

TODAY: Predecessor lower bounds

- history/survey
- communication complexity perspective of a data structure
- round elimination
- $\Omega(\min\{\frac{\lg w}{\lg n}, \log_w n\})$ proof

(for polynomial space DS)

- information theory for round elimination lemma] very briefly covered in class

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 ~ clean
 - introduction of round elim. technique
- } citation

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

- $\forall w \exists n$ s.t. $\Omega\left(\frac{\lg w}{\lg \lg w}\right)$
 - $\forall n \exists w$ s.t. $\Omega\left(\sqrt{\frac{\lg n}{\lg \lg n}}\right)$ complicated
 - static DS achieving $O\left(\min\left\{\frac{\lg w}{\lg \lg w}, \sqrt{\frac{\lg n}{\lg \lg n}}\right\}\right)$
- \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

[Patrascu & Thorup - STOC 2006; SODA 2007]
 - tight n vs. w vs. space trade-off: (static)
 $n \cdot 2^a$

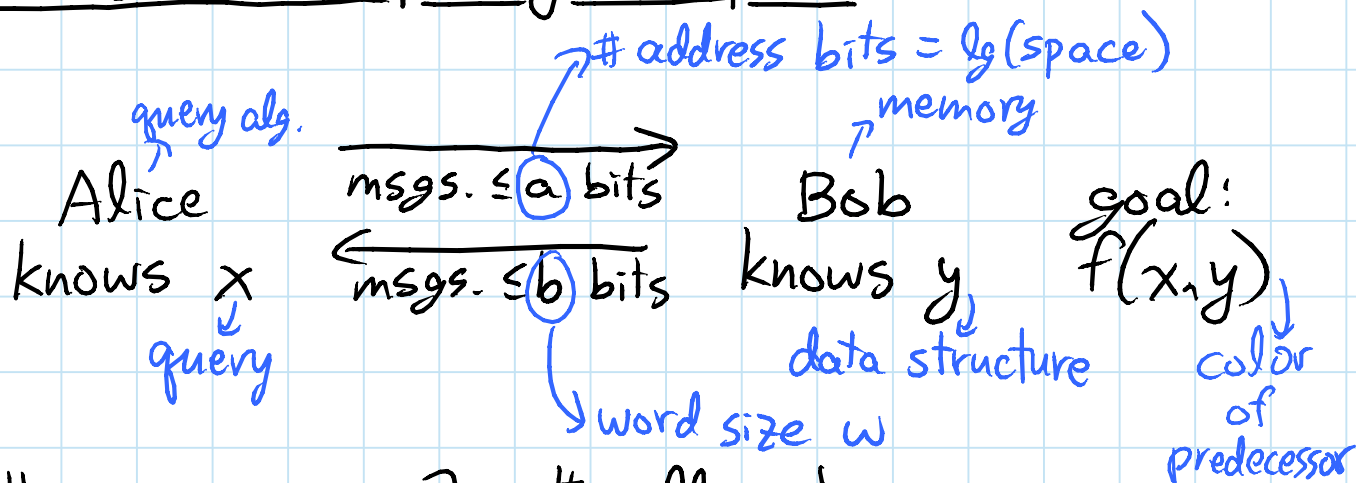
$$\Theta\left(\min\left\{\underbrace{\log_w n}_{\text{fusion}}, \underbrace{\lg\left(\frac{w - \lg n}{a}\right)}_{\text{van Emde Boas}} \rightarrow \text{see PS7}, \frac{\lg \frac{w}{a}}{\lg\left(\frac{a}{\lg n} \lg \frac{w}{a}\right)}, \frac{\lg \frac{w}{a}}{\lg\left(\lg \frac{w}{a} / \lg \frac{\lg n}{a}\right)}\right\}\right)$$

- $O(n \text{ poly} \lg n)$ space $\Rightarrow \Theta\left(\min\left\{\log_w n, \lg \frac{\lg w}{\lg \lg n}\right\}\right)$
 \Rightarrow van Emde Boas is optimal for $w = O(\text{poly} \lg n)$
 & fusion trees optimal for $\lg w = \Omega(\sqrt{\lg n} \lg \lg n)$

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 = $2 \cdot$ # cell probes

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

$\Rightarrow \Omega(\min\{\underbrace{\frac{\lg w}{\lg \lg n}}_{\approx \sqrt{EB}}, \underbrace{\log_w n}_{\text{fusion}}\})$ for $a = O(\text{poly} \lg n)$ (e.g. $\text{poly}(n)$ space)

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. $\lg^2 w = \lg n \cdot \lg \lg n \Rightarrow \lg \lg w = \lg \lg n$

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 Bob \rightarrow 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 error increase = $1 - 1/2^{a/k}$ (union bound)
 $\approx a/k$ ($1 - 1/e^x \approx x$)

- 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:

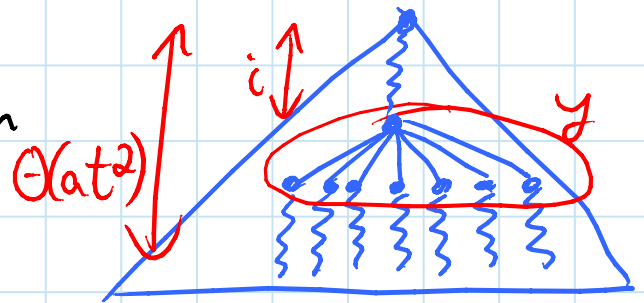
$$x_1, x_2, \dots, x_k$$

\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

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

$$= E_{y_0} [H(x|y=y_0)]$$

propagate into Pr's

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

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

- $I(x:y|z) = E_{z_0} [I(x:y|z=z_0)]$

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)

MIT OpenCourseWare
<http://ocw.mit.edu>

6.851 Advanced Data Structures
Spring 2012

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.