Proof of predecessor lower bound:

6.897
L 11.4
Mar. 10, 2005

- let t = # cell probes made by predecessor
- goal: t round eliminations
  - $\Rightarrow$ remaining protocol has 0 messages
  - $\Rightarrow$ answer must be guessed — assuming $n' \geq 2$
  - $\Rightarrow \Pr[\text{success}] \leq 1/2$ ~ use to get contradiction if t small

① eliminating message from Alice to Bob

van Emde Boas: binary search to find longest prefix match & relevant branching

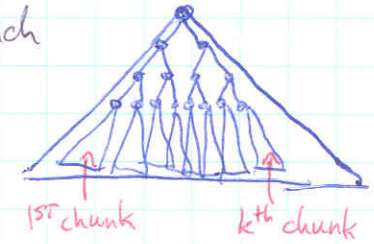
- Alice's input has w' bits (initially w)
- break into $k = \Theta(at^2)$ equal-size chunks $x_1, x_2, \ldots, x_{\Theta(at^2)}$
  - $\Rightarrow$ error increase from elimination $= O(\sqrt{\frac{a}{at^2}}) = O(1/t)$
- tell Alice & Bob that elements differ only in ith chunk but only Bob knows i
- Bob also knows $x_1, x_2, \ldots, x_{i-1}$ of query
- goal: query x_i in y DS (ith chunk)

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

② eliminating message from Bob to Alice

fusion tree: branch by polynomial factor in w, reducing n

- Bob's input is n' integers of w' bits each
- divide integers into $k = \Theta(bt^2)$ equal chunks
- tell Alice & Bob that i^{th} chunk x_i starts with prefix of "i"
- goal: search for query in ith chunk x_i containing query y
  - only Alice knows i



$\Rightarrow$ elimination reduces n' to $\Theta(n'/bt^2)$
& w' to $w' - \lg(bt^2)$ ($\leq \lg^2 w$) ← negligible ~ at most factor 2 if $w' \geq c \cdot \lg b = \lg w$

- round elimination reduces n' to $\Theta(n'/bt^2)$ & error $= O(1)$ $\leq 1/3$ if constants set right
  & w' to $\Theta(w'/at^2)$
- stop when w' hits $\lg b$ or when n' hits 2

$\Rightarrow$ lower bound of $t = \Omega(\min\{\lg_{at^2} w, \lg_{bt^2} n\})$

($at^2 = O(a^3)$ because $t = O(\lg n)$, $a \geq \lg n$; $bt^2 = O(b \lg^2 b)$ because $t = O(\lg w)$, $b = w$)

$= \Omega(\min\{\lg_a w, \lg_b n\})$.