

Reducing randomness
w/ random walks

Probability (and techniques)

Algorithms (models and applications)

Random Walks

Stationary Distribution

Perron-Frobenius Theorem

Pagerank

Probability (and techniques)

Algorithms (models and applications)

Hitting times

Cover times

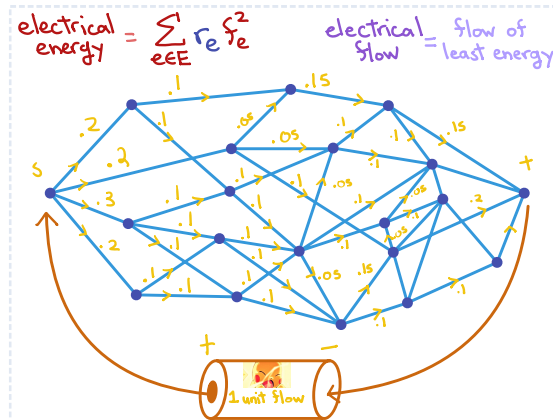
Electrical networks

Connectivity
in $O(\log n)$ space

random walk terminology:

Hitting time $H(s, t)$ = expected # steps until a random walk from s reaches t

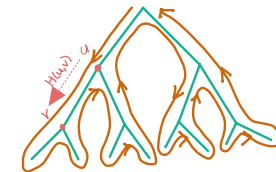
Cover time $C(s)$ = expected # steps until a random walk from s visits every vertex



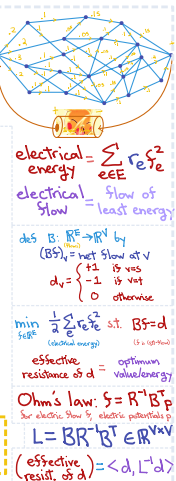
Lemma $H(u, v) + H(v, u) = 2m \cdot (\text{energy of unit flow } (u, v))$

Theorem $C(s) \leq 2mn$

proof Six traversal of spanning tree



$$\begin{aligned} \text{total time} &= \sum_{u, v \in V} H(u, v) + H(v, u) \\ &= 2m \sum_{u, v \in V} (\text{energy of unit flow } (u, v)) \leq 2m(n-1) \end{aligned}$$



Probability (and techniques)

Algorithms (models and applications)

Spectral theorem
for symmetric maps

Spectral analysis of
random walks

Probability

(and techniques)

Conductance

Cheeger's inequality

Conductance-based
mixing time

Algorithms

(models and
applications)

Fiedler's algorithm
for low-conductance
cuts

Probability (and techniques)

Algorithms (models and applications)

Expanders

Zigzag product

tensors

Deterministic

Connectivity in

$O(\log n)$ space

Expander graphs

G is an expander if the spectral gap γ is at least a constant

Theorem, restated: let G be a dir. graph and R the random walk linear map. Then R has an eigenvector $x \in \Delta^V$ w/ eigenvalue 1. If G is strongly connected, then x is the unique eigenvector w/ eigenvalue 1

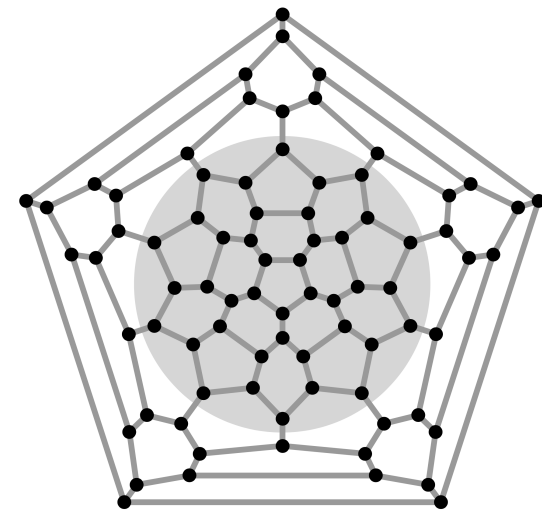
Theorem: $G=(V,E)$ undirected, $w:E \rightarrow \mathbb{R}_{>0}$
let $R: \mathbb{R}^V \rightarrow \mathbb{R}^V$ be random walk map
then R has stationary distr. $s \in \Delta_V$ w/
 $s_v = \frac{\deg(v)}{2W}$ $\deg(v) = \sum_{e \in \mathcal{E}(v)} w(e)$
 $W = \sum_{e \in E} w(e)$

Theorem. let $\gamma = 1 - \max\{\mu_2, |\mu_n|\}$
 $\|R^k x - s\| \leq (1-\gamma)^k \sqrt{\frac{\Delta_{\max}}{\Delta_{\min}}}$
stationary distribution
 $1 \geq \mu_2 \geq \dots \geq \mu_n = \text{eigenvalues of } R$

Q: deterministic connectivity for constant-degree expanders?

- Diameter $O(\log n)$
- $O(1)$ random bits per random step

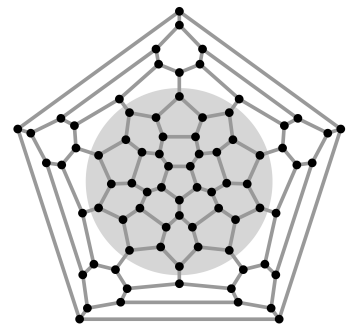
$\Rightarrow$ enumerate all paths of length $O(\log n)$!



Theorem: $O(\log n)$ space, poly-time [Reingold, 2005]
deterministic connectivity in undirected graphs.

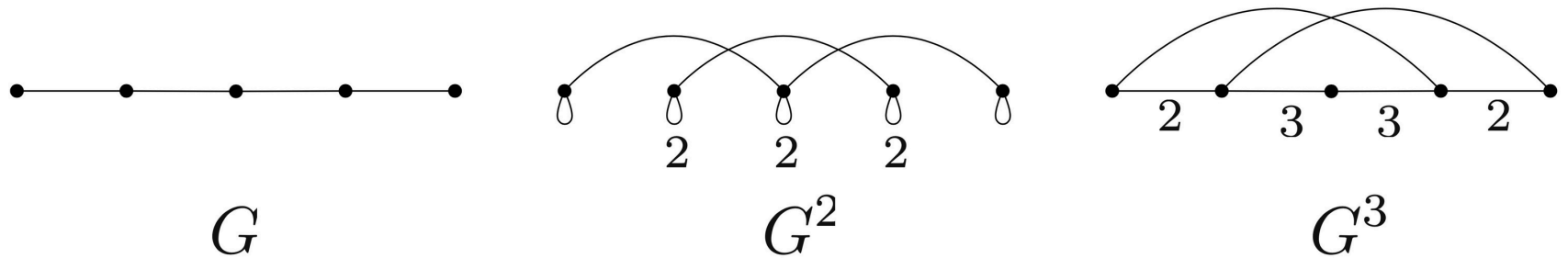
High level idea:

- convert G into $O(1)$ -degree expander
by sequence of "graph transformations"
(graph transformations applied implicitly due to space constraints)
- derandomize the random walk
algo (implicitly) on the expander



Lemma: $O(\log n)$ space, poly-time
deterministic connectivity in
 $O(1)$ -degree expanders

Powering



$G^k =$ graph w/ an edge for every k step walk in G
(w/ repetition)

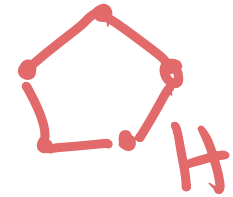
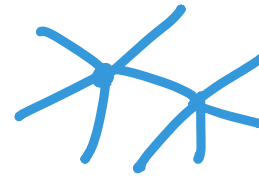
random walk R^k has eigenvalues $1, \mu_2^k, \dots, \mu_n^k$

$$\delta(G^k) = 1 - (1 - \delta(G))^k \quad \text{😊}$$

degree increases from d to d^k 😞

Zig-zag product $Z(G, H)$

let G be d -regular

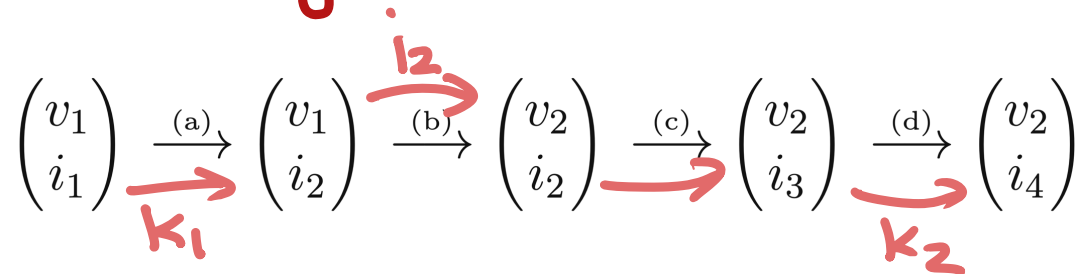


H be d_0 -regular w/ d_0 vertices (H will be $O(D)$ -degree expander)

vertices: $V_G \times V_H = \{(u, v) : u \in V_G, v \in V_H\}$

edges: for $(v_1, i_1) \in V_G \times V_H$, $k_1, k_2 \in [d_0]$:

the (k_1, k_2) th neighbor of (v_1, i_1) is (v_2, i_4) where:



where:

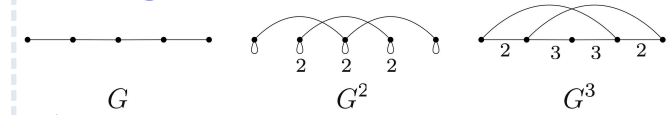
- (a) is a step in H from i_1 to its k_1 th neighbor, i_2 .
- (b) moves v_1 to the i_2 th outgoing neighbor of v_1 , v_2 .
- (c) moves from i_2 to i_3 where v_1 is the i_3 th neighbor of v_2 .
- (d) moves i_3 to its k_2 th neighbor in H .

(so $Z(G, H)$ is d_0^2 -regular)

	G^k	$Z(G, H)$
vertices	n	nd
degree	d^k	d_0^2
spectral gap	$1 - (1 - \gamma_G)^k$	$\gamma_G \gamma_H^2$

	$Z(G^2, H)$
vertices	nd
degree	d_0^2
spectral gap	$(1 - (1 - \gamma_G^2)) \gamma_H^2 = (2\gamma_G - \gamma_G^2) \cdot \gamma_H^2$

Powering



G^k = graph w/ edge for every k step walk in G
(w/ repetition)

random walk R^k has eigenvalues $1, \mu_1^k, \dots, \mu_n^k$

$$\gamma(G^k) = 1 - (1 - \gamma(G))^k \quad \text{😊}$$

degree increases from d to d^k 😞

Zig-zag product $Z(G, H)$

let G be d -regular

H be d_0 -regular w/ d vertices (H will be $O(d)$ -degree expander)

vertices: $V_G \times V_H = \{(u, v) : u \in V_G, v \in V_H\}$

edges: for $(v_1, i_1) \in V_G \times V_H$, $k_1, k_2 \in [d_0]$:

the (k_1, k_2) th neighbor of (v_1, i_1) is (v_2, i_2) where:

$$\begin{pmatrix} v_1 \\ i_1 \end{pmatrix} \xrightarrow{(a)} \begin{pmatrix} v_1 \\ i_2 \end{pmatrix} \xrightarrow{(b)} \begin{pmatrix} v_2 \\ i_2 \end{pmatrix} \xrightarrow{(c)} \begin{pmatrix} v_2 \\ i_3 \end{pmatrix} \xrightarrow{(d)} \begin{pmatrix} v_2 \\ i_4 \end{pmatrix}$$

where:

- (a) is a step in H from i_1 to its k_1 th neighbor, i_2 .
- (b) moves v_1 to the i_2 th outgoing neighbor of v_1 , v_2 .
- (c) moves from i_2 to i_3 where v_1 is the i_3 th neighbor of v_2 .
- (d) moves i_3 to its k_2 th neighbor in H .

(so $Z(G, H)$ is d_0^2 -regular)

today

Probability
(and techniques)

classes RP and BPP

tensors of graphs

Algorithms
(models and applications)

More efficient
amplification

Efficient construction
of exponentially
large expanders

A language L is in...

P if there is a (det.) polytime algo to decide if $x \in L$
(polynomial time)

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

A language L is in...

no error

P if there is a (det.) polytime algo to decide if $x \in L$
(polynomial time)

one-sided
error

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

two-sided
error

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

no error

one-sided
error

two-sided
error

A language L is in...

P if there is a (det.) polytime algo to decide if $x \in L$
(polynomial time)

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

$$P \subseteq RP \subseteq BPP$$

we don't know if they are distinct!

major question of field of pseudorandomness

Amplification

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

let LERP

$\Rightarrow$ algo w/ False-negative error prob. (say) $1/2$
using (say) m random bits

how to reduce error prob. to δ ?

1. run algo $O(\log(1/\delta))$ times
2. Output disjunction (or) of all trials

total # of random bits?

$$O(m \log(1/\delta))$$

Better?

Amplification

let **LEBPP**

BPP is there's a random. polytime algo that, on input x :
(bounded error
probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

$\Rightarrow$ algo w/ error prob. $1/3$ on both sides
using (say) m random bits

how to reduce error prob. to δ ?

1. run algo $O(\log(1/\delta))$ times
2. Output majority decision over all trials

total # of random bits?

$$O(m \log(1/\delta))$$

Better?

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

ideas?

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

RP if there's a random. polytime algo that, on input x :

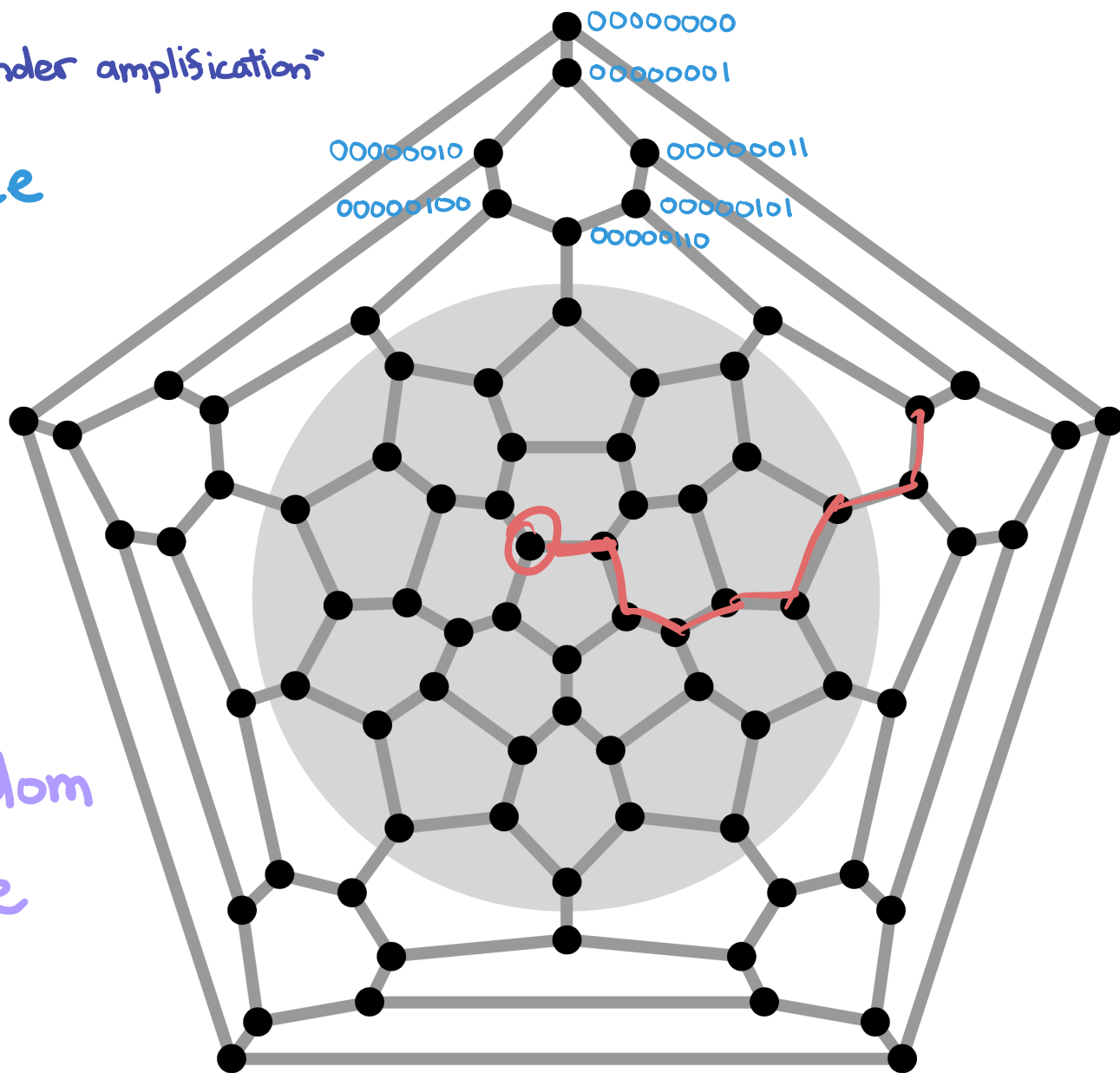
- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

High level idea "expander amplification"

- make constant degree expander $G=(V,E)$ w/ $V = \{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t = O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo



Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

constructed implicitly b/c its so big

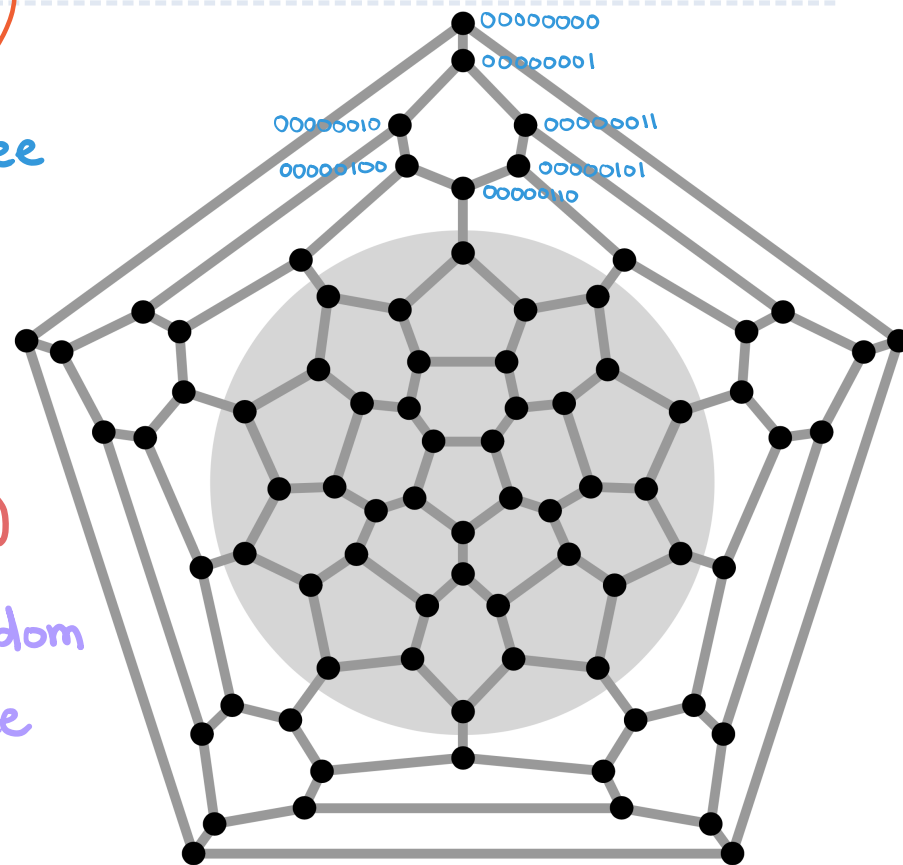
m random bits
to sample v_i

$O(1)$ random bits
per $v_i, i \geq 1$

intuitively,
random walk on
expander is like
uniform sampling

High level idea

- make constant degree expander $G=(V,E)$
w/ $V = \{0,1\}^m$
- take random walk
 $v_1, \dots, v_t \in \{0,1\}^m$
w/ $t = O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo



High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

consider RP (one-sided error)

all $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{2} \quad (\text{for example})$$

expander amplification fails iff entire random walk is in B

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

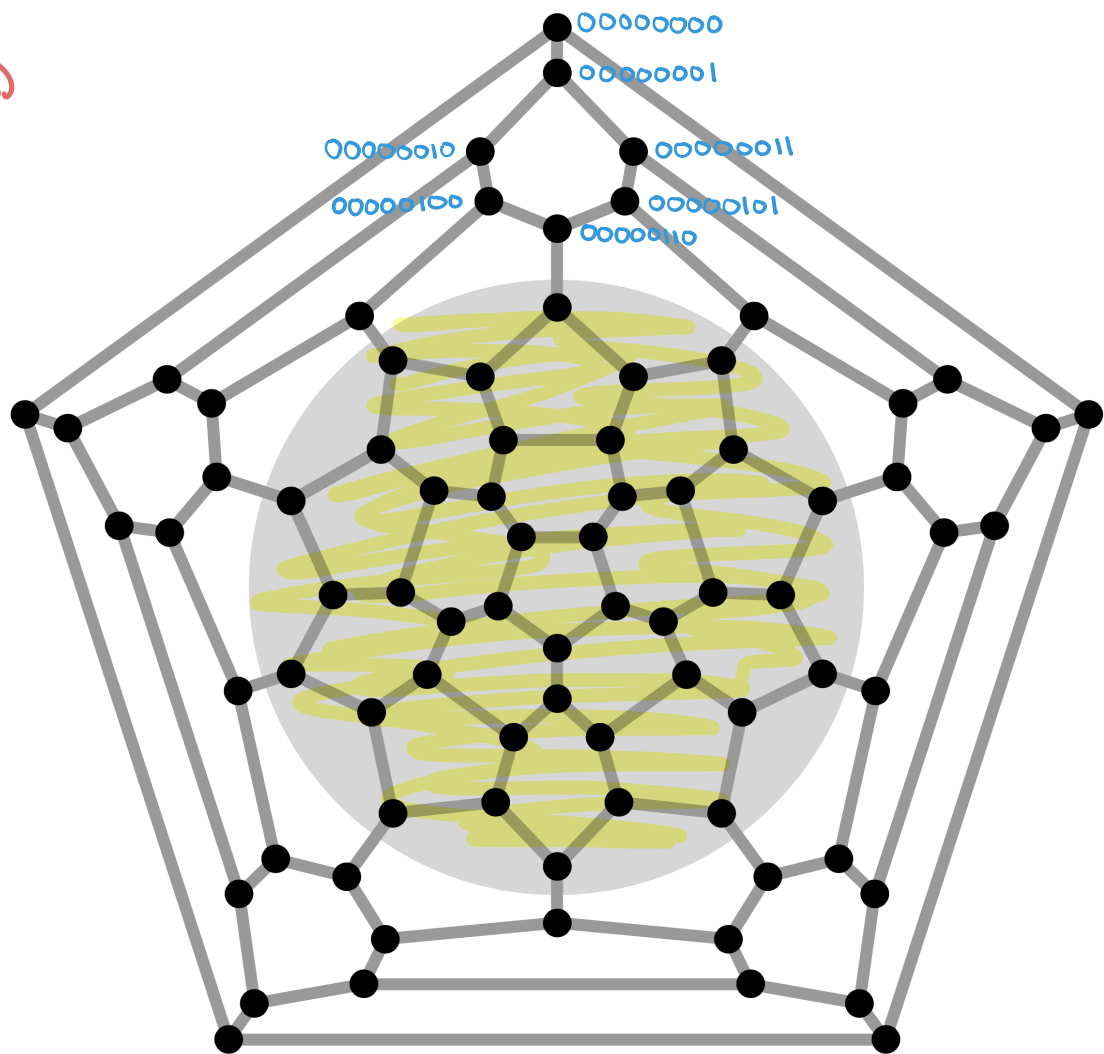
BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t = O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

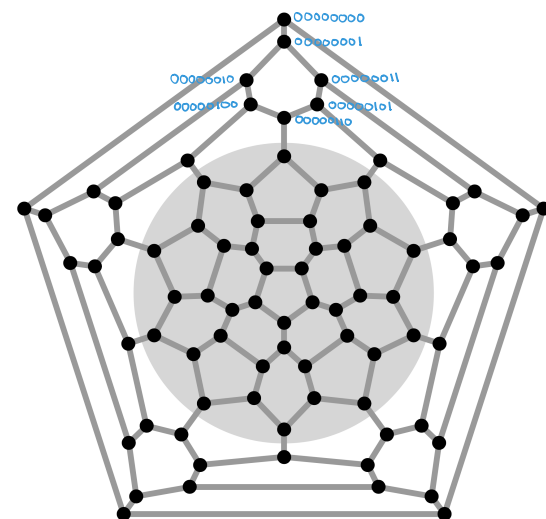
Lemma

G regular, undirected w/ spectral gap γ

$B \subset V$, $\mu = |B|/|V|$

random walk $v_1, \dots, v_t$ (v_1 unif. random)

$$P_r[v_1, \dots, v_t \in B] \leq (1 - (1 - \mu)\gamma)^t$$



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification
fails iff entire random
walk is in B

High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

consider **BPP** (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification

fails iff at least half of random walk is in B

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

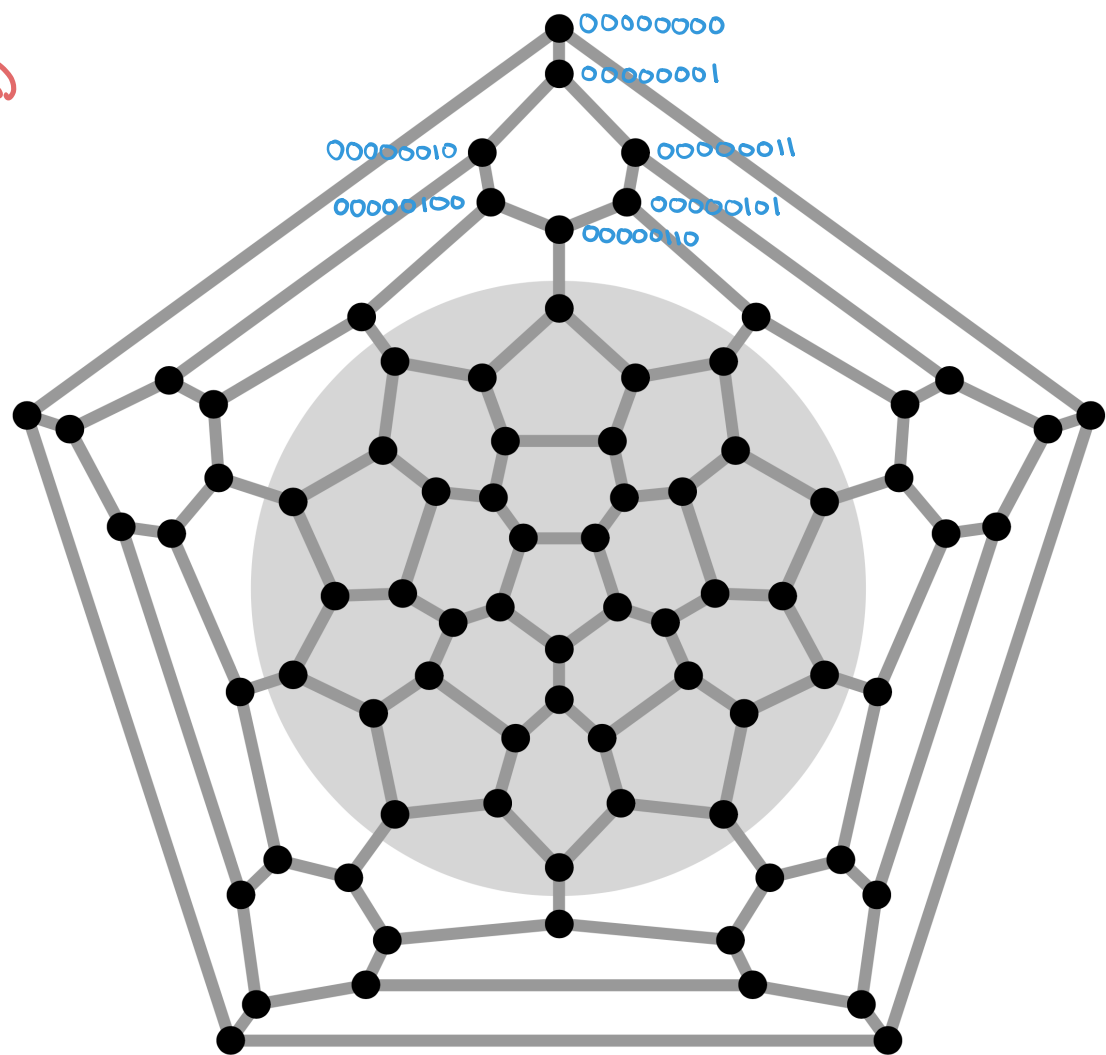
BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

Lemma "expander Chernoff"

G regular, undirected w/ spectral gap γ

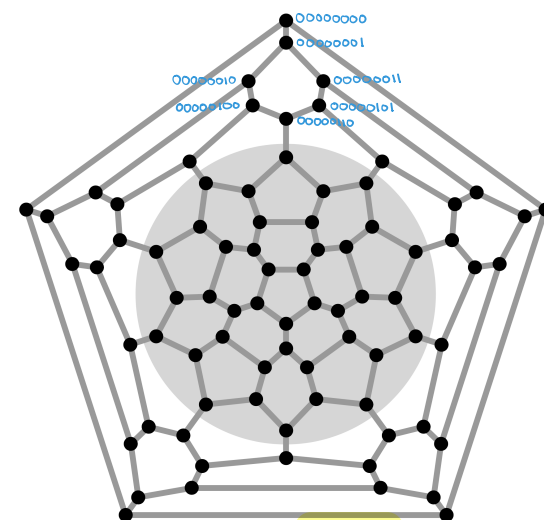
random walk $v_1, \dots, v_t$ (v_1 unif. random)

$f: V \rightarrow [0,1]$, $\mu = E[f(v)]$ (w/ $v \in V$ unif. random)

for $\epsilon, \beta \in (0,1)$,

$$\Pr\left[\left|\frac{1}{k} \sum_{i=1}^k f(v_i) - \mu\right| \geq \epsilon\mu + \beta\right] \leq O(e^{\epsilon k}(\epsilon + \epsilon^2 - \beta))$$

$$\approx e^{\epsilon k(\epsilon - \beta)}$$



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{2} \quad (\text{for example})$$

expander amplification fails iff entire random walk is in B

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

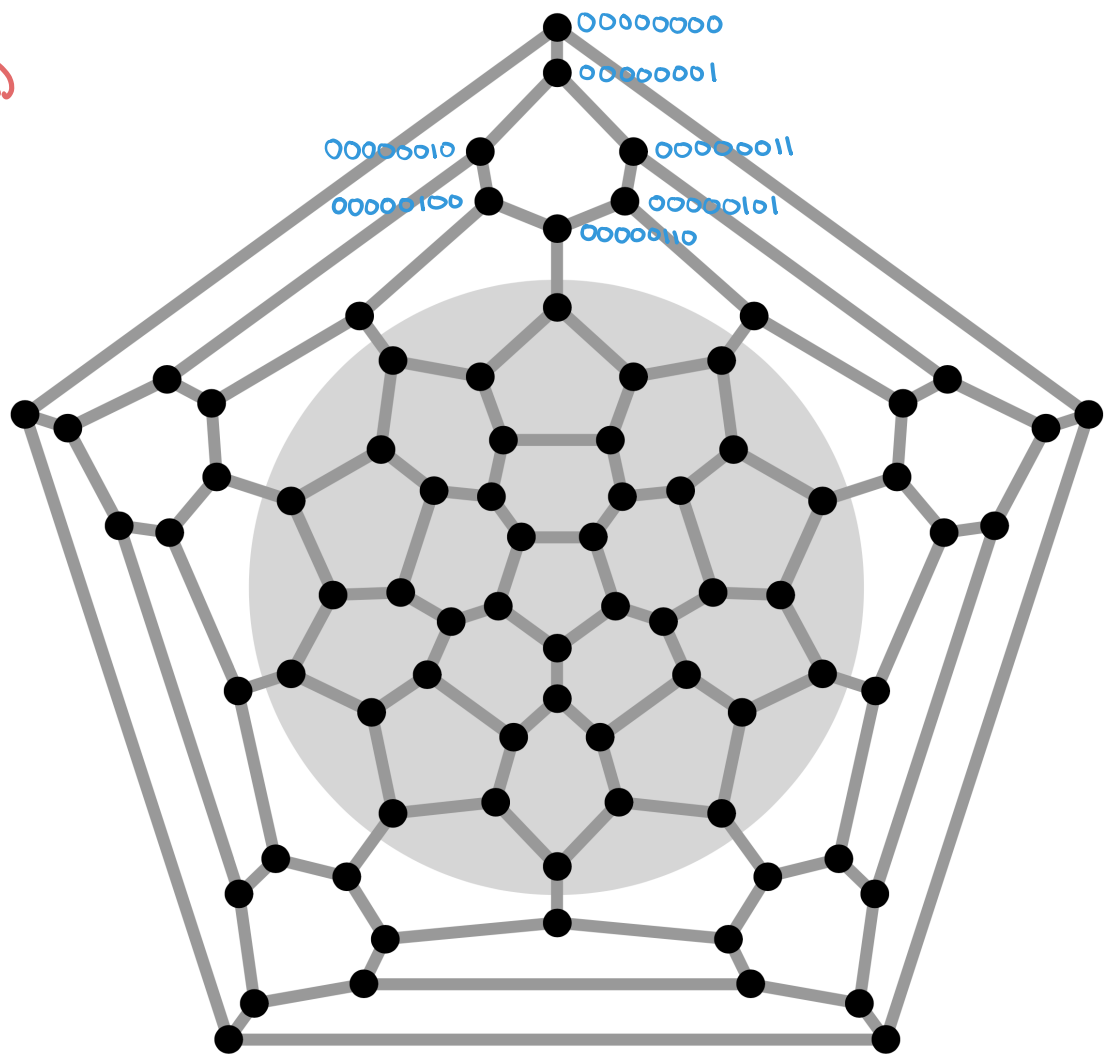
BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :
(bounded error, probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

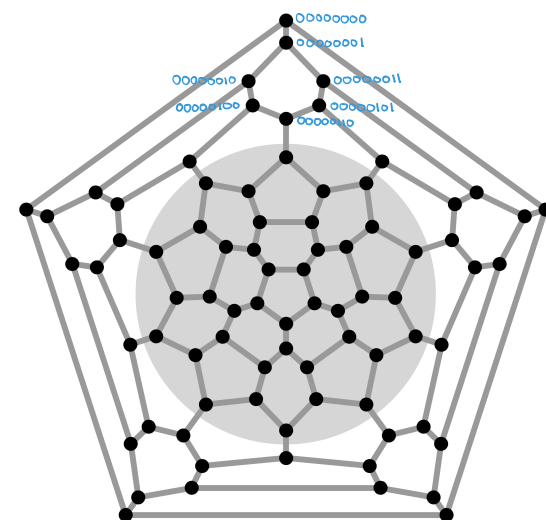
Lemma

G regular, undirected w/ spectral gap γ

$B \subset V$, $\mu = |B|/|V|$

random walk $v_1, \dots, v_t$ (v_1 unif. random)

$$P_r[v_1, \dots, v_t \in B] \leq (1 - (1 - \mu)\gamma)^t$$



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification
fails iff entire random
walk is in B

Lemma

G regular, undirected w/ spectral gap γ

$$B \subset V, \mu = |B|/|V|$$

random walk $v_1, \dots, v_t$ (v_1 unif. random)

$$P_r[v_1, \dots, v_t \in B] \leq (1 - (1 - \mu)\gamma)^t$$

Proof. let R = random walk matrix

$$\text{def } P: \mathbb{R}^V \rightarrow \mathbb{R}^V \text{ by } (Px)_v = \begin{cases} x_v & \text{if } v \in B \\ 0 & \text{otherwise} \end{cases}$$

$$\text{PRP} = \begin{cases} 1. \text{ drop mass outside } B \\ 2. \text{ take random step} \\ 3. \text{ drop mass outside } B \end{cases}$$

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

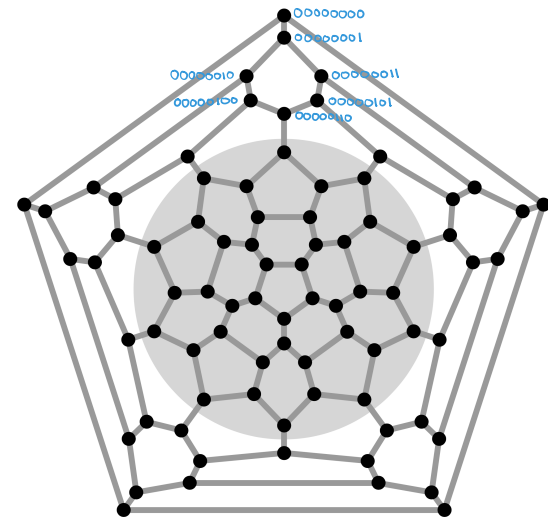
BPP if there's a random. polytime algo that, on input x :
(bounded error, probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification
fails iff entire random
walk is in B

$$(Px)_v = \begin{cases} x_v & \text{if } v \in B \\ 0 & \text{otherwise} \end{cases}$$

G regular, undirected w/ spectral gap γ
 $B \subset V$, $\mu = |B|/|V|$
 random walk $v_1, \dots, v_t$ (v_1 uniform random)

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error, probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

$$\text{PRP} = \begin{cases} 1. \text{ drop mass outside } B \\ 2. \text{ take random step} \\ 3. \text{ drop mass outside } B \end{cases}$$

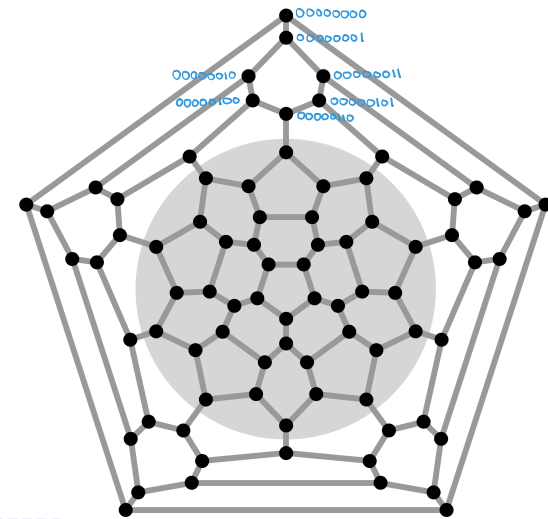
$$\langle 1, (\text{PRP})^\dagger(1/n) \rangle = \text{prob. } v_1, \dots, v_t \in B$$

$$\langle 1, (\text{PRP})^\dagger(1/n) \rangle = \frac{\langle 1, (\text{PRP})^\dagger 1 \rangle}{\langle 1, 1 \rangle} \leq \|\text{PRP}\|^\dagger$$

where $\|\cdot\|$ = operator norm = max abs. eigenvalue

$$\text{claim: } \|\text{PRP}\| \leq 1 - (1 - \mu)\gamma = 1 - \gamma + \gamma\mu$$

(which completes the proof)



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification fails iff entire random walk is in B

claim: $\|PRP\| \leq 1 - (1 - \mu)\delta$

G regular w/ spec gap δ
 $B \subset V$, $\mu = |B|/|V|$

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

G regular $\Rightarrow R$ symmetric

$$R = \frac{1 \otimes 1}{n} + \mu_2(v_2 \otimes v_2) + \dots + \mu_n(v_n \otimes v_n)$$

$$= \frac{\delta}{n} (1 \otimes 1) + R' \quad \text{w/ } \|R'\| \leq 1 - \delta$$

$$\|PRP\| \leq \frac{\delta}{n} P(1 \otimes 1)P + \|PR'P\|$$

$$= \frac{\delta}{n} (P1 \otimes P1) + \|PR'P\|$$

$$= \left\| \frac{\delta}{n} (1_B \otimes 1_B) + \|PR'P\| \right\|$$

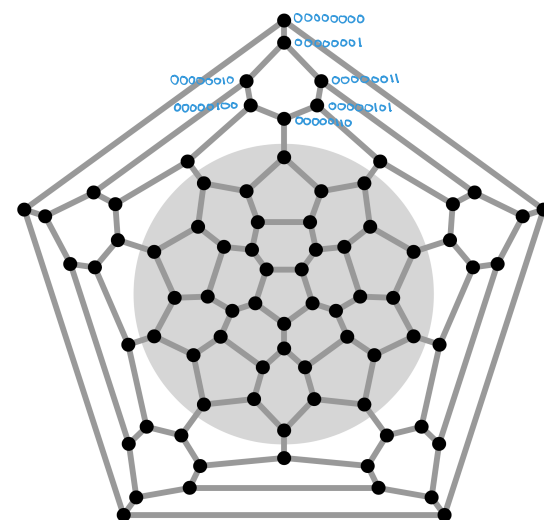
$$= \frac{\delta |B|}{n} + \|PR'P\|$$

$\|x\|=1$

$$\|1_B \otimes 1_B\| = |B|$$

$$\leq |B| \cdot \frac{1_B}{\sqrt{|B|}} \otimes \frac{1_B}{\sqrt{|B|}}$$

$$= \delta \mu + 1 - \delta$$



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification fails iff entire random walk is in B

$$\delta_m + \delta$$

G regular w/ spec gap δ
 $B \subset V$, $m = |B|/|V|$

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

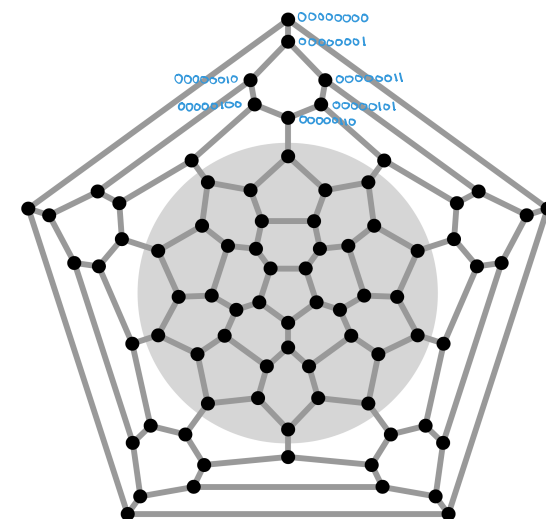
BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification
 fails iff entire random
 walk is in B

High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

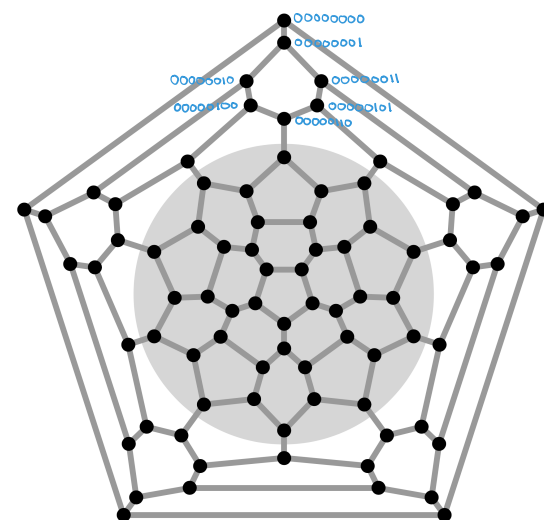
Lemma

G regular, undirected w/ spectral gap γ

$$B \subset V, \mu = |B|/|V|$$

random walk $v_1, \dots, v_t$ (v_1 unif. random)

$$P_r[v_1, \dots, v_t \in B] \leq (1 - (1 - \mu)\gamma)^t$$



consider RP (one-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

expander amplification

fails iff entire random walk is in B

High level idea

- make constant degree expander $G=(V,E)$ w/ $V = \{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t = O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

Lemma "expander Chernoff"

G regular, undirected w/ spectral gap $\gamma = 1 - \epsilon$

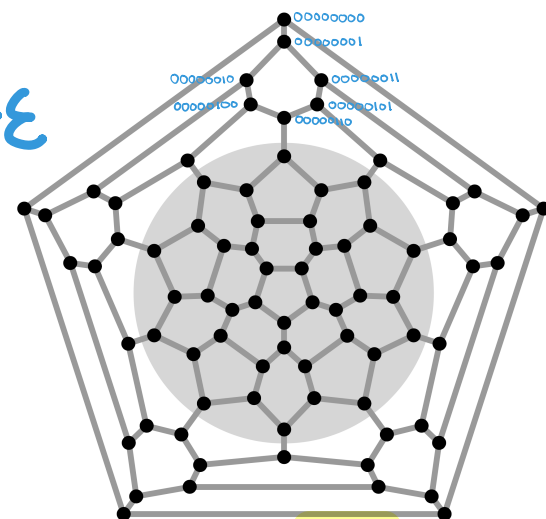
random walk $v_1, \dots, v_t$ (v_1 unif. random)

$f: V \rightarrow [0,1]$, $\mu = E[f(v)]$ (w/ $v \in V$ unif. random)

for $\beta \in (0,1)$,

$$\Pr\left[\left|\frac{1}{k} \sum_{i=1}^k f(v_i) - \mu\right| \geq \epsilon\mu + \beta\right] \leq O(e^{\epsilon k}(\epsilon + \epsilon^2 - \beta))$$

$$\approx e^{\epsilon k(\epsilon - \beta)}$$



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

proof

G regular w/ spec gap γ
 $f: V \rightarrow [0,1]$, $\mu = E[f(v)]$
 $\epsilon, \beta \in (0,1)$

$$P[f(v_1) + \dots + f(v_k) \geq \lambda] \\ \leq E[e^{t(f(v_1) + \dots + f(v_k))}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{tf(v_1)}, \dots, e^{tf(v_n)})$

claim: $E[e^{t(f(v_1) + \dots + f(v_k))}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

$FR \frac{\mathbf{1}}{n} = E[\text{take a step, collect } e^{f(v)}]$

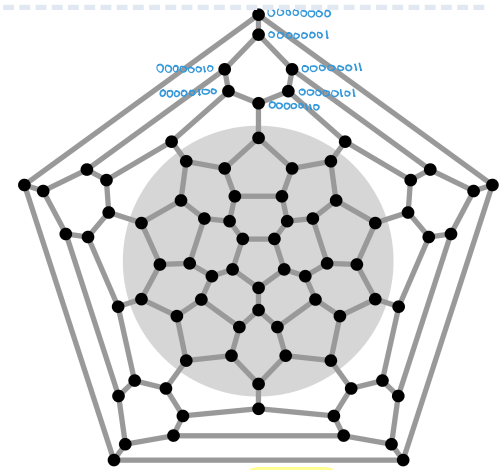
$(FR)^k \frac{\mathbf{1}}{n} = E[\text{take } k \text{ steps, collect } e^{f(v)} \text{ each step}]$

$F(RF)^k \frac{\mathbf{1}}{n} = (FR)^k F \frac{\mathbf{1}}{n} = E[\uparrow]$

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)
 • if $x \in L$, decides $x \in L$ w/ constant prob.
 • if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)
 • if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
 • if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem
 Given RP/BPP algo, one can get error prob δ w/
 • $O(\log(1/\delta))$ -factor increase in running time
 • $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)
 call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)
 let $B = \{ \text{bad } v \}$
 $\frac{|B|}{|V|} \leq \frac{1}{3}$ (for example)
 expander amplification fails iff at least half of random walk is in B

$$P[f(v_1) + \dots + f(v_k) \geq \lambda]$$

$$\leq E[e^{t(f(v_1) + \dots + f(v_k))}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{tf(v_1)}, \dots, e^{tf(v_n)})$

✓ $E[e^{t(f(v_1) + \dots + f(v_n))}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

Let $R = \frac{\delta}{n}(\mathbf{1}\mathbf{1}^T) + R'$ w/ $\|R'\| \leq 1 - \delta = \epsilon$

claim: $\|F^{1/2} R' F^{1/2}\| \leq \epsilon e^t$

$$\langle x, F^{1/2} R' F^{1/2} x \rangle = \langle F^{1/2} x, R' (F^{1/2} x) \rangle$$

$$\leq \epsilon \|F^{1/2} x\|^2$$

$$\leq \epsilon e^t \|x\|^2$$

$f: V \rightarrow [0,1], \mu = E[f(v)]$

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

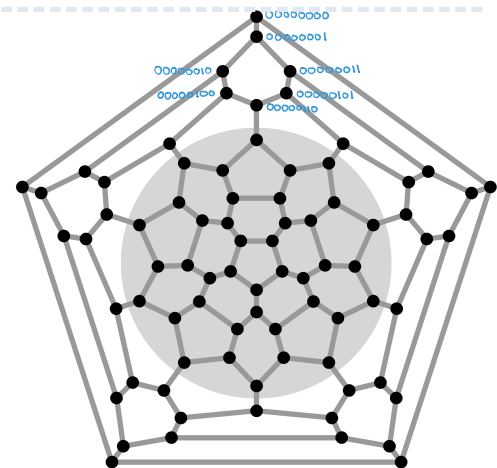
BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{ \text{bad } v \}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

$$P[f(v_1) + \dots + f(v_k) \geq \lambda]$$

$$\leq E[e^{t(f(v_1) + \dots + f(v_k))}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{tf(v_1)}, \dots, e^{tf(v_n)})$

✓ $E[e^{t(f(v_1) + \dots + f(v_n))}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

Let $R = \frac{\delta}{n}(\mathbf{1} \otimes \mathbf{1}) + R'$ w/ $\|R'\| \leq 1 - \delta = \varepsilon$

✓ $\|F^{1/2} R' F^{1/2}\| \leq \varepsilon e^t$

claim: $\|F^{1/2}(\mathbf{1} \otimes \mathbf{1})F^{1/2}\| \leq n E[e^{tf(v)}]$

$$F^{1/2}(\mathbf{1} \otimes \mathbf{1})F^{1/2} = (F^{1/2} \mathbf{1}) \otimes (F^{1/2} \mathbf{1})$$

$$\|F^{1/2} \mathbf{1}\|^2 = \langle \mathbf{1}, F \mathbf{1} \rangle = n E[e^{tf(v)}]$$

$f: V \rightarrow [0,1], \mu = E[f(v)]$

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

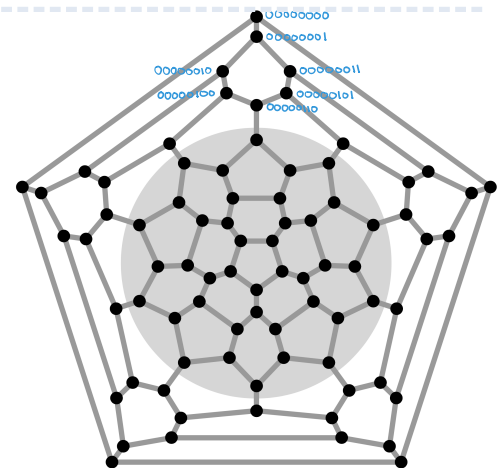
BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

$$P[f(v_1) + \dots + f(v_k) \geq \lambda]$$

$$\leq E[e^{t(f(v_1) + \dots + f(v_k))}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{tf(v_1)}, \dots, e^{tf(v_n)})$

✓ $E[e^{t(f(v_1) + \dots + f(v_n))}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

Let $R = \frac{\delta}{n}(\mathbf{1} \otimes \mathbf{1}) + R'$ w/ $\|R'\| \leq 1 - \delta = \epsilon$

✓ $\|F^{1/2} R' F^{1/2}\| \leq \epsilon e^t$

✓ $\|F^{1/2}(\mathbf{1} \otimes \mathbf{1}) F^{1/2}\| \leq n E[e^{tf(v)}]$

$$\|F^{1/2} R F^{1/2}\| \leq \frac{\delta}{n} \|F^{1/2}(\mathbf{1} \otimes \mathbf{1}) F^{1/2}\| + \|F^{1/2} R' F^{1/2}\|$$

$$\delta E[e^{tf(v)}] + \epsilon e^t \leq \epsilon + t\epsilon + t^2\epsilon$$

✓ $\leq \delta E[1 + t f(v) + t^2 f^2(v)] \leq \delta(1 + t\mu + t^2\mu)$

$f: V \rightarrow [0,1], \mu = E[f(v)]$

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

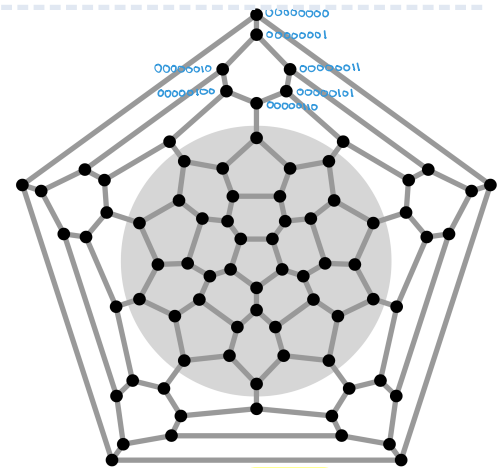
BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification

fails iff at least half of random walk is in B

$$e^x \leq 1 + x + \frac{x^2}{2}$$

$$\epsilon + t\epsilon + t^2\epsilon + (1-\epsilon)(1+t\mu + t^2\mu) \quad t = \epsilon$$

$$\epsilon + \epsilon^2 + \epsilon^3 + (1-\epsilon)(1+\epsilon\mu + \epsilon^2\mu)$$

$$= 1 + (\epsilon + \epsilon^2)(\mu + \epsilon) \leq e^{(\epsilon + \epsilon^2)(\mu + \epsilon)}$$

$$P[f(v_1) + \dots + f(v_k) \geq \lambda]$$

$$\leq E[e^{t(f(v_1) + \dots + f(v_k))}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{tf(v_1)}, \dots, e^{tf(v_n)})$

✓ $E[e^{t(f(v_1) + \dots + f(v_n))}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

Let $R = \frac{\delta}{n}(\mathbf{1} \otimes \mathbf{1}) + R'$ w/ $\|R'\| \leq 1 - \delta = \epsilon$

✓ $\|F^{1/2} R' F^{1/2}\| \leq \epsilon e^t$ $t = \epsilon$

✓ $\|F^{1/2}(\mathbf{1} \otimes \mathbf{1}) F^{1/2}\| \leq \underbrace{E[e^{tf(v)}]}_{1+O(\epsilon)} E[H 2tf(v)] \leq 1+2\epsilon$

✓ $\|F^{1/2} R F^{1/2}\| \leq e^{(t+t^2)(\epsilon+\mu)}$

$$\frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle = \frac{1}{n} \langle F^{1/2} \mathbf{1}, (F^{1/2} R F^{1/2})^k F^{1/2} \mathbf{1} \rangle \leq \frac{1}{n} \|F^{1/2} \mathbf{1}\|^2 e^{k(t+t^2)(\epsilon+\mu)} = \cancel{E[e^{tf(v)}]}_0$$

$f: V \rightarrow [0,1], \mu = E[f(v)]$

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

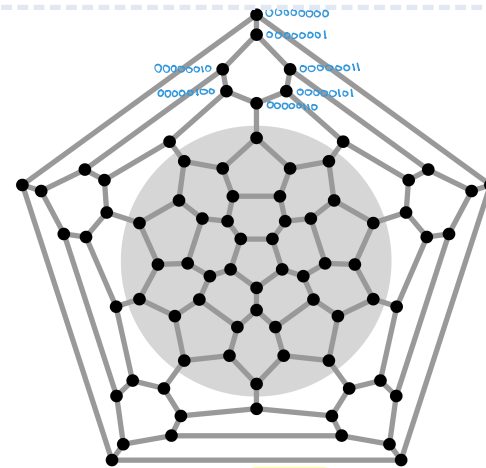
BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^n$ "bad" if algo makes error w/ v (as random bits)

let $B = \{ \text{bad } v \}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

$$P[\sum_{i=1}^n \epsilon_i \geq \lambda]$$

$$\leq E[e^{t(\sum_{i=1}^n \epsilon_i)}] e^{-t\lambda}$$

Let $F = \text{diag}(e^{t\epsilon_1}, \dots, e^{t\epsilon_n})$

✓ $E[e^{t(\sum_{i=1}^n \epsilon_i)}] = \frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle$

✓ $\|F^{1/2} R F^{1/2}\| \leq e^{(t+t^2)(\epsilon+\mu)}$

$\frac{1}{n} \langle \mathbf{1}, F(RF)^k \mathbf{1} \rangle \leq (1+O(\epsilon)) e^{k(1+\epsilon)\epsilon(\mu+\epsilon)}$

$$E[e^{t(\sum_{i=1}^n \epsilon_i)}] e^{-t\lambda}$$

$$\leq (1+O(\epsilon)) e^{\underline{k(1+\epsilon)\epsilon(\mu+\epsilon)} - \epsilon\lambda}$$

$\epsilon: V \rightarrow [0,1], \mu = E[\epsilon(v)]$

RP if there's a random. polytime algo that, on input x:

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

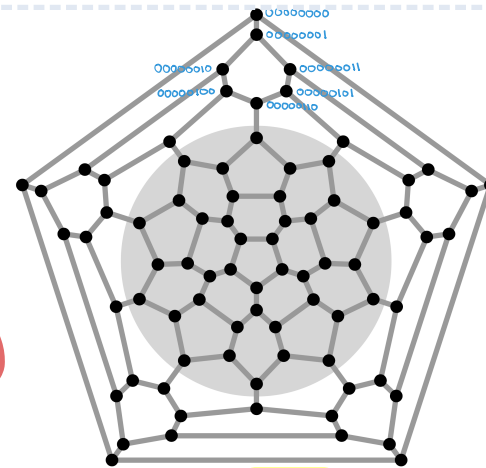
BPP is there's a random. polytime algo that, on input x:

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{ \text{bad } v \}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

$$\lambda = (1+2\epsilon)k(\mu+\epsilon)$$

$$= e^{-\frac{e^2}{\#k\mu}} + e^2$$

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

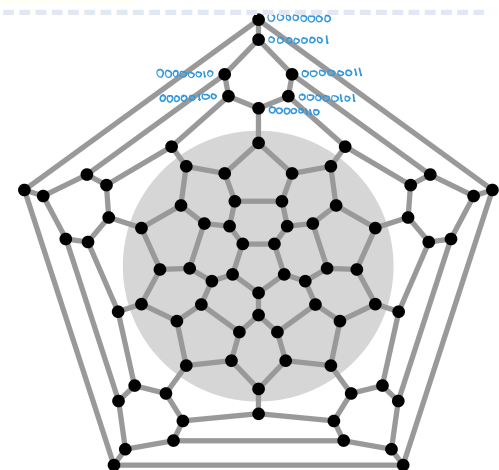
BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification

fails iff at least half of random walk is in B

High level idea

- make constant degree expander $G=(V,E)$ w/ $V=\{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t=O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP is there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

✓ Lemma "expander Chernoff"

G regular, undirected w/ spectral gap $\gamma=1-\epsilon$

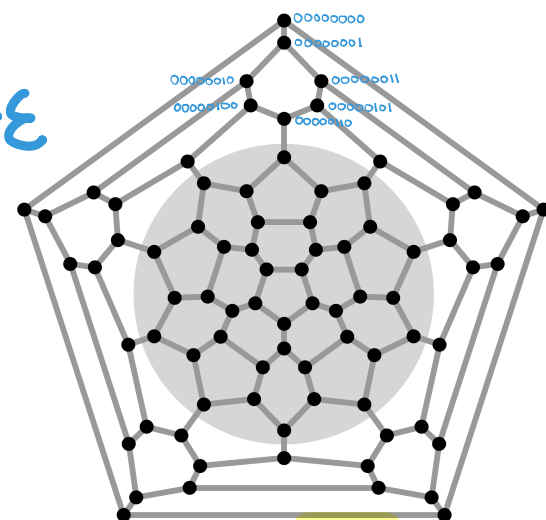
random walk $v_1, \dots, v_t$ (v_i unif. random)

$f: V \rightarrow [0,1]$, $\mu = E[f(v)]$ (w/ $v \in V$ unif. random)

for $\beta \in (0,1)$,

$$\Pr\left[\left|\frac{1}{k} \sum_{i=1}^k f(v_i) - \mu\right| \geq \epsilon\mu + \beta\right] \leq O(e^{\epsilon k}(\epsilon + \epsilon^2 - \beta))$$

$$\approx e^{\epsilon k(\epsilon - \beta)}$$



consider BPP (two-sided error)

call $v \in \{0,1\}^m$ "bad" if algo makes error w/ v (as random bits)

let $B = \{\text{bad } v\}$

$$\frac{|B|}{|V|} \leq \frac{1}{3} \quad (\text{for example})$$

expander amplification fails iff at least half of random walk is in B

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error, probabilistic polynomial time)

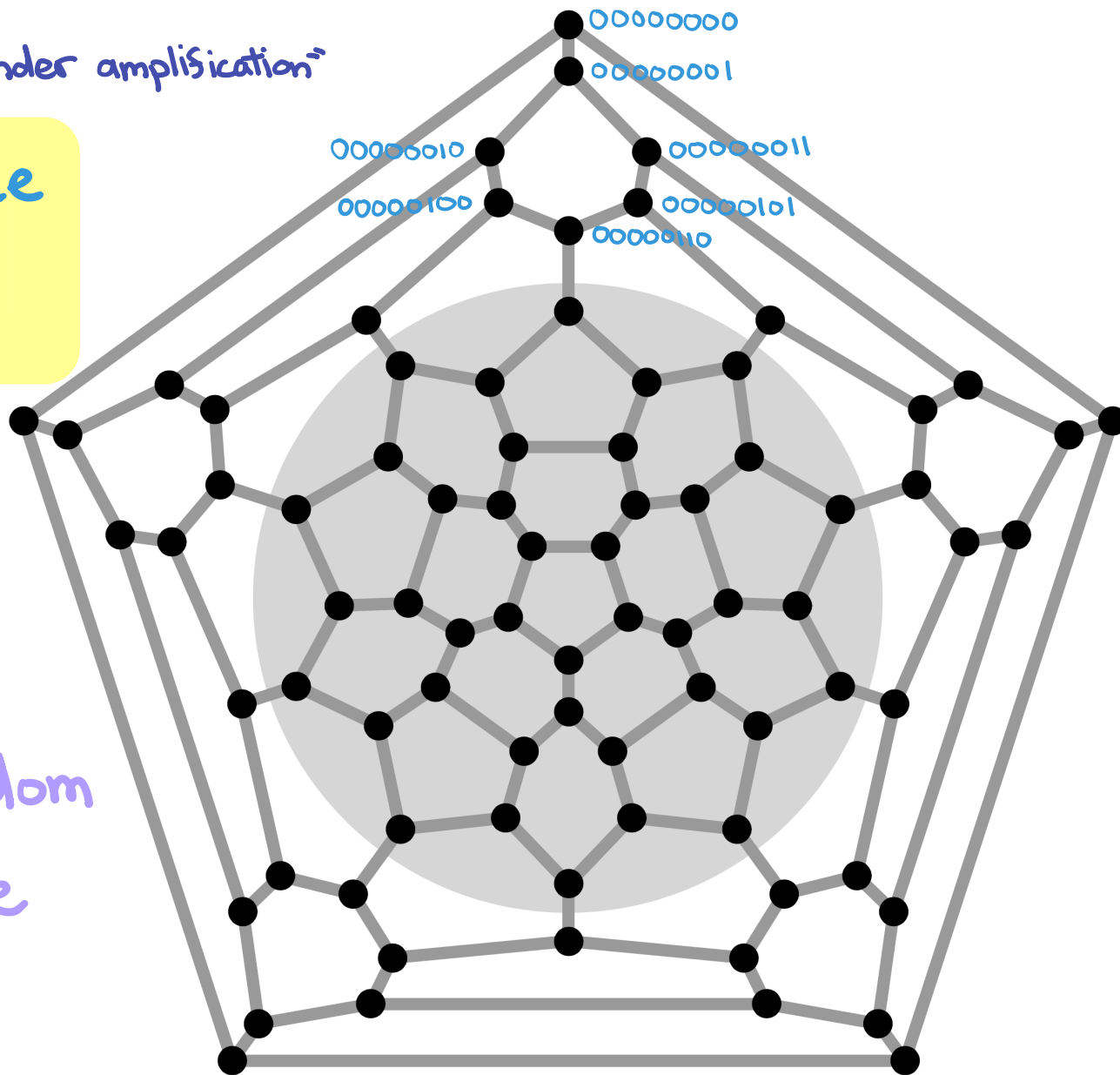
- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

High level idea "expander amplification"

- make constant degree expander $G=(V,E)$
w/ $V = \{0,1\}^m$

- take random walk
 $v_1, \dots, v_t \in \{0,1\}^m$
w/ $t = O(\log(1/\delta))$

- use each v_i as random bits for i th instance of algo



Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :

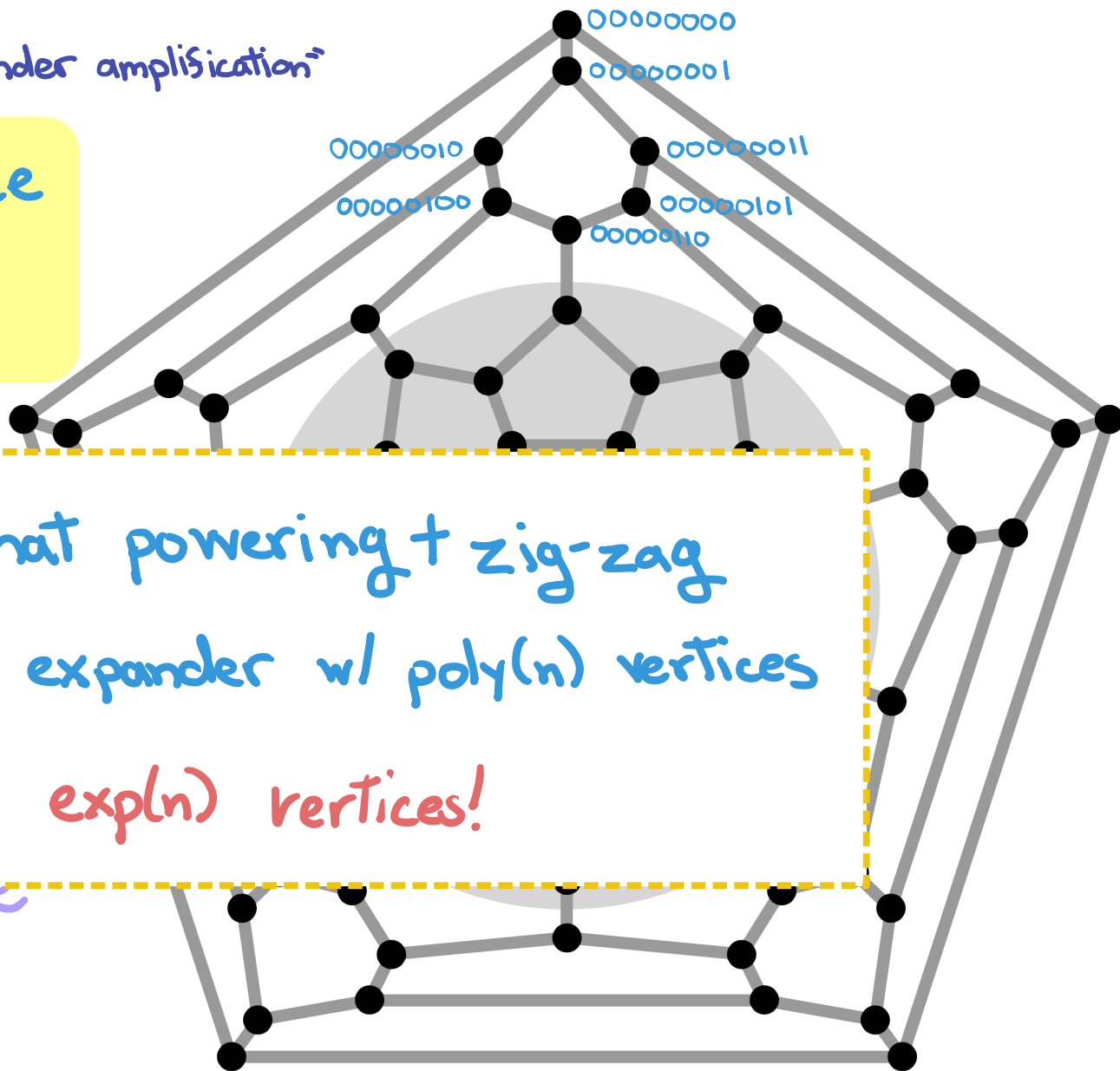
- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

High level idea "expander amplification"

- make constant degree expander $G=(V,E)$ w/ $V = \{0,1\}^m$

- take V_1 we know that powering + zig-zag $\Rightarrow$ const. degree expander w/ $\text{poly}(n)$ vertices

- use bits for an instance of algo we need $\exp(n)$ vertices!



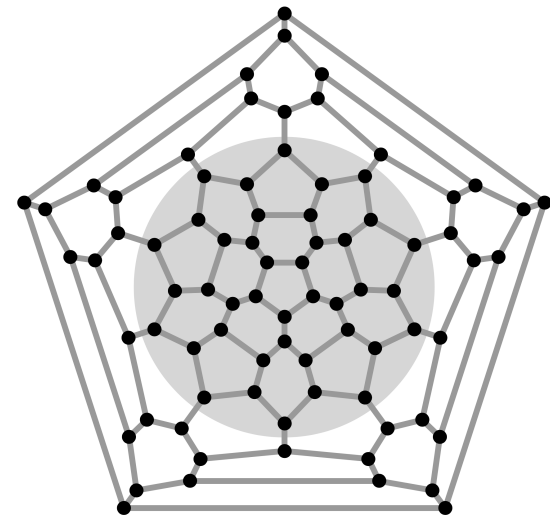
let H be constant degree expander
w/ degree d , d^8 vertices, $\gamma \geq 7/8$

$$G_1 = H^2$$

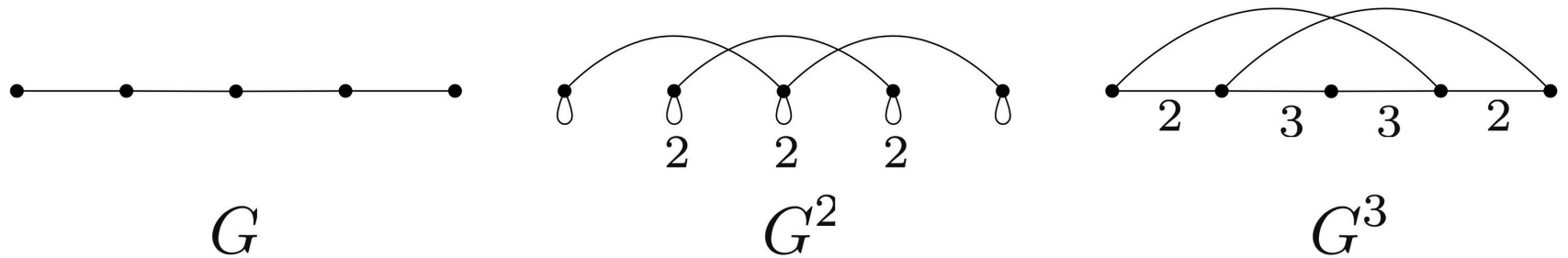
graph tensor product

$$G_{t+1} = Z((G_t \otimes G_t) \mid H)$$

zig-zag product



Powering



$G^k =$ graph w/ an edge for every k step walk in G
(w/ repetition)

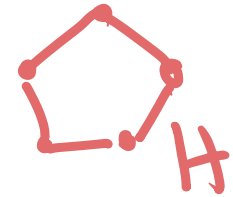
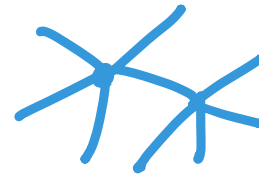
random walk R^k has eigenvalues $1, u_2^k, \dots, u_n^k$

$$\delta(G^k) = 1 - (1 - \delta(G))^k \quad \text{😊}$$

degree increases from d to d^k 😞

Zig-zag product $Z(G, H)$

let G be d -regular

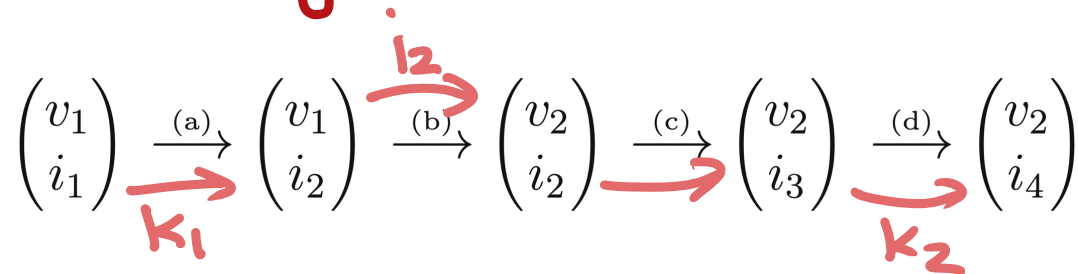


H be d_0 -regular w/ d_0 vertices (H will be $O(D)$ -degree expander)

vertices: $V_G \times V_H = \{(u, v) : u \in V_G, v \in V_H\}$

edges: for $(v_1, i_1) \in V_G \times V_H$, $k_1, k_2 \in [d_0]$:

the (k_1, k_2) th neighbor of (v_1, i_1) is (v_2, i_4) where:



where:

- (a) is a step in H from i_1 to its k_1 th neighbor, i_2 .
- (b) moves v_1 to the i_2 th outgoing neighbor of v_1 , v_2 .
- (c) moves from i_2 to i_3 where v_1 is the i_3 th neighbor of v_2 .
- (d) moves i_3 to its k_2 th neighbor in H .

(so $Z(G, H)$ is d_0^2 -regular)

Lemma: $Z(G|H)$ has

- n vertices
- degree d_0^2 😊
- spectral gap $\gamma_G \gamma_H^2$ 😊

Zig-zag product $Z(G,H)$

let G be d -regular

H be d_0 -regular w/ d vertices (H will be $O(n)$ -degree expander)

vertices: $V_G \times V_H = \{(u,v) : u \in V_G, v \in V_H\}$

edges: for $(v_1, i_1) \in V_G \times V_H$, $k_1, k_2 \in [d_0]$:

the (k_1, k_2) th neighbor of (v_1, i_1) is (v_2, i_4) where:

$$\begin{pmatrix} v_1 \\ i_1 \end{pmatrix} \xrightarrow{(a)} \begin{pmatrix} v_1 \\ i_2 \end{pmatrix} \xrightarrow{(b)} \begin{pmatrix} v_2 \\ i_2 \end{pmatrix} \xrightarrow{(c)} \begin{pmatrix} v_2 \\ i_3 \end{pmatrix} \xrightarrow{(d)} \begin{pmatrix} v_2 \\ i_4 \end{pmatrix}$$

where:

- (a) is a step in H from i_1 to its k_1 th neighbor, i_2 .
- (b) moves v_1 to the i_2 th outgoing neighbor of v_1 , v_2 .
- (c) moves from i_2 to i_3 where v_1 is the i_3 th neighbor of v_2 .
- (d) moves i_3 to its k_2 th neighbor in H .

(so $Z(G,H)$ is d_0^2 -regular)

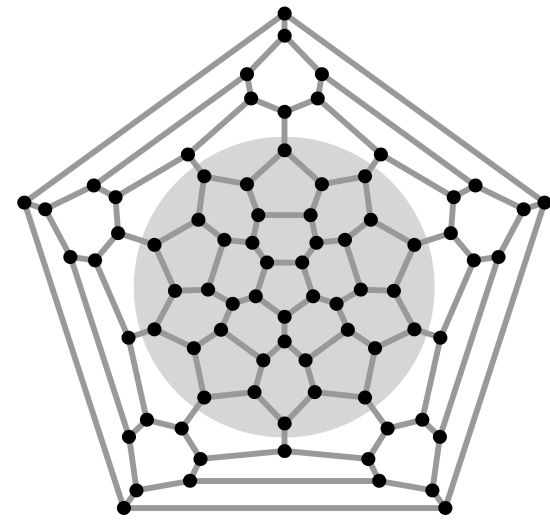
let H be constant degree expander
w/ degree d , d^8 vertices, $\gamma \geq 7/8$

$$G_1 = H^2$$

$$G_{t+1} = Z((G_t \otimes G_t) \mid H)$$

zig-zag product

graph tensor product



Tensor products

for $A \in \mathbb{R}^{m \times m}$, $B \in \mathbb{R}^{n \times n}$,

$A \otimes B$ is a linear map on $\mathbb{R}^{m \times n}$ defined by

$$(A \otimes B)C = ACB \quad \text{for } C \in \mathbb{R}^{m \times n}$$

special case:

$$(A \otimes B)(c \otimes d) = (Ac) \otimes (Bd) \quad c \in \mathbb{R}^m, d \in \mathbb{R}^n$$

Fact: $A \otimes B$ has eigenvalues $\lambda_A \lambda_B$ where

λ_A is an eigenvalue of A ,

λ_B B

Tensor product $I \otimes R_H$

$I \otimes R_H$ is a linear map on $\mathbb{R}^{V \times d}$ defined by

$$((I \otimes R_H)X)_v = R_H X_v \quad X \in \mathbb{R}^{V \times d}$$

where $X_v = v$ th row of X .

Fact: $I \otimes (A+B) = I \otimes A + I \otimes B$

Graph tensor

$$\text{let } G_1 = (V_1, E_1), \quad G_2 = (V_2, E_2)$$

$$G_1 \otimes G_2 = (V_1 \times V_2, E_1 \times E_2)$$

$$V_1 \times V_2 = \{(v_1, v_2) : v_1 \in V_1, v_2 \in V_2\}$$

$$E_1 \times E_2 = \{((u_1, u_2), (v_1, v_2)) : (u_1, v_1) \in E_1, (u_2, v_2) \in E_2\}$$

is $R_1 =$ random walk for G_1

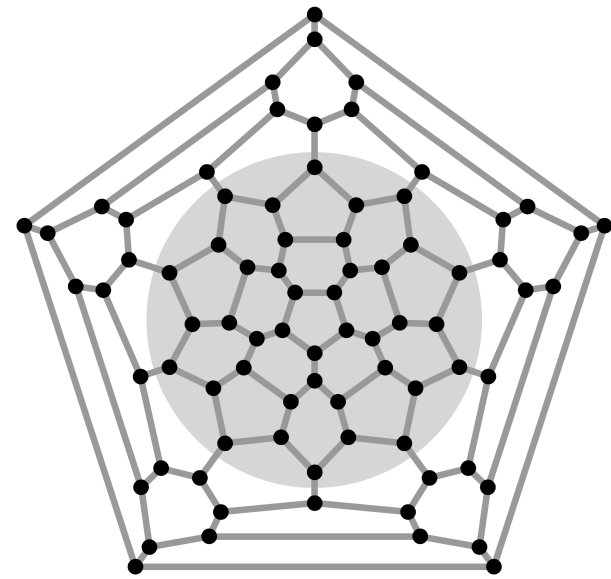
$R_2 =$    G_2

then $R_1 \otimes R_2 =$ random walk for $G_1 \otimes G_2$

let H be constant degree expander
w/ degree d , d^8 vertices, $\gamma \geq 7/8$

$$G_1 = H^2$$

$$G_{t+1} = Z((G_t \otimes G_t) | H)$$



G^k = graph w/ edge for every k step walk
(w/ repetition)

$$\gamma(G^k) = 1 - (1 - \gamma(G))^k$$

degree increases from d to d^k

graph

G

$G \otimes G$

$(G \otimes G)^2$

$Z((G \otimes G)^2 | H)$

vertices

n

degree

d^2

γ

γ

Lemma: $Z(G | H)$ has

- n vertices
- degree d^2
- spectral gap $\gamma_G \gamma_H^2$

Fact: $A \otimes B$ has eigenvalues $\lambda_A \lambda_B$
w/ λ_A is an eigenvalue of A ,
 λ_B is an eigenvalue of B

$$\gamma \geq \frac{1}{2} \Rightarrow$$

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob. $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

ideas?

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

RP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

High level idea "expander amplification"

- make constant degree expander $G=(V,E)$ w/ $V = \{0,1\}^m$
- take random walk $v_1, \dots, v_t \in \{0,1\}^m$ w/ $t = O(\log(1/\delta))$
- use each v_i as random bits for i th instance of algo

