LECTURE 11 — 10/12/2020

MAXIMAL INDEPENDENT SET ON PRAM – DERANDOMIZATION

RANDOMIZED ALGORITHM

PARAL – MAXIMAL IS

1. $I := \emptyset$; $V' := V$; $G' := G$
2. while $(V' \neq \emptyset)$ do
3. in parallel (for $\forall v \in V'$: if $d_v = 0$, then $I := I \cup \{v\}$; $V' := V' \setminus \{v\}$)

RANDOM STEP

4. ⇒ in parallel for $\forall v \in V'$ mark v with prob $\frac{1}{2d_v}$ (independently for different vertices & iterations)
5. → in parallel for $\forall \{u,v\} \in E(G')$: if both u, v marked, then unmark the lower degree vertex of u, v (break ties arbitrarily) – e.g. unmark the lower
   let S be the set of marked vertices and $N(S)$ be their neighbours
6. $I := I \cup S$; $V' := V' \setminus (S \cup N(S))$; $G' := G[V']$ induced by V'
7. OUTPUT I

independence of the random choices was needed only in the proof of:

Lemma 2: A good vertex v with $d_v > 0$ has marked neighbour with probability $> (1 - e^{-1/6}) =: \alpha$.

Recall: fix a vertex v: let $L(v) = \{w \in N(v) \mid d(w) \leq d(v)\}$

the probability that no $w \in L(v)$ is marked

is $\leq \prod_{w \in L(v)} \left(1 - \frac{1}{2d(v)}\right) = \cdots \leq e^{-\frac{1}{6}}$

↑ independent random choices

HALFWAY GOAL:

use pairwise independent random choices in step 4

Def: Random variables $X_1, \dots, X_n$ are **pairwise independent** if for all $i \neq j$ and any values a, b:

$$\Pr[X_i = a, X_j = b] = \Pr[X_i = a] \cdot \Pr[X_j = b].$$

Lemma: Let X_i, $1 \le i \le n$ be $\{0,1\}$ random variables and $p_i := \Pr[X_i = 1]$. If X_i's are pairwise independent then $\Pr\left[\sum_{i=1}^{n} X_i > 0\right] \ge \frac{1}{2} \min\left\{\frac{1}{2}, \sum_{i=1}^{n} p_i\right\}$.

(In our setting: $|L(v)| \ge \frac{d_v}{3}$ ...

fix a good vertex v, $L(v) = \{w \in N(v) \mid d_w \le d_v\}$

for $w \in L(v)$ --- $X_w = 1$ with prob. $p_w = \frac{1}{2d_w} \ge \frac{1}{2d_v}$

note: $\sum_{w \in L(v)} p_w \ge \frac{1}{2d_v} \cdot \frac{d_v}{3} = \frac{1}{6}$

$$\Pr[\exists w \in L(v) \text{ that is marked}] = \Pr\left[\sum_{w \in L(v)} X_w > 0\right] \overset{\text{Lemma}}{\ge} \frac{1}{2} \cdot \frac{1}{6} = \frac{1}{12}$$

Proof Lemma:

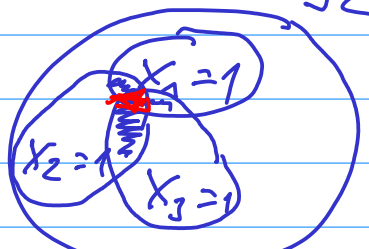
if $\sum_{i=1}^{n} p_i > 1$ then let $S \subseteq \{1, \dots, n\}$ s.t.

$$\frac{1}{2} \le \sum_{i \in S} p_i \le 1 \quad \text{(clearly exists)}$$

otherwise $S = \{1, \dots, n\}$

$$\Pr\left[\sum_{i=1}^{n} X_i > 0\right] \ge \Pr\left[\sum_{i \in S} X_i > 0\right] \ge \Pr\left[\sum_{i \in S} X_i = 1\right] \ge$$

$$\ge \sum_{i \in S} \Pr[X_i = 1] - \sum_{\substack{i<j, \\ i,j \in S}} \Pr[X_i = 1, X_j = 1]$$



pairwise ind.

$$= \sum_{i \in S} p_i - \frac{1}{2} \sum_{\substack{i \ne j, \\ i,j \in S}} p_i \cdot p_j$$

$$\ge \sum_{i \in S} p_i - \frac{1}{2}\left(\sum_{i \in S} p_i\right)^2 = \left(\sum_{i \in S} p_i\right)\underbrace{\left(1 - \frac{1}{2}\sum_{i \in S} p_i\right)}_{\ge \frac{1}{2}} \ge \frac{1}{2}\sum_{i \in S} p_i \ge$$

$$\ge \frac{1}{2} \min\left\{\frac{1}{2}, \sum_{i=1}^{n} p_i\right\}$$

∎

HOW TO GET PAIRWISE INDEP. BITS

Def: Random bit X is uniform if $\Pr[X=1] = \Pr[X=0] = \frac{1}{2}$

How to generate $2^b - 1$ uniform pairwise independent bits from b independent uniform random bits

$\underbrace{X_1, X_2, \ldots, X_b}_{b \text{ bits}}$

Note: if poly(n) pairwise independent bits needed
.... it is sufficient to have $O(\log(n))$ random bits
→ it's possible to try all possibilities of these
(i.e. ~ poly(n) possibilities)

Enumerate all non-empty subsets of $\{1, 2, \ldots, b\}$ in some order,
let S_j be the jth subset .... note: $2^b - 1$ of these

Define: $\boxed{Y_j = \left(\sum_{i \in S_j} X_i\right) \bmod 2}$ --- parity of $\sum_{i \in S_j} X_i$

Lemma: The Y_j's are uniform pairwise independent bits.

Proof: • Y_j is uniform rand. bit

S_j: $1 \quad \ell \quad b = z$

Let z be the largest index of an element in S_j

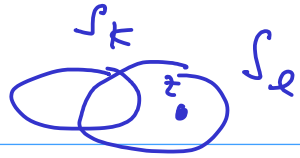
Then $Y_j = \left(\left(\sum_{i \in S_j \cdot [z]} X_i\right) \bmod 2 + X_z\right) \bmod 2$

$= a$

Note: whatever the value of a is (i.e., 0 or 1)

$\Pr[Y_j = 1] = \Pr[Y_j = 0] = \frac{1}{2}$

since X_z determines the value of Y_j, and X_z is independent on X_i, $i \in S_j \cdot [z]$, and uniform



$k \neq \ell$

- Y_k, Y_ℓ ~~~ S_k, S_ℓ, w.l.o.g. $\exists\, z \in S_\ell \setminus S_k$

for any values $c, d \in \{0,1\}$ consider the conditional probability
$\Pr[Y_\ell = c \mid Y_k = d]$ (goal: $= \frac{1}{2}$)
suppose that X_i are revealed for all $i \in (S_k \cup S_\ell) \setminus \{z\}$
then Y_k determined but Y_ℓ not yet!
conditioning on the value Y_k does not affect Y_ℓ
--- Y_ℓ is equally likely to be 0 and 1 ✓

$$\Pr[Y_\ell = c, Y_k = d] = \underbrace{\Pr[Y_\ell = c \mid Y_k = d]}_{= \frac{1}{2}} \cdot \underbrace{\Pr[Y_k = d]}_{= \frac{1}{2} \text{ as } Y_k \text{ is uniform}} = \frac{1}{4}$$

HASHING

... $O(1)$

- randomization used to obtain efficient data structures

Problem: given a set S of items, we want to store them so that we can do efficiently

- lookups FIND
- insertions INSERT
- deletions DELETE

} static dictionary
} dynamic dictionary

The dictionary can be implemented, e.g. balanced trees, the static dict ... array ...
$\Omega(\log n)$

Setup:
- large universe $U = \{0, 1, \ldots, m-1\}$
- $S \subseteq U$, $|S| \ll |U|$ ~ space
- a family of hash functions $h: U \to \{0, 1, \ldots, n-1\}$
- a collision: a situation when $h(x) = h(y)$ for $x \neq y \in S$

Desired properties:

- not too many collisions
- $n = O(|S|)$ ... space efficient
- the function h is fast to compute

Basic intuition

- spread the element randomly

  however: to be able to access them efficiently, can't do it completely randomly

Def: A family of hash functions $\mathcal{H}$ for U to $\{0,\dots,n-1\}$ ($=V$)

- is **2-universal** if for any $x, y \in U$, $x \neq y$ and a hash function $h \in \mathcal{H}$ chosen uniformly at random, we have $\Pr[h(x) = h(y)] \leq \frac{1}{n}$.
- is **strongly 2-universal** if for any $x, y \in U$, $x \neq y$, and any values $a, b \in V$, and a hash function $h \in \mathcal{H}$ chosen uniformly at random we have

$$\Pr[h(x) = a \wedge h(y) = b] = \frac{1}{n^2}.$$

Example: $U = \{0, 1, \dots, m-1\}$, $V = \{0, 1, \dots, n-1\}$, $m \geq n$

choose a prime $p \geq m$

define $h_{a,b}(x) = ((a \cdot x + b) \bmod p) \bmod n$

$$\mathcal{H} = \{h_{a,b} \mid 1 \leq a \leq p-1,\ 0 \leq b \leq p\}$$

Lemma: $\mathcal{H}$ is 2-universal.

Proof: consider $x_1, x_2 \in U$, $x_1 \neq x_2$ ← fix

count: $|\{h \in \mathcal{H} \mid h(x_1) = h(x_2)\}|$

☺: $\forall\ a x_1 + b \not\equiv a x_2 + b \bmod p$

proof: by contradiction: $a x_1 + b \equiv a x_2 + b \bmod p$

$$\Rightarrow a(x_1 - x_2) \equiv 0 \bmod p$$

but p is a prime, $x_1 \neq x_2$, $a \neq 0$ ↯ □