

Predecessor lower bounds:

[Ajtai - Combinatorica 1988]

- first $w(1)$ bound: complicated (accidental claim)
- $\forall w \exists n$ s.t. $\Omega(\sqrt{\lg w})$ (of $\Omega(\lg w)$)

[Miltersen - STOC 1994]

- better understanding of "same" proof
- connection to communication complexity
- $\forall w \exists n$ s.t. $\Omega(\sqrt{\lg w})$
- $\forall n \exists w$ s.t. $\Omega(\sqrt[3]{\lg n})$

[Miltersen, Nisan, Safra, Wigderson - STOC 1995 & JCSS 1998]

- round elimination proof \sim clean
- introduction of round elim. technique

[Beame & Fich - STOC 1999 & JCSS 2002 & manuscript 1994]

- $\forall w \exists n$ s.t. $\Omega(\frac{\lg w}{\lg \lg w})$
- $\forall n \exists w$ s.t. $\Omega(\sqrt{\frac{\lg n}{\lg \lg n}})$
- static DS achieving $\tilde{O}(\min\{\frac{\lg w}{\lg \lg w}, \sqrt{\frac{\lg n}{\lg \lg n}}\})$
- \Rightarrow best "pure" bounds in n & w

[Xiao - Ph.D. thesis 1992 @ U.C. San Diego] < citation

- Same lower bounds! (still complicated)
- Beame & Fich was independent discovery

[Sen - CCC 2003; Sen & Venkatesh - JCSS 2006]

- round elimination proof ~ clean

TODAY

[Pătrașcu & Thorup - STOC 2006; SODA 2007]

- tight n vs. w vs. space trade-off: (static)

$n \cdot 2^a$

$$\Theta\left(\min\left\{\log_w n, \lg\left(\frac{w - \lg n}{a}\right), \frac{\lg \frac{w}{a}}{\lg\left(\frac{a}{\lg n} \lg \frac{w}{a}\right)}, \frac{\lg \frac{w}{a}}{\lg\left(\lg \frac{w}{a} / \lg \frac{\lg n}{a}\right)}\right\}\right)$$

fusion

van Emde Boas

$$-\text{Space } n \lg^{O(1)} n \Rightarrow \Theta\left(\min\left\{\log_w n, \frac{\lg w}{\lg \lg n}\right\}\right)$$

\Rightarrow van Emde Boas is optimal for $w = O(\lg n)$

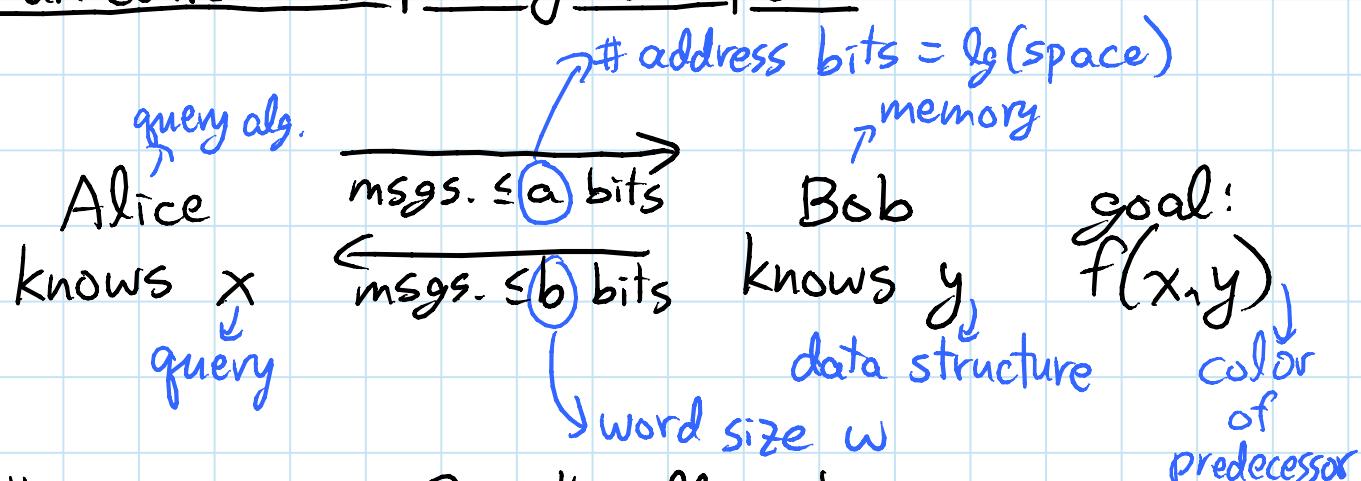
& fusion trees optimal for $\lg w = \Omega(\sqrt{\lg n \lg \lg n})$

new

Colored predecessor problem:

- each element is colored red or blue
- predecessor/succ. query just needs to return color
- easier problem \Rightarrow stronger lower bound
- useful for reductions later

Communication complexity viewpoint:



- # messages = $2 \cdot \# \text{cell probes}$
 (LOADs from memory)

Claim: $\Omega(\min\{\log_a w, \log_b n\})$

Corollary: Beame-Fich-Xiao pure bound

- assume $a = O(\lg n)$ (polynomial space)
- lower bound largest when

$$\log_a w = \log_b n$$

i.e. $\frac{\lg w}{\lg \lg n} = \frac{\lg n}{\lg w}$ (up to Θ)

i.e. $\lg^2 w = \lg n - \lg \lg n \Rightarrow \lg \lg w = \lg \lg n$

i.e. $\lg w = \sqrt{\lg n \cdot \lg \lg n}$

\Rightarrow lower bound is $\frac{\lg w}{\lg \lg n} = \sqrt{\frac{\lg n}{\lg \lg n}} = \frac{\lg w}{\lg \lg w}$

Round elimination:

$f^{(k)}$: variation on problem f

- Alice has k inputs x_1, x_2, \dots, x_k
- Bob has input y & integer $i \in \{1, 2, \dots, k\}$
& already knows x_1, x_2, \dots, x_{i-1}
- goal: compute $f(x_i, y)$

Intuition: first message sent by Alice nearly useless
if a bits $\ll k$ inputs (don't know i)

\Rightarrow should eliminate first message &
start communication protocol from second msg.

- apply to $\text{Bob} \rightarrow \text{Alice}$ direction \Rightarrow eliminate round

Round elimination lemma:

if \exists protocol for $f^{(k)}$ where Alice speaks first
using m messages & error probability δ

then \exists protocol for f where Bob speaks first
using $m-1$ messages & error probability $\delta + O(\sqrt{\frac{a}{k}})$

Intuition: if i were chosen uniformly at random
then expect a/k bits to be "about" x_i

- Bob can guess these bits randomly

$$-\Pr\{\text{correct guess}\} = 1/2^{a/k}$$

$$\Rightarrow \text{error increase} = 1 - 1/2^{a/k} \quad (\text{union bound}) \\ \approx a/k \quad (1 - \frac{1}{e^x} \approx x)$$

- correct bound is $\sqrt{a/k}$ (proof below)

Proof of predecessor lower bound:

- let $t = \#$ cell probes (rounds) for predecessor
- goal: t round eliminations
 - \Rightarrow remaining protocol has no messages
 - \Rightarrow answer must be guessed (if $n' \geq 2$)
 - $\Rightarrow \Pr\{\text{success}\} \leq 1/2$
 - get contradiction if error $< 1/2$ (t small)

① eliminate message from Alice to Bob:

- Alice's input has w' bits (initially w)
- break into $k = \Theta(at^2)$ equal-size chunks

\Rightarrow error increase will be $O(\sqrt{\frac{a}{at^2}}) = O(1/t)$

- constrain n' elements to all differ in i th chunk

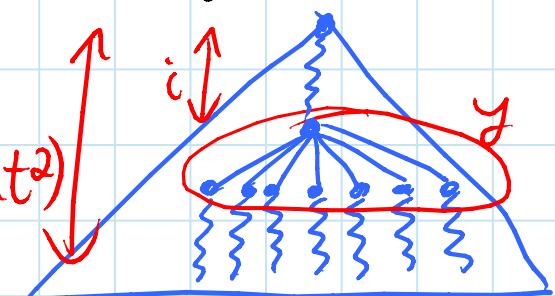
- only Bob knows i

- Bob also knows common prefix of all elements

$$(x_1, x_2, \dots, x_{i-1})$$

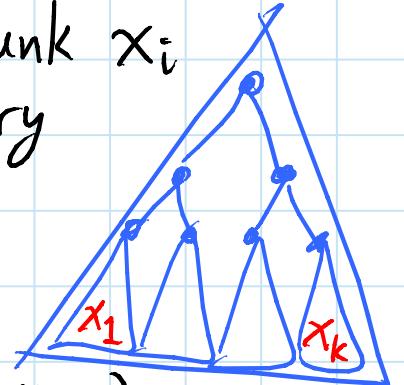
- goal: query x_i in DS y for i th chunk

\Rightarrow elimination reduces $w' \rightarrow \Theta(w'/at^2)$



ANALOGY: van Emde Boas binary searches on levels to find longest prefix match, reducing w as it goes

- ② eliminate message from Bob to Alice
- Bob's input is n' integers of w' bits each
 - divide integers into $k = \Theta(bt^2)$ equal chunks
 - \Rightarrow error increase will be $\Theta(1/t)$
 - constrain input so that i th chunk x_i starts with prefix " i " in binary
 - only Alice knows i : which x_i contains query (prefix " i ")
 - goal: search for query in x_i
 - \Rightarrow elimination reduces $n' \rightarrow \Theta(n'/bt^2)$
 $w' \rightarrow w' - \lg(bt^2) \leq \lg^2 w$
 $\geq w'/2$ if $w' \geq c \lg b = c \lg w$



ANALOGY: fusion trees branch by polynomial factor in w , reducing n

- round elimination reduces $w' \rightarrow \Theta(w'/at^2)$
 $n' \rightarrow \Theta(n'/bt^2)$
- t -round error $\leq 1/3$ if set constants right
- stop when w' hits $\lg b$ or when n' hits 2
- $\Rightarrow t = \Omega(\min\{\log_{at^2} w, \log_{bt^2} n'\})$
- because $t = O(\lg n) \& a > \lg n$ $O(a^3)$ because $O(b^3)$ because
 $t = O(\lg w) = O(\lg b)$
- $= \Omega(\min\{\log_a w, \log_b n'\})$

□

Information-theory basics:

- $H(x)$ = entropy of x

= # bits to represent x as sample from distribution

$$= \sum_{x_0} \Pr\{x=x_0\} \cdot \lg \frac{1}{\Pr\{x=x_0\}}$$

- $H(x|y)$ = entropy of x given y

= # bits to represent x if you know y

$$= \mathbb{E}_{y_0} [H(x|y=y_0)]$$

propagate into \Pr 's

- $I(x:y)$ = shared information between x & y

$$= H(x) + H(y) - H((x,y))$$

- $I(x:y|z)$ = $\mathbb{E}_{z_0} [I(x:y|z=z_0)]$

propagate into H 's

Proof sketch of round elimination lemma:

- call Alice's first message $m = m(x_1, \dots, x_k)$
- $a = |m| \geq H(m) = \sum_{i=1}^k I(x_i : m | x_1, \dots, x_{i-1})$
↑ "chain rule for information"
- if i is distributed uniformly
then $E_i[I(x_i : m | x_1, \dots, x_{i-1})] = \text{average term in sum}$
 $\leq H(m)/k \leq a/k$
- intuition: Bob knows x_1, \dots, x_{i-1} & receives m
 \Rightarrow learns $I(x_i : m)$ about x_i
- build protocol for $f(x)$ as follows:
 - fix x_1, \dots, x_{i-1} & i randomly in advance
 - now query x comes along
 - set $x_i = x$
 - run $f^{(k)}$ protocol, starting at second message,
assuming first message $m = m(x_1, \dots, x_{i-1}, \tilde{x}_i, \dots, \tilde{x}_k)$
chosen uniformly by Bob
 - guess $I(x_i : m)$ correctly with probability $\approx a/k$
 - Average Encoding Theorem:
with probability $\geq \sqrt{a/k}$,
 $\exists x_{i+1}, \dots, x_k$ such that $m(x_1, \dots, x_{i-1}, \tilde{x}_i, \dots, \tilde{x}_k)$
 $= m(x_1, \dots, x_k)$
distributed roughly the same
(\Rightarrow error probability δ preserved)