PSRGs

Why?

1. Random bits are sort of rare.
2. So can re-run algorithm.
3. Analyzable - understand how much randomness is necessary.

examples: eigenvector/value computation.
primality testing

How?

Good enough - standard in most languages.

example: random d-regular is expander.
But Klawe proved need good psrg.

Cryptographic

* For specific sorts of algorithms.

Today: re-running an algorithm to boost confidence.

Say is right 99% of the time, but want more.
(maybe outputs yes/no)

Re-run, use majority answer

Fix input, and now view random bits $r \in \{0,1\}^n$ as input

Or, view as repeating an experiment
input $r \in \{0,1\}^n$, and output will be correct 99% of the time.

$X = \{ r \in \{0,1\}^n$ on which wrong$\}$ $\quad |X| \le \frac{2^n}{100}$

$Y = \{0,1\}^n - X$. $\quad |Y| \ge \frac{99}{100} 2^n$

To run k times, will generate $r_0, r_1, r_2, \ldots, r_k$ each in $\{0,1\}^n$.

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

Naive approach: use $n(k+1)$ bits.

Today: only need $n + 9k$ bits, for $\varepsilon = \frac{2}{\sqrt{5}}$

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

Recall $\Rightarrow$ all eigvals of adjacency $\le \frac{d}{10}$

For $\omega_1, \omega_2, \ldots, \omega_n$ eigvals of $W = MD^{-1}$

satisfy $|\omega_i| \le \frac{1}{10}$, $i \ge 2$

Can find with $d = 400$, $\log_2 d \le 9$, is why 9 bits.

Choose r_0 uniform in $\{0,1\}^n$.

For each i, let r_i be random neighbor of r_{i-1}.

Use random walk.

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

To write using matrices,

$$D_X = \text{diagonal}(1_X) \qquad D_Y = \text{diagonal}(1_Y)$$

Let $S \subseteq \{0, \dots, k\}$

$\Pr[\, r_i \in X \text{ for } i \in S \text{ and } r_i \in Y \text{ for } i \notin S \,]$ $(*)$

will prove $\leq \left(\frac{1}{5}\right)^{|S|}$

So, $\Pr[\text{walk in } X \text{ most steps}]$

$$\leq \sum_{|S| > \frac{k}{2}} \left(\tfrac{1}{5}\right)^{|S|} \leq \sum_{|S| > \frac{k}{2}} \left(\frac{1}{5}\right)^{(k+1)/2} \leq 2^{k+1} \left(\frac{1}{5}\right)^{\frac{k+1}{2}} = \left(\frac{2}{\sqrt{5}}\right)^{k+1}$$

Define $D_i = D_X \quad i \in S$
$ = D_Y \quad i \notin S$

$$(*) = 1^T D_k W_k \cdots W D_1 W D_0 =$$
$$1^T D_k W_k \cdots W D_1 W D_0 W \tfrac{1}{n}$$

To bound this, use matrix norms.

Recall $\|M\| = \max_x \frac{\|Mx\|}{\|x\|}$

Note $\|M_1 M_2\| \leq \|M_1\| \cdot \|M_2\|$

And, for symmetric M, $\|M\| =$ max abs eigval.

<u>Claim 1</u> $\|D_Y W\| \le 1$

proof $\|W\| = 1$, $\|D_Y\| = 1$, so $\|D_Y W\| \le 1$

Will prove claim 2: $\|D_X W\| \le \frac{1}{5}$

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

$$\Rightarrow \quad \| D_k W \cdots D_0 W \cdot \frac{\mathbb{1}}{n} \| \le \left(\frac{1}{5}\right)^{|S|} \cdot \| \frac{\mathbb{1}}{n} \|$$

$$= \left(\frac{1}{5}\right)^{|S|} \cdot \frac{1}{\sqrt{n}}$$

and $\mathbb{1}^T D_k W \cdots D_0 W \cdot \frac{\mathbb{1}}{n} \le \left(\frac{1}{5}\right)^{|S|} \cdot \frac{1}{\sqrt{n}} \cdot \|\mathbb{1}\| = \left(\frac{1}{5}\right)^{|S|}$

Proof of claim 2:

$\|D_X W\| \le \frac{1}{5}$. Will prove for all z,

$$\|D_X W z\| \le \frac{\|z\|}{5}.$$

let $z = c\mathbb{1} + y$, where $\mathbb{1}^T y = 0$.

$D_X W \mathbb{1} = D_X \mathbb{1} = 1_X$, $\quad \|1_X\| \le \sqrt{\frac{n}{100}} = \frac{\sqrt{n}}{10}$

As $\mathbb{1}^T y = 0$, $\|Wy\| \leq \|y\| \cdot \max(\omega_2, |\omega_n|) \leq \frac{\|y\|}{10}$

So, $\|D_x W z\| \leq \|D_x W c \mathbb{1}\| + \|D_x W y\|$

$$\leq \frac{c\sqrt{n}}{10} + \frac{1}{10}\|y\|$$

$$= \frac{1}{10}\|c\mathbb{1}\| + \frac{1}{10}\|y\|$$

$$\leq \frac{2}{10}\|z\| \quad \text{because } \|c\mathbb{1}\| \leq \|z\|, \ \|y\| \leq \|z\|$$

Note: very odd, because used 2-norms for probabilities

Note: for asymmetric, norm has little to do with eigenvalues.

Generalized Hypercube.

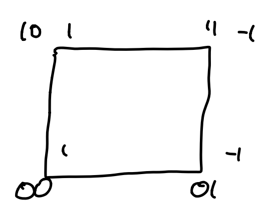
$V = \{0,1\}^d$ mod 2. $(a,b) \in E$ if $b = a + \delta_i$ mod 2

1 in pos i.

From product theorem,

have eigenvectors for each $c \in \{0,1\}^d$

$\psi_c(a) \triangleq (-1)^{c^T a}$ eg.



$c = 01$

Generalized. Pick $g_1, \ldots, g_k \in \{0,1\}^d$, $k > d$

edges are $(a, a+g_i) \bmod 2 \quad 1 \le i \le k$

Claim: has same eigenvectors.

<u>Lem</u> For $c \in \{0,1\}^d$, ψ_c is an eigvec of M with eigval

$$\sum_{i=1}^{k} (-1)^{c^T g_i}$$

First $\psi_c(a+b) = (-1)^{c^T(a+b)} = (-1)^{c^T a} (-1)^{c^T b} = \psi_c(a)\, \psi_c(b)$

For any vertex a, compute

$$(M\psi_c)(a) = \sum_{i=1}^{k} \psi_c(a+g_i)$$

$$= \sum_{i=1}^{k} \psi_c(a)\, \psi_c(g_i)$$

$$= \sum_{i=1}^{k} \psi_c(g_i)$$

$$= \sum_{i=1}^{k} (-1)^{c^T g_i}$$

need all these small...