Communication with Imperfect Shared Randomness

(Joint work with Venkatesan Guruswami (CMU), Raghu Meka (?) and Madhu Sudan (MSR))

Who? Clément Canonne (Columbia University)
When? November 19, 2014
Communication & Complexity

There is a world outside of $n$

Context

There is Alice, Bob, what they communicate and what they don’t have to.
Communication & Complexity
There is a world outside of $n$

Context

There is Alice, Bob, what they communicate and what they don’t have to.
The
$$f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\},$$
they compute; the protocol

$$\Pi$$

they use; from which

$$D_x, D_y$$

their inputs come; what is blue and what red means.
Communication & Complexity

But context is not perfect...

Context is almost never perfectly shared.

Noise, misunderstandings, false assumptions
Communication & Complexity
But context is not perfect . . .

Context is almost never perfectly shared.

My periwinkle is your orchid.
Communication & Complexity

But context is not perfect…

Context is almost never perfectly shared.

- My *periwinkle* is your *orchid*.
- the printer on the 5th floor of Columbia is not *exactly* the model my laptop has a driver for.
Communication & Complexity

But context is not perfect... 

Context is almost never perfectly shared.

- My *periwinkle* is your *orchid*.
- the printer on the 5th floor of Columbia is not *exactly* the model my laptop has a driver for.
- what precisely is a “French baguette” around here?
Communication & Complexity

What about randomness?

I have \( x \in \{0, 1\}^n \), you have \( y \in \{0, 1\}^n \), are they equal?

- Deterministic \( \text{det-cc}(\text{EQ}) = \Theta(n) \)
- Private randomness \( \text{private-cc}(\text{EQ}) = \Theta(\log n) \)
- Shared randomness \( \text{psr-cc}(\text{EQ}) = O(1) \)

(Recall Newman’s Theorem:

\[
\text{private-cc}(P) \leq \text{psr-cc}(P) + O(\log n).
\]
This work

Randomness and uncertainty

What if the randomness ("context") was not perfectly in sync?

To compute $f(x, y)$:

- Alice: has access to $r \in \{\pm 1\}^*$, gets input $x \in \{0, 1\}^n$
- Bob: has access to $s \in \{\pm 1\}^*$, gets input $y \in \{0, 1\}^n$

w/ $r \sim \rho s$: $\mathbb{E}r_i = \mathbb{E}s_i = 0$, $\mathbb{E}r_is_i = \rho$, $(r_i, s_i) \perp \perp (r_j, s_j)$. 

Studied (independently) by [BGI14] (different focus: "referee model"; more general correlations).
This work
Randomness and uncertainty

What if the randomness ("context") was not perfectly in sync?

To compute $f(x, y)$:
- Alice: has access to $r \in \{\pm 1\}^*$, gets input $x \in \{0, 1\}^n$
- Bob: has access to $s \in \{\pm 1\}^*$, gets input $y \in \{0, 1\}^n$

w/ $r \sim \rho s$: $\mathbb{E}r_i = \mathbb{E}s_i = 0$, $\mathbb{E}r_is_i = \rho$, $(r_i, s_i) \perp \perp (r_j, s_j)$.

Studied (independently) by [BGI14] (different focus: "referee model"; more general correlations).
ISR: general relations

For every $P$ with $x, y \in \{0, 1\}^n$ and $0 \leq \rho \leq \rho' \leq 1$,

$$\text{psr-cc}(P) \leq \text{isr-cc}_{\rho'}(P) \leq \text{isr-cc}_{\rho}(P) \leq \text{private-cc}(P) \leq \text{psr-cc}(P) + O(\log n).$$

(also true for one-way: $\text{psr-cc}^{ow}, \text{isr-cc}_{\rho}^{ow}, \text{private-cc}^{ow}$)

$\rightsquigarrow$ but for many problems, $\log n$ is already huge.
Rest of the talk

1. A first example: the **Compression** problem
2. General upperbound on ISR in terms of PSR
First result: Compression

Alice has $P$, gets $m \sim P$; Bob knows $Q \simeq P$, wants $m$.

**Previous work**

- $P = Q$
- $P \sim_{\Delta} Q$
- $P \approx_{\Delta} Q$

- $H(P)$ (Huffman coding)
- $H(P) + 2\Delta$ [JKKS11] (w/ shared randomness)
- $O(H(P) + \Delta + \log \log N)$ [HS14] (deterministic)
First result: Compression

Alice has $P$, gets $m \sim P$; Bob knows $Q \simeq P$, wants $m$.

Previous work

$P = Q$

$P \simeq \Delta Q$

$P \simeq \Delta Q$

This work

For all $\epsilon > 0$,\[ \text{isr-cc}^\text{ow}_\rho (\text{COMPRESS}_\Delta) \leq \frac{1+\epsilon}{1-h(\frac{1-\rho}{2})}(H(P) + 2\Delta + O(1)) \]

“natural protocol”
Theorem

∀ρ > 0, ∃c < ∞ such that ∀k, we have

$$\text{PSR-CC}(k) \subseteq \text{ISR-CC}^\text{ow}_\rho (c^k).$$

Proof.

(Outline)

- Define $\text{GapInnerProduct}$, “complete” for PSR-CC($k$) (see strategies as $X_R, Y_R\{0, 1\}^{2^k}$; use Newman’s Theorem to bound $\# R$’s);
- Show there exists a (Gaussian-based) isr protocol for $\text{GapInnerProduct}$, with $O_\rho(4^k)$ bits of comm.
General upperbound

Can we do better?

For problems in PSR-CC\(^\omega(k)\)?

\[
\text{PSR-CC}^{\omega}(k) \subseteq \text{ISR-CC}^{\omega}(c^{o(k)})?
\]

For ISR-CC\(_\rho\)?

\[
\text{PSR-CC}(\omega(k)) \subseteq \text{ISR-CC}_\rho(c^k)\
\]
General upperbound
Can we do better?

For problems in $\text{PSR-CC}^{\omega w}(k)$?

For $\text{ISR-CC}_\rho$?

Answer: No.

$\text{PSR-CC}^{\omega w}(k) \subseteq \text{ISR-CC}^{\omega w}_\rho(c^{o(k)})$?

$\text{PSR-CC}(\omega(k)) \subseteq \text{ISR-CC}_\rho(c^k)$?
Strong converse: lower bound

It’s as good as it gets.

∀k, ∃P = (P_n)_{n \in \mathbb{N}} \text{ s.t. } \text{psr-cc}^{ow}(P) \leq k, \text{ yet } \forall \rho < 1 \text{ isr-cc}_\rho(P) = 2^{\Omega_\rho(k)}.

Proof.

(High-level)

- Define \text{SparseGapInnerProduct}, relaxation of \text{GapInnerProduct}.
- Show it has as $O(\log q)$-bit one-way psr protocol (Alice uses the shared randomness to send one coordinate to Bob)
- isr lower bound: argue that for any (fixed)* strategy of Alice and Bob using less than $\sqrt{q}$ bits, either (a) something impossible happens in the Boolean world, or (b) something impossible happens in the Gaussian world.
Strong converse: lower bound
Two-pronged impossibility, first prong.

Case (a)

The strategies \((f_r, g_s)_r,s\) have common high-influence variable (*recall the one-way psr protocol*).
But then, two players Charlie and Dana can* leverage this strategies to win an *agreement distillation* game:

Charlie and Dana have no inputs. Their goal is to output \(w_C\) and \(w_D\) satisfying:

\[
\Pr[w_C = w_D] \geq \gamma; \\
H_\infty(w_C), H_\infty(w_D) \geq \kappa.
\]

But this requires \(\Omega(\kappa) - \log(1/\gamma)\) bits of communication (via [BM10, Theorem 1]).
Strong converse: lower bound

Two-pronged impossibility, second prong.

Case (b)

\[ f_r : \{0, 1\}^n \rightarrow K_A \subset [0, 1]^{2^k}, \ g_s : \{0, 1\}^n \rightarrow K_B \subset [0, 1]^{2^k} \]

have no common high-influence variable.

We then show that this implies \( k = 2^{\Omega(\sqrt{q})} \), by using an Invariance Principle (in the spirit of [Mos10]) to “go to the Gaussian world”: if \( f, g \) are low-degree polynomials with no common influential variable, then

\[
E_{(x,y) \sim N^\otimes n} [\langle f(x), g(y) \rangle] \simeq E_{(X,Y) \sim G^\otimes n} [\langle F(X), G(Y) \rangle]
\]

and Charlie and Dana can use this solve (yet another) problem, the Gaussian Inner Product (GAUSSIANCORRELATION_\xi).

But... a reduction to DISJOINTNESS shows that (even with psr) this requires \( \Omega 1/\xi \) bits of communication.
Conclusions

Summary

- Dealing with more realistic situations: Alice, Bob, and what they do not know about each other;
- Comes into play when $n$ is huge (Newman’s Theorem becomes loose);
- Show general and tight relations and reductions in this model, with both upper and lower bounds.
- A new invariance theorem, and use in comm. complexity.
Conclusions

Summary

- Dealing with more realistic situations: Alice, Bob, and what they do not know about each other;
- comes into play when $n$ is huge (Newman’s Theorem becomes loose);
- show general and tight relations and reductions in this model, with both upper and lower bounds.
- a new invariance theorem, and use in comm. complexity.

What about. . .

- more general forms of correlations?
- cases where even randomness is expensive? (minimize its use)
- one-sided error?
Thank you.

(Questions?)
Theorem (Our Invariance Principle)

Fix any two parameters $p_1, p_2 \in (-1, 1)$. For all $\varepsilon \in (0, 1]$, $\ell \in \mathbb{N}$, $\theta_0 \in [0, 1)$, and closed convex sets $K_1, K_2 \subseteq [0, 1]^\ell$ there exist $\tau > 0$ and mappings

$$
T_1 : \{f : \{+1, -1\}^n \to K_1\} \to \{F : \mathbb{R}^n \to K_1\}
$$
$$
T_2 : \{g : \{+1, -1\}^n \to K_2\} \to \{G : \mathbb{R}^n \to K_2\}
$$

such that for all $\theta \in [-\theta_0, \theta_0]$, if $f, g$ satisfy

$$
\max_{i \in [n]} \min_{j \in [\ell]} \left( \max_{j \in [\ell]} \inf_i (d) f_j, \max_{j \in [\ell]} \inf_i (d) g_j \right) \leq \tau
$$

then, for $F = T_1(f)$ and $G = T_2(g)$, we have where $N = N_{p_1, p_2, \theta}$ and $G$ is the Gaussian distribution which matches the first and second-order moments of $N$. 


Let $(\Omega, \mu)$ be a finite prob. space with each prob. at least 
\[ \alpha \leq 1/2. \] Let \( b = |\Omega| \) and \( \mathcal{L} = \{\chi_0 = 1, \chi_1, \chi_2, \ldots, \chi_{b-1}\} \) be 
a basis for r.v.'s over \( \Omega \). Let \( \Upsilon = \{\xi_0 = 1, \xi_1, \ldots, \xi_{b-1}\} \) be 
an ensemble of real-valued Gaussian r.v.'s with 1\textsuperscript{st} and 2\textsuperscript{nd} 
moments matching those of the \( \chi_i \)’s; and 
\( h = (h_1, h_2, \ldots, h_t): \Omega^n \to \mathbb{R}^t \) s.t.

\[ \inf_i (h_\ell) \leq \tau, \quad \text{Var}(h_\ell) \leq 1 \]

for all \( i \in [n] \) and \( \ell \in [t] \). For \( \eta \in (0, 1) \), let \( H_\ell \ (\ell \in [t]) \) be 
the multilinear polynomial associated with \( T_{1-\eta} h_\ell \) w.r.t. \( \mathcal{L} \).

If \( \Psi: \mathbb{R}^t \to \mathbb{R} \) is \( \Lambda \)-Lipschitz (w.r.t. the \( L_2 \)-norm), then

\[
\left| \mathbb{E}\left[ \Psi(H_1(\mathcal{L}^n), \ldots, H_t(\mathcal{L}^n)) \right] - \mathbb{E}\left[ \Psi(H_1(\Upsilon^n), \ldots, H_t(\Upsilon^n)) \right] \right| 
\leq C(t) \cdot \Lambda \cdot \tau^{\frac{n}{18}} \log \frac{1}{\alpha} = o_\tau(1)
\]

for some constant \( C = C(t) \).
Mohammad Bavarian, Dmitry Gavinsky, and Tsuyoshi Ito.
On the role of shared randomness in simultaneous communication.
In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors,

Andrej Bogdanov and Elchanan Mossel.
On extracting common random bits from correlated sources.

Venkatesan Guruswami, Johan Håstad, Rajsekar Manokaran, Prasad Raghavendra, and Moses Charikar.
Beating the random ordering is hard: Every ordering CSP is approximation resistant.

Elad Haramaty and Madhu Sudan.
Deterministic compression with uncertain priors.
In Proceedings of the 5th Conference on Innovations in Theoretical Computer Science,
ITCS ’14, pages 377–386, New York, NY, USA, 2014. ACM.

Brendan Juba, Adam Tauman Kalai, Sanjeev Khanna, and Madhu Sudan.
Compression without a common prior: an information-theoretic justification for ambiguity in language.

Elchanan Mossel.
Gaussian bounds for noise correlation of functions.