[Braverman- Rao] Coding Scheme

• ~~States of A are~~

Terminology : Alice's Input = set of edges in binary tree of depth n ;
one edge out of every node at level i for even i going to level $(i+1)$.

Bob : Similar.

States Alice: $S_1 \subseteq S_2 \subseteq S_3 \ldots$

S_i = Subset of Alice's edges ; Ones she thinks are relevant.

Evolution of S_i: Alice remembers S_i ;
Compute $\tilde{T}_i$ = guess of Bob's state
Uses $\underbrace{S_i \cup \tilde{T}_i}$ to determine S_{i+1}.
⇓
gives unique path from root (+ isolated edges/paths).
$v(S_i \cup \tilde{T}_i)$ = bottom vertex.
If v is even vertex then add edge out of v to S_i to get S_{i+1} else $S_{i+1} = S_i$.

Encoding of S_i:

① Obvious idea: $S_i = S_{i-1} \cup e_i$

Need to send only e_i in round i: $\Omega(n)$ bits!

② Can encode e_i as $(j, b_1 b_2)$ s.t.

- e_j = granparent edge of e_i
- b_1, b_2: specify e_i given e_j.
- $\Theta(\log n)$ bits.

③ Final Encoding

- $\Delta_i = i - j$ where e_j = grandparent of e_i.
- Send Δ_i,
- Still uses $O(\log n)$ bits to send Δ_i in worst case.
- But amortized complexity ~~on~~ for ~~good~~ correct path $= O(n)$.

Need some care.

- if # rounds $= R = C \cdot n$, then $\sum_{\substack{i \text{ on} \\ \text{correct path}}} \Delta_i \leq R$

$$\Rightarrow \sum_{\substack{i \text{ on} \\ \text{correct path}}} \log \Delta_i \leq n \log C \quad (\text{convexity}) \ll C \cdot n.$$

Full Protocol

State : $S_i = A_i + \cancel{e_t}$ prefix (encoding (e_i))

set of added edges; ~~pending~~

Use $A_i \cup \tilde{B}_i$ & to determine next edge to send. if next edge $= e_i$ then send few more bits about e_i ;
else $\boxed{\text{abort}}$ e_i, start sending next edge;
if e_i completely sent then $A_{i+1} = A_i \cup \{e_i\}$.

$\boxed{\text{abort}}$ crucial to analysis

Analysis: key notions:

$\ell^A(t) \triangleq$ Decode-length $(a_2, a_4, a_6 \dots a_t)$ = largest ℓ s.t.

$$(a_2, a_4 .. a_\ell) = (b_2, b_4, .. b_\ell).$$

$\ell^B(t) \triangleq$ Decode-length $(b_1, b_3, b_5, .. b_t)$ = largest ℓ s.t.

$$(b_1 .. b_\ell) = (a_1 .. a_\ell)$$

$$m(t) \triangleq \min\{\ell^A(t), \ell^B(t)\}.$$

Note : $m(t)$ not monotone with t ; but as $t \to \infty$

$$m(t) \to \infty.$$

$\boxed{m^{-1}(\ell) = t \text{ s.t. } \forall\, t' \geq t \ \ m(t') \geq \ell.}$

- $t(i)$ = smallest round i for which first i edges of P are in $A_t \cup B_t$.

- $N(t_1, t_2)$ = # errors in rounds $(t_1 \ldots t_2)$

Key Observations: ① Once $t > t(i)$, only a matter of time till the $i+1^{st}$ edge enters $A_t \cup B_t$.

Main (Only) Obstacle to this is $N(t, t')$

② if $t - m(t)$ large then $N(m(t)+1, t)$ large.

[purely function of tree code, not protocol].

③ if $t < t(k)$ then $N(1,t) \geq$ ~~$(t-k+1)\cdot\delta$~~

$\delta \hat{=}$ ~~dist. of tree code.~~

~~{follows from ① + ②~~

$$\left(t - k + 1 - \sum c \log \Delta_s\right)\left(\frac{\delta}{2}\right)$$

$[\exists \Delta_1 \ldots \Delta_k$ s.t. $\sum \Delta_i \leq t] \ldots$

Schulman vs. Braverman Rao (in joke form)

(A) Suppose you ask me "Proof of Fermat's Theorem = ?"

(B) I start filling the board with "Group Theory", "Galois Groups" "Modular Forms", "Semi Stable Representations"

(C) You stop me (after 3 hours) and say "I mean Fermat's little Theorem" ....

Schulman approach.

1. Be embarrassed
2. Erase the board & start again

Braverman Rao Approach

1. Be shameless & continue [Use existing contents of Board "Group Theory"]
2. Focus more on "Basic Group Theory", "Pigeonhole Principle" etc.
3. & Just in case I misheard you on round (C) throw in a few more steps of F.Last.T. "Semistable Representations", "Galois Cohomology" ....

Shockingly: Latter is the right approach? ☺

Main Deficiency with Schulman / Braverman-Rao

1. Tree Codes not explicit
2. Decoding of Tree Codes not explicit.

Fixed (to some extent) by

[Brakerski - Kalai] ; [Ghaffari- Haeupler].

Key Idea : (1) ~~Sender~~ A + B use private randomness.

(2) Hash then check.

Recall Alice has states $S_1^A, S_2^A, \ldots S_t^A \ldots$

& Bob . . . . $S_1^B, S_2^B \ldots S_t^B$

- At round t Alice hopes to have communicated S_t^A to Bob ; and recovered S_t^B.

- Brakerski - Kalai Idea : Start with both players knowing

$$(S_{t-1}^A, S_{t-1}^B)$$

$$(S_t^A, S_t'^B), \quad (S_t'^A, S_t^B)$$

Use hash function h & hash value to check equality

$$\xrightarrow{h,\ h(S_t^A, S_t'^B)}$$

if $|S_A, S_B| \approx n$, $|h, h(\ )| \approx \log n$.

- But $|(S_A | S_{A-1})| \approx O(1)$? (in Schulman, B-R)
- take every $(\log n)^{th}$ round state in π;

  so that $(S_A | S_{A-1}) \cong O(\log n)$;

  So hashing cost $= \Theta$(State Progress).

- Use Schulman-like progress measure to roll back interaction or make progress.

Theorems: [Brakerski-Kalai] Randomized efficient Communication scheme with positive rate & error

[Ghaffari-Haeupler] "

" & error $\to \frac{1}{4}$.

[Haeupler] Randomized scheme (with <u>no</u> tree coding) with rate $1 - \tilde{O}(\sqrt{\epsilon})$ & error ϵ.