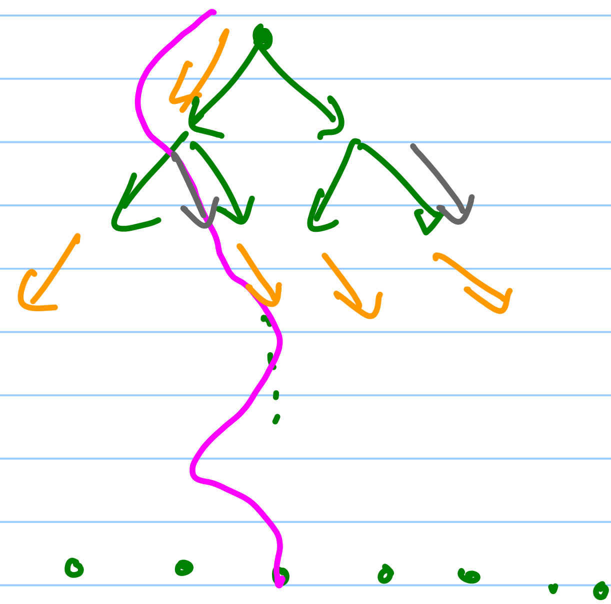
Notes on Interactive Coding

Note Title 10/1/2014

Instance of communication problem

- Tree of depth n ;



- Alice gets one outgoing edge for every vertex at odd depth
- Bob .... even depth
- Goal : Compute leaf

For simplicity Alice & Bob alternate.

Noisy channels :

- Channel takes symbols from finite alphabet;
- Transmits most as is ;
- Flips (adversarially) ϵ fraction.

Interactive Coding Scheme

Alice's Edges $\longmapsto$ Tree for Alice

Bob's Edges $\longmapsto$ Tree for Bob.

History

Tree Codes

Computationally Inefficient

$$
\begin{tikzcd}
\text{Schulman : '92, '93} \arrow[r] \arrow[d] & \text{Braverman-Rao} \arrow[dd] \\
\text{Brakerski-Kalai} \arrow[d] & \\
\text{Kol-Raz} \arrow[d] \arrow[dr] & \text{Braverman-Efremenko} \arrow[d] \\
\text{Haeupler} & \text{Ghaffari-Haeupler}
\end{tikzcd}
$$

Low Error State of the Art

High-error S-o-t-A.

Tree Codes

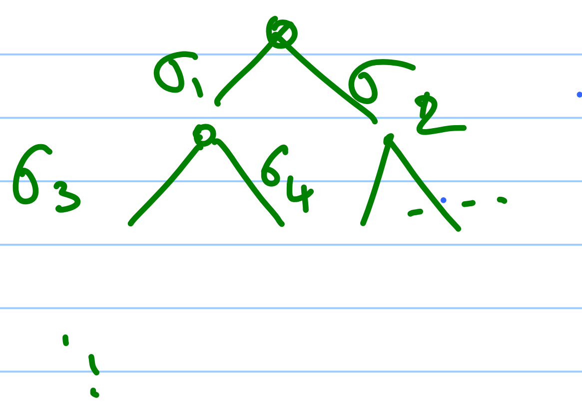
Solution tool due to [Schulman].

- "Online Error-Correcting Code"

$$T : \Sigma^n \longrightarrow \Gamma^n$$

$$\left(\text{Rate} = \frac{\log_2 |\Sigma|}{\log_2 |\Gamma|}\right)$$

- i^{th} symbol of $T(x_1 \ldots x_n)$ only depends on $x_1 \ldots x_i$.



Tree Encoder.

- Distance Property?

$$\Delta(T(0000000), T(0000001)) \le \frac{1}{n}!$$

* Can expect if

$$\underset{\text{transmitted}}{\Delta(T(x)}, \underset{\text{received}}{r)} < \epsilon \cdot n$$

then x_1 is uniquely determined

* More generally if

$$\Delta\left(T(x)_{j\ldots n}, y_{j\ldots n}\right) < \epsilon \cdot (n-j)$$

$\forall\, j \le i$, then x_i is uniquely determined

- Formalizing above gives defn. of ϵ-tree code.

Many Trees !

- Problem : Tree ①
- Alices Encoding : Tree ②
- Bob's Encoding : Tree ③
- Tool : Tree Code ④

- All are distinct entities.
- In particular ① & ④ mentioned often ...

[Schulman]:

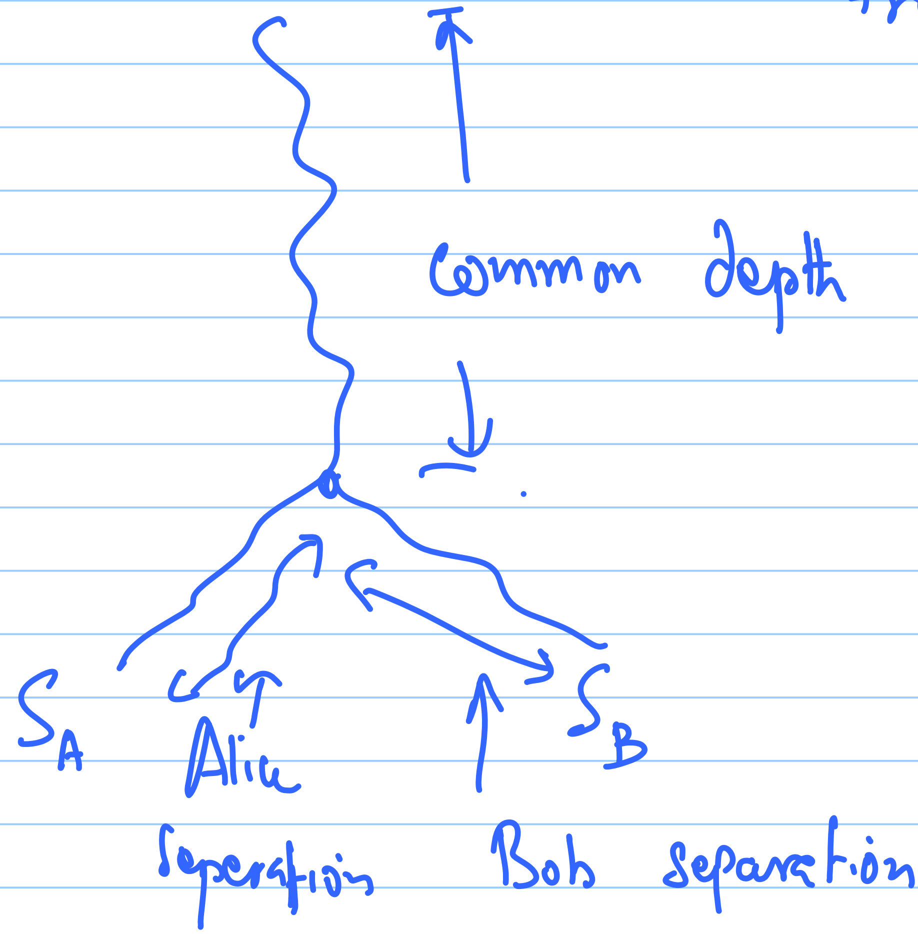
Central Idea:

- Alice + Bob maintain & communicate states on problem-tree
- if states agree proceed to next level
- if not backtrack
- Incrementally: Next State one of five given current state

  $\Rightarrow$ Wish to communicate sequence of 5-ary symbols

$\Rightarrow$ Use tree code with $|\Sigma| = 5$

- Quantities to track (on Problem tree)



- Invariant: At time t

$\alpha \cdot$ common depth $+$ $\beta \cdot$ #errors $\geq t$

- Will skip details

Caveats: Tree code exists. But not constructive.

[Braverman - Rao]

- Key Idea: Alice + Bob exchange sets of edges

$A \to B$: $S_1 \subseteq S_2 \subseteq S_3 \ldots \quad S_k \ldots$

$B \to A$: $T_1 \subseteq T_2 \subseteq T_3 \ldots \quad T_k \ldots$

- Alice :- Maintains S_i subset of <u>her</u> edges that she wishes to tell Bob about
  - Decodes Bob's communication to determine $\tilde{T}_i$ (set he seems to be sending).
  - Uses $S_i \cup \tilde{T}_i$ to determine S_{i+1}

- Analysis :

① Encoded properly $S_i \mid S_{i-1}$ is $O(1)$ bits.

② j_i = time i^{th} relevant edge appears in $S_j \cup T_j$

then #errors in $(j_i - j_{i-1})$

$$= \Omega(j_i - j_{i-1})$$

Efficiency + Brakerski-Kalai

- Both solutions so far need tree codes. ⇒ Non-constructive.
- Overcome this by a more "dynamic" status check.

[Brakerski-Kalai] + [Haeupler]

Suppose initial problem has

$A \to B \longrightarrow \log n$ bits per round

$B \to A \longrightarrow \log n$ bits per round.

[B-12] Solution :

- No coding / Simple ECC within round
- After each round of interaction

$$A \to B : \ h, \ h(S)$$

$$B \to A : \ h', \ h'(S')$$

- if any party finds hash mismatch it backtracks.

- Yields $\Omega(1)$ rate & $\Omega(1)$ error.

Why?

- $|h|, |h(S)| = O(\log n)$
- Round has few errors

$\Rightarrow$ Common length $-$ (divergence) $\uparrow$

- Careful analysis : ϵ-error $\Rightarrow$ $1-\sqrt{\epsilon}$ -rate.

Randomized Eff vs. Det. Exp. Time?

[Brakerski - Naor]

- Can fix sequence of "h"s in advance.
- Beats any fixed oblivious adversary with exp(-n) prob.
- Union bound ⟹ beats all adversaries.

Hashing dominates Tree Coding ....

(for low error).

(log n bit rounds).