(x)_i = E(y)_i$.

WHAT ARE OTHER CONSTANT-TIME EXAMPLES?

- HAMMING DISTANCE

$H_k(x,y)=1 \iff \Delta(x,y)\le k$;

$CC(H_k)=O(k\log k)$ [Huang et al]

- SMALL SETS INTERSECTION:

· $\cap_k(x,y)=1 \iff wt(x), wt(y)\le k$

& $\exists\, i: x_i = y_i = 1$.

· $CC(\cap_k)=O(k)$ [Håstad Wigderson]

poly(k) PROTOCOL:

USE COMMON RANDOMNESS

TO HASH $[n]\to[k^2]$.

G GAP (REAL) INNER PRODUCT

$x,y\in R^n$; $|x|_2; |y|_2=1$.

$GIP(x,y)=1$ IF $(x,y)\ge\varepsilon$; $=0$ IF $(x,y)\le 0$.

- $CC(GIP)=O\left(\frac{1}{\varepsilon^2}\right)$; [Alon, Matias, Szegedy]

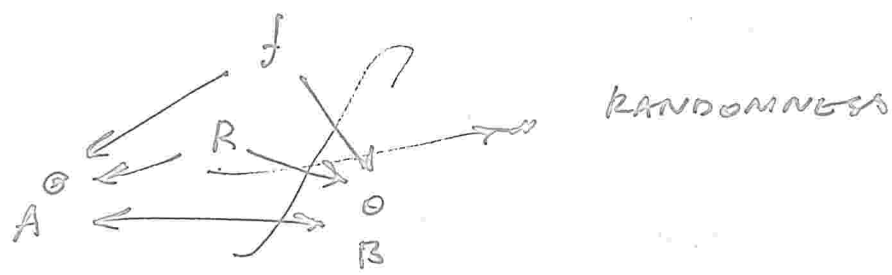
- IF $G\leftarrow N(0,1)^n$ then

$$E\underbrace{[\langle G,x\rangle\cdot\langle G,y\rangle]}_{\text{UNBIASED ESTIMATOR}}=\langle x,y\rangle$$

SUMMARY FROM [Ghazi, Kamath 16]

UNCERTAINTY IN COMMUNICATION

ARE THE COMMUNICATION MECHANISM THAT CAN OVERCOME UNCERTAINTY ?



MODEL: IMPERFECTLY SHARED RANDOMNESS

- ALICE ← r, B ← s WHERE

(r, s) = INDEPENDENT SEQUENCE OF CORRELATED PAIRS $(r_i, s_i)_i$;

$r_i, s_i \in \{-1, +1\}$; $E(r_i) = E(s_i)$;

$E(r_i s_i) = \rho \geq 0$

- NOTATION

- $isr_\rho(f)$ = CC of f with ρ-correlated bits
- cc(f) perfectly shared randomness
- priv(f): cc with PRIVate randomness

- starting point: for Boolean f:

- $cc(f) \leq isr_p(f) \leq priv(f) \leq cc(f) + \log n$

Can we get away with constant communication?

- What if $cc(f) << \log(n)$?

DISTILL PERFECT RANDOMNESS FROM ISR

- AGREEMENT DISTILLATION:

— Alice $\leftarrow r$, Bob $\leftarrow s$; (r, s) p-corr. unb. bits.

— outputs: $A \longrightarrow u$, $B \longrightarrow v$

$H_\infty(u), H_\infty(v) \geq k$

— communication $= c$ bits

— what is max prob. r of agreement $(u = v)$

— well studied!

We cannot individually reduce randomness and compute

$\longrightarrow$ requires the use of a new model.

Results.

model first studied by [Bavarian, Gavinsky, Ito K]

- Their focus: simultaneous communication, general models of correlation
- isr (Equality) = $O(1)$

- ?'s results

$$cc(f) \le k \Rightarrow isr(f) \le 2^k$$

Converse

$$\exists f \text{ with } cc(f) \le k \ \& \ isr(f) \ge 2^k$$

Equality testing proof

- encode $x \mapsto X = \mathcal{E}(x)$; $y \mapsto Y = E(y)$; $X, Y \in \{-1,+1\}^N$
- $x = y \Rightarrow \langle X, Y \rangle = N$
- $x \ne y \Rightarrow \langle X, Y \rangle \le \frac{N}{2}$

so not look at a particular coordinate!

Better: how do they correlate with random Gaussian vectors

Bending on sketching protocols

A: pick Gaussians $G_1, \dots, G_t \in \mathbb{R}^N$

sends $i \in [t]$ maximizing

$\langle G_i, x \rangle$ to Bob.

Bob: accepts iff $\langle G'_i, y \rangle \geq 0$.

Thought that the same random vectors are not necessary

$\longrightarrow$ can use slightly positively correlated Gaussians.

Averaging Gaussians $\longrightarrow$ same correlation as the initial sequence.

Analysis: $O_p(1)$ bits suffice if $G \sim G_{p}'$

Matching lower bound:

There exists a (promise) problem f:

$$ee(f) \leq k$$
$$\text{isup}(f) \geq \exp(k)$$

- Gap Sparse Inner Product
- Alice gets <u>sparse</u>

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

- 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.

Invariance Principle MOO 08

Informally:

. Analysis of prob. processes with bits often hard

. related processes with Gaussian variables is easy

. $\boxed{IV:}$ under suff. general conditions prob. of events "invariant" when switching from bits to Gaussians

---

k bits of comm. with pub. sharing

$\longrightarrow$ 2^k bits with imp. sh.

this is right

What's necessary: introducing scale (constant very large)

9

what happens when randomness is private.

$\longrightarrow$ ~~the~~ sample the entire distribution corresponding to messages

$\Longrightarrow$ makes randomness deterministic

If problems are solved on the sphere

$\Rightarrow$ easy to solve on the cube

---

equality testing: can we get away with constant cost?

---

no shared randomness: everything that can be done

works by adding a constant term