2023 - March - 5 PSRG

short random seed → long pseudo-random sequence

Why?

1. So can re-run and check.
2. Random bits are rare
3. Interesting to understand how much randomness we need.

Today. Randomized algorithms that can make errors, both positive and negative.
Hypothesis testing. Or, is volume of $\{x : Ax \le b\} \le 1$?

To boost accuracy, run many times and take majority vote

Assume have alg A takes input x and random bits r. To answer yes/no question P.

And, is correct ≥ 99% of the time $\Pr_{r \in \{0,1\}^n} [A(x,r) = P(x)] \ge 0.99$

To improve accuracy, run k times on $r_1, \dots, r_k$, output majority answer.

Will show can do this well with $n + 9k$ bits. (can get $9 \to 1$)

Fix problem to solve, x, view random bits as input.

Let $X = \{r \in \{0,1\}^n$ on which $A(x,r) \neq P(x)\}$ - wrong $\qquad |X| \leq \frac{1}{100} 2^n$

$Y = \{r \in \{0,1\}^n$ s.t. $A(x,r) = P(x)\}$ - correct $\qquad |Y| \geq \frac{99}{100} 2^n$

To run $k+1$ times, generate $r_0, r_1, \dots, r_k \in \{0,1\}^n$

Want $\Pr[\text{most } r_i \in X] \leq \varepsilon^{k+1}$

naive: need $(k+1)n$ bits

we will do with $n+9k$ bits,
for $\varepsilon = 2/\sqrt{5} < 1$

Can improve a lot!
Is a huge field.

Let G be a d-regular $\frac{1}{10}$-expander with vertex set $V = \{0,1\}^n$

Too big to write down.

$\Rightarrow$ adjacency eigenvalues $\mu_1 = d$, $\mu_2 \leq \frac{d}{10}$, $\mu_n \geq -\frac{d}{10}$

Ramanujan bound says $d \sim 400$, $\qquad \frac{2\sqrt{d-1}}{d} \leq \frac{40}{400} = \frac{1}{10}$

Pick $r_0 \in V$ uniformly at random. Needs n bits

For $i \leq k$, pick r_i to be random neighbor of r_{i-1} : need $\lg_2 d \leq 9$ bits.

Random walk on G of length k.

Will prove $\Pr[\text{rand walk in } X \text{ most of } k+1 \text{ steps}] \leq \left(\frac{2}{\sqrt{5}}\right)^{k+1}$

Lem 1 For $S \subseteq \{0, \dots k\}$. $\Pr[S = \{i : r_i \in X\}] \le \left(\frac{1}{5}\right)^{|S|}$

proof of theorem $\Pr[\text{walk in } X \text{ most steps}] = \sum_{|S| > \frac{k}{2}} \Pr[S = \{i : r_i \in X\}] \le \sum_{|S| > \frac{k}{2}} \left(\frac{1}{5}\right)^{\frac{k+1}{2}} \le 2^{k+1} \left(\frac{1}{5}\right)^{\frac{k+1}{2}} = \left(\frac{2}{\sqrt{5}}\right)^{k+1}$

Let $W = MD^{-1}$, $|\omega_i| \le \frac{1}{10}$ for $i \ge 2$. $D_X = \text{diag}(\mathbb{1}_X)$ $D_Y = \text{diag}(\mathbb{1}_Y)$

Fix S. Let $D_i = \begin{cases} D_X & i \in S \\ D_Y & i \notin S \end{cases}$

claim $\Pr[\{i : r_i \in X\} = S] = \mathbb{1}^T D_k W D_{k-1} W \cdots W D_1 W D_0 \frac{\mathbb{1}}{n}$ $(*)$

Why? Initial distribution is $\frac{\mathbb{1}}{n} = p_0$. $(D_X p_0)(a) =$ prob walk starts at a and $a \in X$

$(W D_X p_0)(a) =$ prob walk started in X and moved to a

$(D_Y W D_X p_0)(a) =$ prob walk starts in X, moves to a, and $a \in Y$ etc.

To bound $(*)$, recall $\|M\| = \max_x \frac{\|Mx\|}{\|x\|}$ so $\|M_1 M_2\| \le \|M_1\| \cdot \|M_2\|$

Lem 2 $\| D_k W D_{k-1} W \cdots W D_1 W D_0 W \| \le \left(\frac{1}{5}\right)^{|S|}$

proof of lem 1 $W\mathbb{1} = \mathbb{1}$. $\mathbb{1}^T (D_k W \cdots W D_0 W) \mathbb{1}/n \le \left(\frac{1}{5}\right)^{|S|} \frac{\|\mathbb{1}\|^2}{n} = \left(\frac{1}{5}\right)^{|S|}$

proof of lem.2 i. $\|W\| = 1$. W is symmetric, so $\|W\| = \omega_1 = 1$

ii. $\|D_y\| = 1$, because is 0/1 diagonal. So $\|D_y W\| \leq 1$.

iii $\|D_x W\| \leq \frac{1}{5}$. Will prove $\forall z$, $\|D_x W z\| \leq \frac{\|z\|}{5}$. Let $z = c\mathbb{1} + y$, where $\mathbb{1}^T y = 0$

$D_x W \mathbb{1} = D_x \mathbb{1} = \mathbb{1}_x$. $\|\mathbb{1}_x\| \leq \sqrt{\frac{n}{100}} = \frac{\sqrt{n}}{10}$. $\|Wy\| \leq \|y\| \cdot \max(\omega_2, |\omega_n|) \leq \frac{\|y\|}{10}$

$\rightarrow \|D_x W z\| \leq \|D_x W c\mathbb{1}\| + \|D_x W y\| \leq \frac{c\sqrt{n}}{10} + \frac{\|y\|}{10} \leq \frac{1}{10}(c\sqrt{n} + \|y\|) \leq \frac{2}{10}\|z\| = \frac{1}{5}\|z\|$

because $\|z\|^2 = c^2 + \|y\|^2 \geq c^2, \|y\|^2$