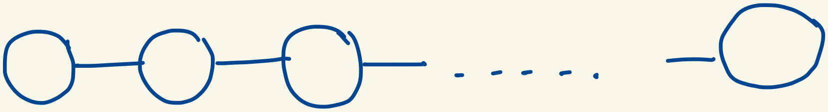
Distributed Algorithms



n computers on a path

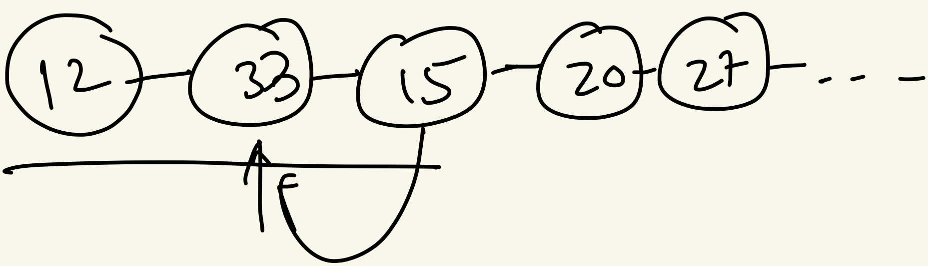
<u>Our goal</u>: color the computers with $\{1,2,3\}$

Such that no nbring pair gets the same color.

<u>Major difficulty</u>: 1) we'll need unique ID in $[1, \ldots, N]$

2) private random coins.

Coloring with unique IDs



Repeat forever

- Send message c to all nbrs.
- Receive msgs from all nbrs.
  Let M be the set received
- If $c \notin \{1,2,3\}$, & $c > \text{Max } \underline{M}$,
  let $c \leftarrow \min\{\{1,2,3\} \setminus M\}$

* Resource complexity : "round complexity"
= number of rounds needed.

* Stopping state : $c \in \{1,2,3\}$.

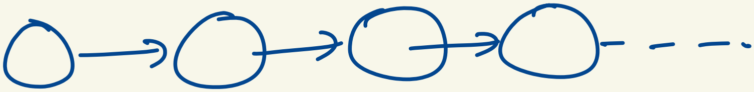
Important to know & let neighbors know that you are done.

* How fast is this algorithm?

$\longrightarrow$ round complexity: n.

Cole-Vishkin's algorithm

directed path



$$2^{128} \longrightarrow 2 \cdot 128 = 2^8$$

$$2^8 \longrightarrow 2 \cdot 8 = 2^4$$

$$2^4 \longrightarrow 2 \cdot 4 = 2^3$$

$$2^3 \longrightarrow 2 \cdot 3 = 6$$

3 more rounds ✓

7 round in total

$\underline{N = 2^{x}}$ $\longrightarrow$ $2 \cdot x = 2^{1+\log_2 x}$

$$\downarrow$$

$$2 \cdot (1 + \log_2 x)$$

<u>each node u:</u>

$C_0(u)$: current color

$C_1(u)$: current color of its successor

$$\downarrow$$

$C(u)$

*: Interpret $C_0(u)$ & $C_1(u)$ as x-bit binary strings.

$i(u) \in \{0, 1, \ldots, x-1\}$ be the index of the first bit that differs between $C_0(u)$ & $C_1(u)$.

$b(u) \in \{0, 1\}$ is the value of bit number $i(u)$ in $C_0(u)$

$$c(u) = 2 \cdot i(u) + b(u)$$

$$(\underbrace{\quad\quad\quad}_{i(u)}, b(u))$$

$u \to v \to \_$

<u>Claim:</u> Case 1:

1) $i(u) = i(v)$

In this case $b(u) \neq b(v)$ ✓

2) $i(u) \neq i(v)$: easy.

<u>Def:</u> $\log^* x$: # of times you need to take logs to reach < 2.

<u>Claim:</u> this algorithm finishes in $O(\log^* x)$ rounds.

* Fault-tolerant distributed Computation.

Feige 1999   Leader election.

1. Broadcast Model: can talk to everyone else

2. every node has access to an RNG.

3. Malicious nodes can solve any problem & can communicate secretly.

Goal: run a protocol on "good" nodes so that at stopping, all good nodes have a single agreed upon UID of a leader.

Randomized Protocol

$k \geq (\frac{1}{2}+\alpha) \cdot n$

Lemma: Suppose there are n nodes & $k > \frac{n}{2}$ are good. Then, there's a leader election protocol with success prob: $\left(\frac{1}{k}\right)^{\log k}$.

Proof: "Lightest bin" protocol

Let $B \leftarrow \{1, \ldots, n\}$

repeat:

every player broadcasts a bit.

for good players $\rightarrow$ random bit.

if $|B_0| \leq \frac{|B|}{2}$, then

$B \leftarrow B_0$.

else $B \leftarrow B_1$

if $|B|=1$, that node is the leader

Analysis:

We will use the following fact:

Fact: $c_2 \cdot \frac{1}{\sqrt{k}} \geq \binom{k}{k/2} \Big/ 2^k \geq c_1 \frac{1}{\sqrt{k}}$

for some constants c_1, c_2.

Here's one way to think about. We know that binomial coefficients add up to 2^k. $\sum_{i=0}^{k} \binom{k}{i} = 2^k$.

There are k of them. The middle coeff (for even k) is the largest of them all.

So $\binom{k}{k/2} \geq \frac{1}{k} \cdot 2^k$. Inequality above says that in fact it's $\geq 1/\sqrt{k} \cdot 2^k$.

We will prove:

Lemma:

$$\Pr[\text{algo succeeds}] \geq \left(\frac{1}{K}\right)^{\log K}.$$

Proof: (Assume k is even)

Consider the first round.

the "good" players toss exactly $\frac{k}{2}$ 0s & $\frac{k}{2}$ 1s is exactly $\binom{k}{k/2}/2^k \gtrsim \frac{c_1}{\sqrt{K}}$.

(by Fact)

Thus the lighter bin must contain at most $\frac{(n-k)}{2}$ "bad" players.

Since $k > n-k$, $\frac{k}{2} > \frac{n-k}{2}$. Thus after round 1, there's a committee of $\leq \frac{n}{2}$

players with majority of them good.

In round i, conditioned on round $1, \ldots i-1$ satisfying that each produced a committee with majority good players, with $\geq c\sqrt{\frac{2^i}{K}}$ chance, the same holds after round i.

after round 1 $K/2$ left
after round 2 $K/4$ ..
⋮
after round i $K/2^i$.

~~After~~ $\log_2(n) < \log_2(2K) = 1 + \log_2 K$ rounds, Committee must have at most 2 members.

Both must be good if all steps "succeed".

Chance of that happening:

$$\Pr[\text{round 1 succeeds} \wedge \dots \wedge \text{round } t \text{ succeeds}]$$

$$= \Pr[\text{round 1 succeeds}] \cdot \Pr[\text{round 2 succeeds} \mid \text{round 1 succeeds}] \dots$$

$$= \prod_{i=1}^{t} \Pr[\text{round } i \text{ succeeds} \mid \text{round} \leq i-1 \text{ succeeds}]$$

$$\geq \left[c_1 \left(\frac{1}{\sqrt{K}}\right)\right]^{1+\log_2 K} \gtrsim C \left(\frac{1}{K}\right)^{\log K}.$$

some constant

$\square$