CS229r - Interactive Coding - 1

[4/18/17 & 4/20/17]

Challenge: Can you preserve an interaction when channel is (adversarially? / randomly?) noisy.

Example: Two players playing online chess over noisy channel. (ignoring strategic / computational issues).

Interaction: $A \rightleftarrows B$:

given by two functions: $\Pi_A = \{\Pi_A^{(i)}\}_{i \text{ odd}}$ & $\Pi_B = \{\Pi_B^{(i)}\}_{i \text{ even}}$

$$\Pi_A^{(i)} : \left(\{0,1\}^*\right)^{i-1} \longrightarrow \{0,1\}^* \cup \{\perp\} \quad i \text{ odd}$$

$$\Pi_B^{(i)} : \left(\{0,1\}^*\right)^{i-1} \longrightarrow \{0,1\}^* \cup \{\perp\} \quad i \text{ even}$$

$\Pi_A^{(i)}(w_1 \ldots w_{i-1})$ ~~says~~ specifies what Alice would say in round i after history of transcript $w_1 \ldots w_{i-1}$.

$\Pi_A^{(i)}(\ldots) = \perp \Rightarrow$ end of interaction. Output $= (w_1 \ldots w_k)$.

In general: w_i may be random variables, but for us w_i = det. function of $w_1 \ldots w_{i-1}$.

In general: $w_i \in \{0,1\}^*$, but for us suffices to consider $w_i \in \{0,1\}$. [stretches interaction by at most factor of 2].

In general: variable length interaction, but for us length $= k$.

Noisy Interactive Coding [Schulman '92]

- What happens to interaction if channel is noisy.
- Send w_i receive w_i'] $\frac{1}{k}$ fraction of interation
  - Without correction $\Rightarrow$ immediately changes all future messages & ~~the~~ so entire interaction changes.
  - With (standard) Error Correction: Adversary can still change $E(w_i)$ to $E(w_i')$ & get same ~~of~~ effect.
  - Need New Solution!

~~Simulating from Noisy interaction~~

~~Given $(\Pi_A, \Pi_B) \Rightarrow (\sigma_A, \sigma_B, f_A, f_B)$~~

~~$\sigma_A, \sigma_B \rightarrow$ N-round interaction outputting $x_1 \ldots x_N$~~

Solution Concept: Interactive Coding with ϵ-fraction error

$\Pi_A, \Pi_B \longrightarrow (\sigma_A, \sigma_B, f_A, f_B)$

s.t. for every sequence $a_1 \ldots a_n$, $b_1 \ldots b_n$ s.t.

- $a_i = \sigma_A^{(i)}(a_1 \ldots a_{i-1})$ odd i
- $b_i = \sigma_B^{(i)}(b_1 \ldots b_{i-1})$ even i
- $\# \{ i \mid a_i \neq b_i \} \leq \epsilon n$

it is the case that

$$f_A(a_1 \ldots a_n) = f_B(b_1 \ldots b_n) = w_1 \ldots w_R = \text{output}(\Pi_A, \Pi_B)$$

(σ_A & σ_B possibly operating on different strings!)

Solution Ingredient: Tree Code: (c, d, δ)-tree code T.

$T: \{0,1\}^{c \cdot n} \rightarrow \{0,1\}^{dn}$

Rate $= \frac{c}{d}$

s.t. (1) $T(m_1 \ldots m_e \ldots m_n)_i$ depends only on $T(m_1 \ldots m_i)$

$T(\ldots)_i \in \{0,1\}^d$ $\qquad m_j \in \{0,1\}^c$

(2) $\forall$ $m_1 \ldots m_n$, $m'_1 \ldots m'_n$ s.t. $m_1 = m'_1 \ldots m_i = m'_i$ & $m_{i+1} \neq m'_{i+1}$

$$\Delta\big(T(m_1 \ldots m_n), T(m'_1 \ldots m'_n)\big) \geq (n-i) \cdot \delta \cdot d$$

[Prefix necessarily agrees; but suffix may not.]

Rest of Lecture

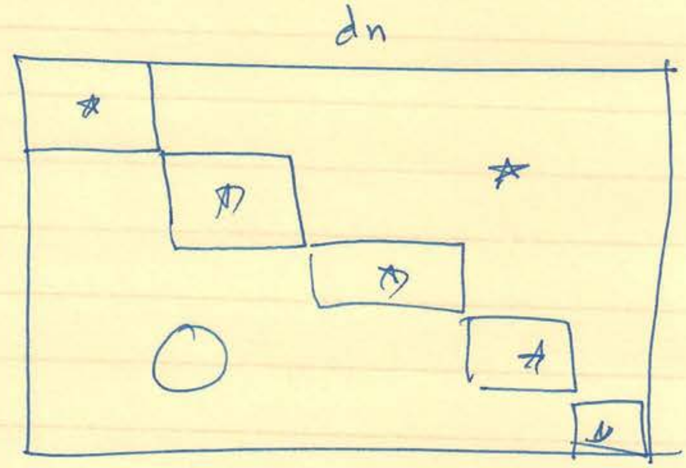
1. Proving Tree Codes exist
2. Using Tree Codes.

—— x ——

(1) • Random "Tree" functions fail w.p. $\to 1$; so need care

• Random linear Code works!

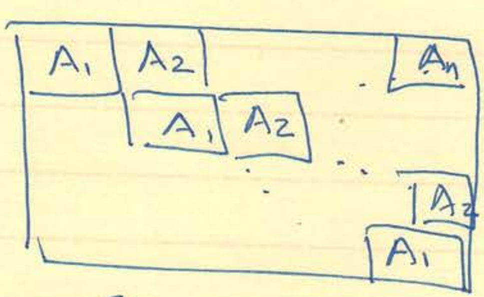
$T(m)$: $\boxed{m_1 \; m_2 \; \ldots \; m_n}$



Encoding matrix is "upper triangular".

Claim: $\Pr_T\left[\, i^{th} \text{ prefix of } T \text{ works} \right] \geq c - \exp(-i)$.

~~"i^{th} prefix works" if $\forall\, m_1 .. m_i$ ω~~ T = Toeplitz =



i^{th} prefix works if $\forall j \leq i$

$\forall\, m_1 .. m_j$ with $m_1 \neq 0$ $\quad \delta(T_j(m_1 .. m_j), 0) \geq \delta \cdot j \cdot d$

$\boxed{\text{Proof Omitted}}$

Using Tree Codes: (Non-Trivial)

Two approaches: (1) Schulman: "Local" approach
(2) Braverman-Rao: "Holistic" approach.

Schulman: More Natural; Analysis weaker
B-R: Less Natural; Less wasteful (provably).

Common features

1) A + B maintain states: $S_A^{(i)}, S_B^{(i)}$ $i = 1 \dots 5n$.
2) Compress: $S_A^{(1)} \dots S_A^{(t)} \Rightarrow x^{(1)} \dots x^{(t)}$
(prefix-respecting
3) Tree code $(x^{(1)} \dots x^{(t)})$ & communicate to B
(similarly for Bob).

Differences

1) State = ?
2) Evolves = How?
3) Analysis ?

Common Preprocessing: 1) Alice + Bob exchange 1 bit simult. at each stage (in original protocol)
2) original protocol extended to $5n$ rounds with $4n$ rounds computing nothing.
$\Rightarrow$ At end of simulation Players agree on ~~at~~ node at n^{th} level. $(w_1 \dots w_n)$.

Schulman Protocol

- Protocol tree : Π

  [~~k-ary~~ binary rooted tree of depth n]

  : Nodes at depth i record bits ~~exchanged~~ sent in first i rounds.

  $\in \cancel{\{0,1\}^{2i}} \cdot \{0,1\}^i$

- $S_A^{(i)}$ = ~~Start node labelled~~ node reached in Π after i rounds (according to A).

- Evolution Property (to be delivered later)

  ⓐ $|S_A^{(i)}| = |S_A^{(i-1)}| \pm 1$. [Move locally]

  length = percieved progress

  can go down. must go down due to errors!

  ⓑ $S_A^{(i)}$ = Bob comm. node.

- Compression $(S_A^{(1)} \cdots S_A^{(i)})$

  $= x_1 \cdots x_i$ s.t. $(S_A^{(i-1)}, x_i) \Rightarrow (S_A^{i})$ determine

  Note $x_i \in \{0,1\}^c$

- Communication : $T(x_1 \ldots x_i)_i$ (A $\to$ B in round i)

State Evolution:

only even # indices

Given communication: $\overset{a_1 \dots a_{i-1}}{\cancel{z_1 \dots z_{i-1}}} \in \{0,1\}^{d\frac{(i-1)}{2}}$ from B→A ~~thus far~~ ~~from B→A~~

(i) $\text{Decode}(\overset{a_1 \dots a_{i-1}}{\cancel{z_1 \dots z_{i-1}}}) = \hat{y}_1 \dots \hat{y}_{i-1} \in \{0,1\}^{c(i-1)}$

(ii) Compute $G_B^{(1)} \dots G_B^{(i-1)}$ from $(\hat{y}_1 \dots \hat{y}_{i-1})$

(iii) <u>if</u> $S_A^{(i-2)} = \text{parent}(G_B^{(i-1)})$

<u>then</u> $S_A^{(i)} =$ "correct child of $G_B^{(i-1)}$"

<u>else</u> let $U =$ <u>least-common-ancestor</u> $(S_A^{(i-2)}, G_B^{(i-1)})$ ← LCA

if $U = S_A^{(i-2)} \Rightarrow S_A^{(i)} = S_A^{(i-2)}$

~~if~~ else Backtrack two steps

$$\left(|S_A^{(i)}| = |S_A^{(i-2)}| - 2\right).$$

<u>Analysis</u>: $\phi_i = |U^{(i)}| - \left(|S_A^{(i)}| - |U|\right) - \left(|S_B^{(i)}| - |U|\right)$

where $U^{(i)} = \underline{LCA}(S_A^{(i)}, S_B^{(i)})$

<u>Claims</u>: ① $\forall i \quad \phi_i \geq \phi_{i-1} -$ <u>const</u>

② For "good" i; $\phi_i \geq \phi_{i-1} +$ const.

③ Fraction of "bad" $i \to 0$ as fraction of errors $\to 0$.

i is ϵ-good if $\forall\ j \in [1 \ldots i]$,

~~# errors~~ $\Delta(a_{j:i}, b_{j:i}) \leq \epsilon \cdot (i-j+1)$

Proofs: 1 By definition + construction

2 if i-good then (i) $G_B^{(i)} = S_B^{(i)}$ (~~By~~ if Tree code decodes ϵ-fraction)

(ii) So if $S_B^{(i)} = \text{child}(S_A^{(i-1)})$

then $|U^{i-1}| = S_A^{(i-1)}$ & $\underbrace{|U^i| \geq |U^{i-1}| + 1}$

So we make progress on $|U|$ part.

(iii) if $S_B^{(i)} \neq \text{child}(S_A^{(i-1)})$

we shrink one of

$|S_A^i| - |U^i|$ or $|S_B^i| - |U^i|$

& don't decrease $|U^i|$

3 Simple counting ... every error hurts $(1/\epsilon)$ i's.

$\Rightarrow \tau$ fraction errors $\Rightarrow \left(\frac{\tau}{\epsilon}\right)$ bad i's.

$\downarrow$

0 as $\tau \to 0$.

Conclusion: at end $\phi_{5n} \geq n \Rightarrow |U| \geq n \Rightarrow A$ & B agree on leaf of Π.

Summary of Schulman Solution

1. Corrects $\Omega(1)$ - fraction error ✓
2. But not maximal - fraction ✗
3. Non-constructive: - Tree Codes "exist"
   - Decoding : Brute Force

Current State of Art

1. Exact capacity (even with random errors) unknown.
2. Maximal Fraction Errors essentially known [Braverman - Rao, ...]
3. Rate as error $\to 0$ essentially known.

$$\text{error} = \epsilon \to 0 \Rightarrow \text{Rate} \approx 1 - \tilde{O}(\sqrt{\epsilon})$$

[Kol, Raz]
[Haeupler]

in contrast to $1 - \tilde{O}(\epsilon)$ for 1-way interaction

4. Polynomial time encoding + decoding essentially known

[Brakerski, Kalai, ...]