Reducing Randomness Via Random Walks on special graphs
Reducing Randomness

For decision problem $L$,

Let $A$ be algorithm st. 1) $\forall x \in L \quad \Pr [A(x) = 1] = 0.99$

2) $\forall x \notin L \quad \Pr [A(x) = 0] = 1$

To get error $< 2^{-k}$:

**Method:**

1) run $k$ times output "yes" if ever see "yes"

2) use p.i. random bits

3) today: use random walk on graph to choose random bits

# random bits used

$O(kr)$

$O(k+r)$

$r + O(k)$

Plan:

- associate all (random) strings in $\{0,1\}^n$ with nodes of a graph $G$

- problem of picking a random string is now equivalent to problem of picking a random node

picking several random strings $\Rightarrow$ picking several nodes

picking several strings, one of which is "good" $\Rightarrow$ picking several nodes, one of which is "good"

*easier?*
The graph \( G \):

- Constant degree \( d \)-regular, connected, nonbipartite

- Transition matrix \( P \) for r.w. on \( G \) has \( |\lambda_2| \leq \frac{1}{10} \)

- Stationary distribution \( \pi \) uniform since \( d \)-reg

- \# nodes = \( 2^r \) \( \sim \) \( r \) random bits

The Algorithm:

- Pick random start node \( w \in \mathbb{S}^{Q, \mathbb{R}}^r \)

- Repeat \( \mathbb{K} \) times:
  
  \( w \leftarrow \) random neighbor of \( w \)
  
  Run \( A(x) \) with \( w \) as random bits
  
  If \( A(x) \) outputs "X\&L", then output "X\&L"; halt.
  
  Else continue.

- Output "X\&L"

Claim: error of new algorithm \( \leq \left(\frac{1}{5}\right)^k \) for X\&L

(0-error for X\&L)
The idea:

very unlikely to get good after 2 steps

pick a start location
that is bad after k steps.
Behavior:

bad case - walk only on "bad" random strings
+ never get out to "good" random strings

why would this not work on arbitrary \( G \)?

\( \{ \text{e.g. } G = \text{lune} \} \)

if \( x \notin L \):
algorithm never errs (there are no bad strings)

if \( x \in L \):
most random bits say \( x \in L \); \( \geq \frac{99}{100} . 2^r \)

\[ |B| \leq \frac{2^r}{100} \]

Want linear algebraic way of describing walks that stay in bad set:

define \( N \) diagonal matrix such that

\[ Nw = \begin{cases} 1 & \text{if } w \in B \rightarrow \text{incorrect} \\ 0 & \text{else} \end{cases} \]

\[
N = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ 0 & 0 & 0 & 0 & 1 & \cdots \\
0 & 0 & 0 & 0 & 0 & \cdots \\
\end{pmatrix}
\]
For any probability distribution, \( q^N \) is

\[ \|q^N\|_1 = \operatorname{Pr}_{w \sim q} \left[ w \text{ is bad} \right] \]

ie. \( q^N \) deletes weight that finds a witness to \( x \in L \)

Can compose:

\[ \|q \cdot PN\|_1 = \operatorname{Pr}_{w \sim q} \left[ \text{start at } q, \text{ take a step \& land on "bad"} \right] \]

\[ \|q \cdot (PN)^k\|_1 = \operatorname{Pr}_{w \sim q} \left[ \text{start at } q, \text{ take } k \text{ steps \& each is "bad"} \right] \]

Lemma

\[ \forall T \quad \|TPN\|_2 \leq \frac{1}{5} \|T\|_2 \]

First: How do we use the lemma?

If always see bad \( w \)'s, then answer incorrect

\[ \operatorname{Pr} \left[ \text{incorrect} \right] \leq \|p_0 \cdot (PN)^k\|_2 \]

\[ \leq \sqrt{2^k} \|p_0 \cdot (PN)^k\|_2 \]

\[ \leq \sqrt{2^k} \cdot \|p_0\|_2 \left( \frac{1}{5} \right)^k \]

\[ \leq \sqrt{2^k} \cdot \frac{1}{5^k} \]

\[ \leq \left( \frac{1}{5} \right)^k \]

since start at uniform + \( l_2 \) norm of uniform = \( \sqrt{\frac{1}{\sqrt{2^n}}} \)
Proof of lemma. Let \( V_1 - V_{ar} \) be e-vects of \( P_j \), \( j \) be such, \( \| V_i \|_2 = 1 \)

Note: \( V_i = (\frac{1}{\| \omega \|_2}, \ldots, \frac{1}{\| \omega \|_2}) \)

Then \( \Pi = \sum_{i=1}^{2^n} \alpha_i \lambda_i V_i \)

Note:
1) \( \| \Pi \|_2 = \sqrt{\sum_i \alpha^2_i} \) (from before)
2) \( \forall \omega \quad \| w N \|_2 = \sqrt{\sum_{i \in B} \omega_i^2} \leq \sqrt{\sum_{i \in A} \omega_i^2} = \| \omega \|_2 \)

So:
\[
\| \Pi P N \|_2 = \| \sum_{i=1}^{2^n} \alpha_i \lambda_i V_i \Pi N \|_2
\]
\[
= \| \sum_{i=1}^{2^n} \alpha_i \lambda_i \lambda_i V_i N \|_2
\]
\[
\leq \| \alpha \lambda_i V_i N \|_2 + \| \sum_{i=2}^{2^n} \alpha_i \lambda_i V_i N \|_2 \]

(A) Cauchy-Schwarz

(B) bunding:
\[
\alpha \lambda_i V_i N \|_2 = \| \alpha \lambda_i V_i N \|_2
\]
since \( \lambda_i = 1 \)
\[
= \alpha \lambda_i \sqrt{\sum_{i \in B} (\lambda_i \omega_i)^2}
\]
since \( V_i = (\frac{1}{\| \omega \|_2}, \ldots, \frac{1}{\| \omega \|_2}) \)
\[
= \alpha \lambda_i \sqrt{\sum_{i=2}^{2^n} (\lambda_i \omega_i)^2}
\]
since \( \frac{\| B \|}{\| \omega \|_2^2} \leq \frac{1}{100} \)
\[
\leq \| \Pi \Pi N \|_2 = \sqrt{\sum_i \lambda_i^2}
\]
since \( \Pi \Pi N \|_2 = \sqrt{\sum \lambda_i^2} \)
Bonding

\[ \| \sum_{i=2}^{2^n} \alpha_i \lambda_i v_i N \|_2 \leq \| \sum_{i=2}^{2^n} \alpha_i \lambda_i v_i v_i^T \|_2 \]

= \sqrt{\sum (\alpha_i \lambda_i)^2}

\leq \sqrt{\sum \alpha_i^2 (\lambda_i)^2}

\leq \frac{1}{10} \| \Pi \Pi \|_2

\lambda_i \leq \frac{1}{10}

So:

\[ \| \Pi P N \|_2 \leq \| \Pi \Pi \|_2 \frac{1}{5} \]