INTERACTIVE CODING II

[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: $S_1 \subseteq S_2 \subseteq S_3 \ldots$

$S_i = \text{subset of Alice's Edges; ones she thinks are relevant.}$

Evolution of $S_i$: Alice remembers $S_i$;
Compute $\hat{T}_i = \text{guards of Bob's State}$
Uses $S_i \cup \hat{T}_i$ to determine $S_{i+1}$.

... gives unique path from root (not isolated edges/path).

$V(S_i \cup \hat{T}_i) = \text{bottom vertex.}$

If $V$ is even vertex then add edge out of $V$ to $S_i$ to get $S_{i+1}$ else $C = C$. 
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.
   - $e_j$ = grandparent 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 $e_j = \text{grandparent of } e_i$.
   - Send $\Delta_i$,
   - Still uses $O(\log n)$ bits to send $\Delta_i$ in worst case.
   - But amortized complexity for correct
     
     $\text{good path} = O(\log n)$

     Need some care.

   - If # rounds $= R = C \cdot n$, then $\leq \Delta_i \leq R$

   $\Rightarrow \leq \log \Delta_i \leq n \log C$ (convexity) $\leq C \cdot n$. 

   $i$ on correct path

   $i$ on incorrect path
Full Protocol

State: \( S_i = A_i + E_i \) pending prefix (decoding \( E_i \))

Use \( A_i \cup B_i \) to determine next edge to send. If next edge = \( e_i \) then send few more bits about \( e_i \);
else abort \( e_i \), start sending next edge;
if \( c_i \) completely sent then \( A_{i+1} = A_i \cup \{c_i\} \).

Abort crucial to analysis

Analysis: key notions:

\( C_{A_i}(t) \triangleq \) Decode length \( (a_2, a_4, a_6 \ldots a_{2t}) = \) largest \( l \) s.t.
\( (a_2, a_4 \ldots a_{2t}) = (b_2, b_4, \ldots b_{2t}) \).

\( C_{B_i}(t) \triangleq \) Decode length \( (b_1, b_3, b_5 \ldots b_{2t}) = \) largest \( l \) s.t.
\( (b_1 \ldots b_{2t}) = (a_1 \ldots a_{2t}) \).

\( m(t) \triangleq \min \{ C_{A_i}(t), C_{B_i}(t) \} \).

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

\((m^{-1}(e) = t \iff 4 \cdot t' \geq t \cdot m(t') \geq e)\).
- $t(i) =$ smallest round $i$ for which first $i$ edges of $P$ are in $A^E \cup U^{BE}$.

- $N(t_1, t_2) = \# \text{ errors in rounds } (t_1, t_2)$

**Key Observations:**
1. Once $t > t(i)$, only a matter of time till the $(i+1)^{st}$ edge enters $A^E \cup U^{BE}$.
2. If $t - m(\ell)$ large then $N(m(\ell) + 1, t)$ large.
   [purely function of tree code, not protocol]
3. If $t < t(k)$ then $N(t, t) \geq (\bar{N})^{\ell} \geq \left( \frac{\ell}{2} \right)$

[follows from (1) + (2)]

$(t - k + 1 - \varepsilon \log \Delta s) \left( \frac{\ell}{2} \right)$

[exists $\Delta_i$ s.t. $\Delta_i \leq t$]
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", "Semistable 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 and start again

Braverman Rao approach:
1. Be shameless and continue [use existing content on board "Group Theory"]
2. Focus more on "Basic Group Theory",
   "Pigeonhole Principle" etc.
3. Just in case I misheard you on round 2
   Throw in a few more steps if I last T.
   "Semistable Representation",
   "Galois Cohomology" ...

Shocking: 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] ; [Ghaithari-Heuerbr].

Key Idea: Sender A + B use private randomness.

1. Hash then check.

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

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

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

$$(S_t^A, S_t^B)$$

Use hash function $h$ & hash values to check equality $h, h(S_t^A, S_t^B)$. 
if $|S_A, S_B| = n$, $h, h(\cdot)| = \log n$.

- But $|S_{A|S_{A-1}}| \approx O(1)$? (in Schulman, B-R)

- take every $(\log n)^n$ round state in $\n$;

so $1/n^* (S_A | S_{A-1}) = O(\log n)$;

so hashing cost $= O(\text{State Progress})$.

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

Theorems: [Braverman-Kalai] Randomized efficient communication scheme with positive rate & error

[Ghaffari, Haeupler]

& error $\rightarrow \frac{1}{4}$.

[Haeupler] Randomized scheme (without tree coding) with rate $1 - O(\varepsilon^2)$, error $\varepsilon$. 