Expanders et al.

10 October 2017 16:47

- HW's — ≥ 50% pts & ≥ 3/4 series

graphs that are hard to separate into pieces

$\forall S, T, |S| \leq |T|$ # of edges between S & T "large"

Be careful: 

single vertex can be separated: "large" ≈ proportional to $|S|, |T|$

Obvious application: clustering
- partitioning graph into well connected pieces

this course: properties, constructions, applications
→ many open problems

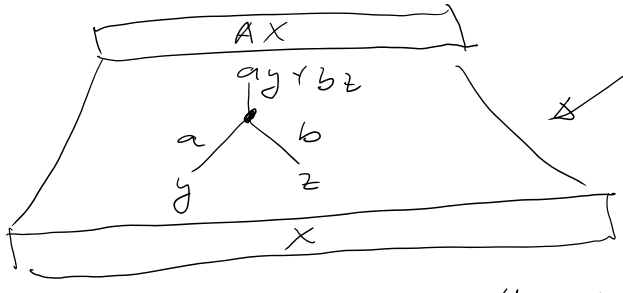
motivating examples

- Valiant '76

Goal: prove that some linear transformation (think FFT) requires circuits of size $\omega(n)$.

Fix matrix A over some Field

Easy: random A requires ckt of size $\Omega(n^2/\log n)$ w.h.p.



(linear) circuit

$a, b \in F$ constants

$y, z \in F$ values

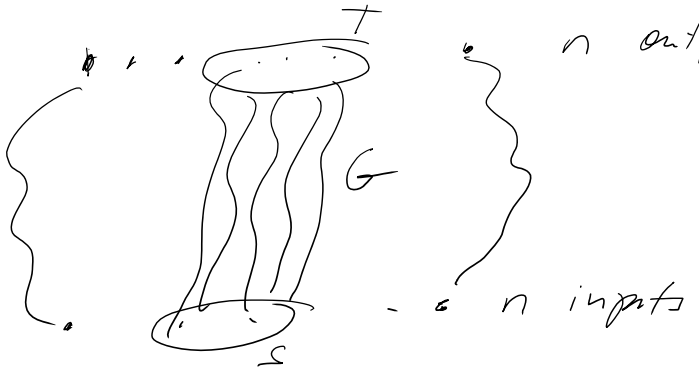
Valiant: A is super-regular if all submatrices are

Valiant: A is super-regular if all submatrices are of full rank.

Hypothesis: A is super-regular $\Rightarrow$ A requires $\omega(n)$ gates in its circuit.

(Valiant disproved his own conjecture ☹)

↳ idea: super-concentrators



- $\forall S$ of inputs $\forall T$ of outputs
  if $|S| = |T|$ then there are $|S|$ vertex disjoint path between S & T
- If A is super-regular then its circuit must be super-concentrator. Pf: easy ☺

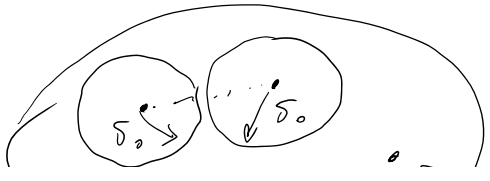
Conjecture: super-concentrators require $\omega(n)$ edges

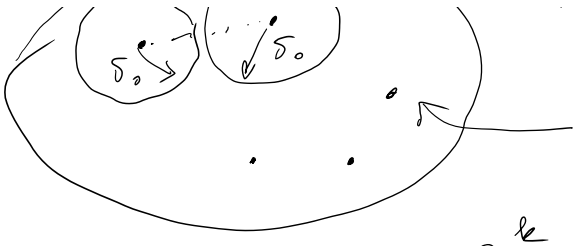
↳ FALSE: Valiant

TRUE: Dolev, Dwork, Pippenger, Wigderson - for bounded-depth graphs

(see later)

Error correcting codes





$C \subseteq \{0,1\}^n$

want: (1) $|C| = 2^k$ $\quad k \geq \tau n$ (rate)

(2) $\forall x, y \in C \quad \Delta(x,y) \geq \delta_0 n$ (relative distance)

↑ Hamming distance

$0 < \tau, \delta_0$ should be some constants

- How to find C?

Explicit constructions?

Eas: random $C \subseteq \{0,1\}^n$ is a good ECC.

Deterministic Error amplification (for RP)

Rabin's primality test

$F(p,r) = 1$ $\quad \forall r$ if p is a prime

$f(p,r) = 1$ $\quad$ for $< \frac{1}{2}$ of r's if p is not a prime

F is pol time computable

by repeating test for $r_1, r_2, \ldots r_k$ chosen independently at random $\Rightarrow$ error 2^{-k}.

requires $k \cdot |r|$ bits. Can we do better?

⟶ Magic graphs

$G = (L, R, E)$ bipartite $\quad |L| = n \quad |R| = m$

- G is (n, m, d)-magical if left-degree $= d$ $\forall$ vertices

- G is (n, m, d)-magical if left-regular, d vertices

$\forall S \subseteq L$

(1) $|S| \le \frac{n}{10d} \Rightarrow |\Gamma(S)| \ge \frac{5d}{8}|S|$

(2) $\frac{n}{10d} \le |S| \le \frac{n}{2} \Rightarrow |\Gamma(S)| \ge |S|$.

Claim: $\exists n_0 \; \forall d \ge 32, \; \forall n \ge n_0, \; m \ge \frac{3}{4}n$

$\exists G$ that is (n, m, d)-magical

Pf: probabilistic construction

- For each vertex $v \in L$, pick independently at random d vertices from R (with repetition, they can be dealt with afterwards)
- Want upper bound the probability (1) or (2) fails

(1) fails $\Rightarrow \exists S \subseteq L, T \subseteq R$ $\left(|S| = s \le \frac{n}{10d}\right.$

$\left(|T| = t = \frac{5}{8}sd\right.$

s.t. $\Gamma(S) \subseteq T$

$$X_{S,T} = \begin{cases} 1 & \Gamma(S) \subseteq T \\ 0 & \text{else} \end{cases} \qquad \Pr[X_{S,T}] = \left(\frac{t}{m}\right)^{sd}$$

$$\Pr\left[\bigcup_{S,T} X_{S,T}\right] \le \sum_{S,T} \Pr[X_{S,T}]$$

union bound

$$\le \sum_{s=1}^{\frac{n}{10d}} \binom{n}{s}\binom{m}{\frac{5}{8}sd}\left(\frac{\frac{5}{8}sd}{m}\right)^{sd}$$

$$\le \sum_{s=1}^{\frac{n}{10d}} \left(\frac{ne}{s}\right)^{s}\left(\frac{me}{\frac{5}{8}sd}\right)^{\frac{5}{8}ds}\left(\frac{\frac{5}{8}sd}{m}\right)^{sd}$$

$\binom{n}{k} \le \left(\frac{ne}{k}\right)^{k}$

$$\le \sum_{s=1}^{\frac{n}{10d}} \left(\frac{ne}{s}\right)^{s}\left(\frac{me}{\frac{5}{8}sd}\right)^{\frac{5}{8}ds}\left(\frac{\frac{5}{8}sd}{m}\right)^{\frac{3}{8}sd}$$

$\binom{k}{k} = \binom{\overline{k}}{k}$

Stirling's fla $\frac{k^k}{e^k} \le k!$

$$\le \sum_{s=1}^{\frac{n}{10d}} \left(\frac{ne}{s}\right)^s e^{5/8 ds} \left(\frac{5sd}{8m}\right)^{\frac{3}{8}sd}$$

$$\le \sum_{s=1}^{\frac{n}{10d}} \left(\frac{ne}{s}\right)^s \left(\frac{5sd}{8m}\right)^{s\frac{d}{16}} e^{5/8 sd} \left(\frac{5sd}{8m}\right)^{\frac{5}{16}sd}$$

$m \ge \frac{3}{4}n$
$s \le \frac{n}{10d}$ $\Rightarrow \frac{5sd}{8m} \le \frac{1}{12}$
$d \ge 32$

$$\le \sum_{s=1}^{\frac{n}{10d}} \left(\frac{45}{38}d\right)^s \left(\frac{5sd}{8m}\right)^{s\frac{d}{32}} \left(\frac{e^2}{12}\right)^{\frac{5}{16}sd}$$

$$\le \sum_{s\ge 1}^{n} \underbrace{\left(\frac{5}{12}\cdot d\right)^s \left(\frac{1}{12}\right)^{s\frac{d}{32}}}_{\le \left(\frac{5\cdot 32}{12^2}\right)^s} \underbrace{\left(\frac{e^2}{12}\right)^{\frac{5}{16}sd}}_{\le \left(\frac{1}{127}\right)^s}$$

$$\le \frac{1}{20^s}$$

$$\le \frac{1}{10}$$

(2) fails $\Rightarrow$ $\exists S, T$ $\quad \frac{n}{10d} \le |S| = s \le \frac{n}{2}$ $\quad |T| = t = s$

$\Gamma(S) \subseteq T$

$$\Pr[(2) \text{ fails}] \le \sum_{S,T} \left(\frac{t}{m}\right)^{sd} \le \sum_{s=n/10d}^{n/2} \binom{n}{s}\binom{M}{s}\left(\frac{s}{m}\right)^{sd}$$

$$\le \sum_{s\ge 1}^{n/2} \underbrace{\left[\left(\frac{ne}{s}\right)\left(\frac{me}{s}\right)\left(\frac{s}{m}\right)^d\right]^s}_{\ll \frac{1}{10000}}$$

$$\le \frac{1}{10}$$

$\Rightarrow \Pr[(1) \text{ or } (2) \text{ fails}] \le \frac{1}{10} + \frac{1}{10} \le \frac{1}{5}$

random G will satisfy (1) & (2) w.p. $\ge \frac{4}{5}$

G might have multiedges as we sampled neighbors

G might have multiedges as we sampled neighbors with replacement. If so redirect edges elsewhere (multi) which certainly doesn't hurt either (2) or (1). ∎

Michal Koucky v 17/10/2017 20:59

Using magic graphs

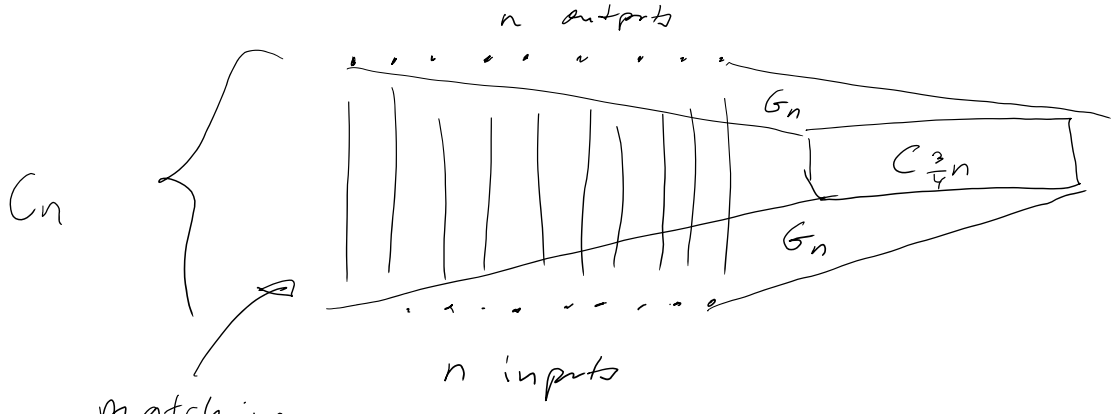
Superconcentrators with $O(n)$ edges

C_n ... n input vertices I, n output vertices O

s.t. $\forall S \subseteq I$, $\forall T \subseteq O$

if $|S| = |T|$ then $\exists$ $|S|$ vertex disjoint paths between S & T.

recursive construction



G_n $(n, \frac{3}{4}n, d)$-magical graph

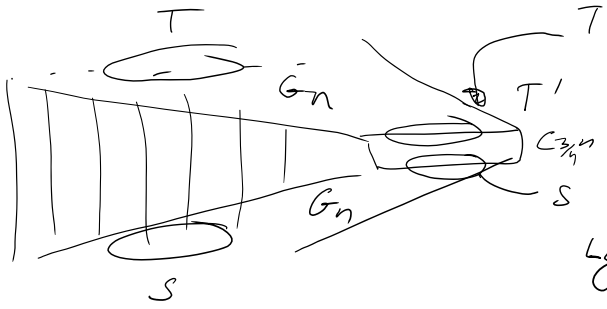
Claim: C_n is a superconcentrator.

Pf: Take any $S \subseteq I$, $T \subseteq O$, $|S| = |T|$.

Case 1: $|S| \leq \frac{n}{2}$.

By (2) of magical graph & using Hall's thm, there is a perfect matching in G_n

thm, there is a perfect matching between S and S' in $C_{\frac{4}{3}n}$



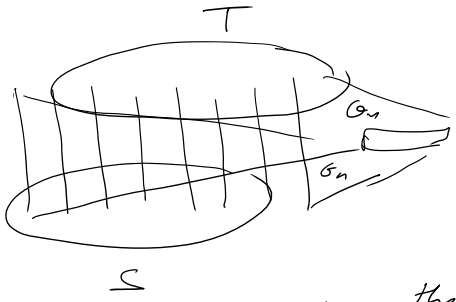
T' connected by a perfect matching to T

S connected by a perfect matching to S

similarly for T.

$C_{\frac{3}{4}n}$ connects S' to T' by vertex disjoint paths & we are done.

case 2: $|S| > \frac{n}{2}$



S & T overlap in $2|S|-n$ vertices that are directly connected by a matching

the # of unmatched vertices in S & T is $\leq \frac{n}{2}$

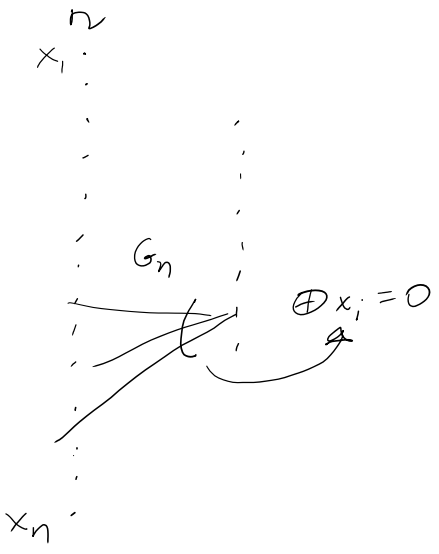
so we can connect them via $C_{\frac{3}{4}n}$ as in case 1. ∎

- The # of edges in C_n is $O(n)$!
  - $|C_n| \leq 2dn + n + |C_{\frac{3}{4}n}|$ if $n \geq n_0$
  - $|C_n| \leq n^2$ if $n \leq n_0$

$$\Rightarrow |C_n| \leq \underbrace{4(2\max(n_0, d) + 1)}_{\text{const.}} n$$

∎

Construction of error correcting codes with constant rate & constant relative distance



$(n, \frac{3}{4}n, d)$-magical graph G_n

$C = \{ x \in \{0,1\}^n$ s.t. the parity of neighbors of every right vertex is $0 \}$

Observations: • C is a linear code, i.e., $\forall x, y \in C$, $x+y \in C$

• $|C| \geq 2^{\frac{1}{4}n}$

• $\forall x \neq y \in C$, $\Delta_{Hamming}(x,y) \geq \frac{1}{10d} n$.

Pf: 1) trivial, 2) $\frac{3}{4}n$ homogeneous linear equations $\Rightarrow$ # of solutions $\geq 2^{n - \frac{3}{4}n}$.

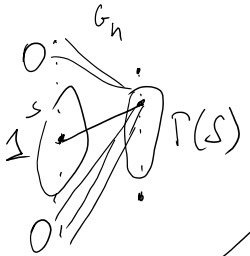
3) $\Delta_{Hamming}(x,y) = \Delta_{Hamming}(x+y, 0^n) =$ # 1's in $x+y$.

($x+y$: n-long non-zero vector)

Let S be the set of i s.t. $(x+y)_i = 1$.

If $|S| \leq \frac{n}{10d}$ then $\exists$ vertex v on the right side, $v \in \Gamma(S)$, s.t. v is connected to exactly one vertex in S.

Parity of neighbors of v is 1 so $x+y$ would not be in C contradicting (1).



would not be in C contradicting $y \in C$.

connecting every $v \in \Gamma(S)$ by ≥ 2 edges requires $\geq \frac{3}{2}d|S|$ edges.

$\Rightarrow |S| > \frac{n}{10d} \Rightarrow D_{Ham}(x,y) \geq \frac{n}{10d}$ ▨

- Codes of this type can be decoded in linear time by a simple iterative algorithm.

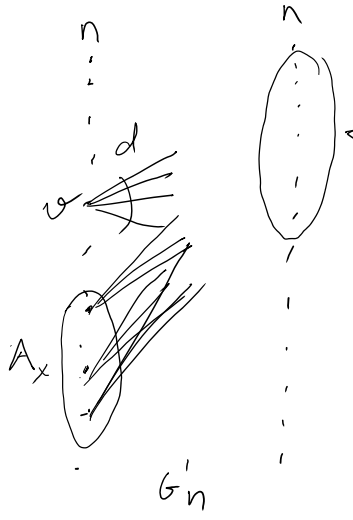
Error Amplification

alg. requires r random bits

$f(x,r) = 1$ $\forall r$ if x is prime

$f(x,r) = 1$ $\leq \frac{1}{16}$ of r's if x is not prime

set $n = 2^r$ & consider (n, n, d) - magical graph. G'_n



Bad random strings B_x for the alg. on input x

$|B_x| \leq \frac{n}{16}$.

$A_x = \{$vertices on left exclusively connected to vertices in $B_x\}$

i.e. $\Gamma(A_x) \subseteq B$.

error amplification:

pick a vertex v on the left in G_n & run the algorithm on random strings given by the neighbors of v. If all of them give $f(x,r) = 1$ say 1 o/w say 0.

Claim: $|A_x| \leq \frac{n}{10d}$

Pf: $|B_x| \geq |\Gamma(A_x)| > \left(\frac{5d}{8}\right) \cdot \frac{n}{10d} \geq \frac{n}{16}$ Contradiction w/ size of B ▨

Expanders

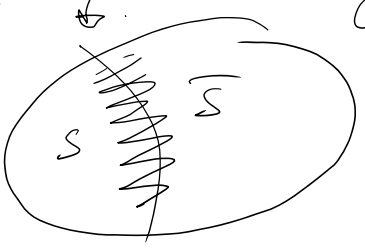
- from now on, graphs need not be bipartite, might have multiple edges & self-loops.

- $G = (V, E)$ $\quad S, T \subseteq V$

$E(S,T) = \{(u,v) \in E,\ u \in S,\ v \in T\}$

↑ set of directed edges, each undirected edge corresponds to two directed edges

- edge boundary $\partial(S) = E(S, \bar{S})$



- edge expansion of G:

$$h(G) = \min_{\substack{S \subseteq V \\ |S| \leq \frac{|V|}{2}}} \frac{E(S, \bar{S})}{|S|}$$

variant: vertex expansion

Def: a family of graphs $\{G_i\}_{i \in \mathbb{N}}$ where $|V(G_i)| > |V(G_{i-1})|$ is ε-edge expanders, $\varepsilon > 0$, if $\forall i$ $h(G_i) \geq \varepsilon$.

Want: "explicit" families of ε-edge expanders

↓

$\exists$ an algorithm on input n constructs G_n.

1) mildly explicit —"—

2) very explicit on input n & $v \in V(G_n)$ outputs neighbors of v in G_n.

... should be polynomial-time in

the algorithms should be polynomial-time in

n & $\log |G_n|$

↑ # of bits needed to specify v.

Examples:

1) $G_n = (V_n, E_n)$ $\quad V_n = \mathbb{Z}_n \times \mathbb{Z}_n$

$d = 4$ $\quad$ d-regular

$(x,y) \sim$ $(x+y, y)$, $(x, x+y)$, $(x-y, y)$, $(x, x-y)$

Margulis '73
Gabber-Galil '80

2) $G_p = (V_p, E_p)$ $\quad V_p = \mathbb{Z}_p$ $\quad p$ is a prime

$d = 3$

$x \sim x+1,\ x-1,\ x^{-1}$

· Lubotzky, Phillips, Sarnak '88

Spectrum of a graph

$A = A(G)$ ... $n \times n$ matrix $\quad A_{u,v} =$ # of edges between u & v.

A ... real, symmetric

Fact: Any real symmetric matrix of dimension $n \times n$ has n real eigenvalues $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n$ associated with orthonormal set of eigenvectors

A has n real eigenvalues

with orthonormal set of eigenvectors

$v_1, v_2, \dots v_n \in \mathbb{R}^n$.

$$\langle v_i, v_j \rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

$$A v_i = \lambda_i v_i$$

Claim:
- $\lambda_1 = d$, $\lambda_n \geq -d$
- $\lambda_2 \neq \lambda_1$ iff G is connected
- $\lambda_1 = -\lambda_n$ iff G is bipartite

(see HW)

Thm: $$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}$$

(left inequality: will see)

$d - \lambda_2$ ... eigenvalue gap

Michal Koucky v 24/10/2017 21:07

Pf: $\frac{d - \lambda_2}{2} \leq h(G)$

fact:

$$\lambda_1 = \max_{\|x\|_2 = 1} x_1^T A x_1$$

$$\lambda_2 = \max_{\|x_2\|_2} x_2^T A x_2$$

$x_2 \perp x_1$

$x_1, x_2, \dots$ orthogonal eigenvectors of A

$$\vdots$$

$$\lambda_n = \max_{\|x\|_2} x^T A x$$

$x \perp x_i \quad i = 1, \dots n-1$

eigenvector of A for $\lambda_1 = d$

$\Rightarrow$ it suffices to find $x \perp (1, 1, \dots 1)$ s.t.

$$\frac{x^T A x}{\|x\|^2} \geq d - 2h(G)$$

$$\frac{x^T A x}{\|x\|_2^2} \geq d - 2h(G)$$

since $\lambda_2 \geq \frac{x^T A x}{\|x\|_2^2}$

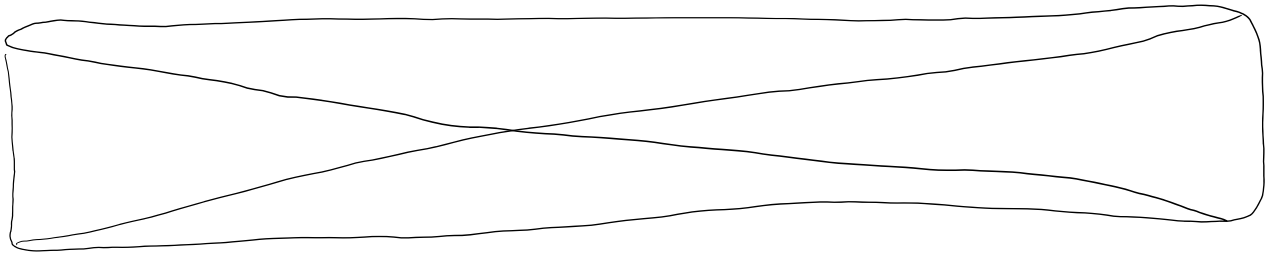
- Pick $S \subseteq V(G)$ s.t. $h(G) = \frac{|E(S,\bar{S})|}{|S|}$

define $x = \mathbb{1}_S \cdot |\bar{S}| - \mathbb{1}_{\bar{S}} |S|$

↑ characteristic vector of S $(0,0,1,0,\dots 1,0)$ — 1 at $\in S$

$x \perp (1,\dots 1) \Rightarrow \lambda_2 \geq \frac{x^T A x}{\|x\|_2^2}$

$$\|x\|_2^2 = |\bar{S}|^2 \cdot |S| + |S|^2 \cdot |\bar{S}| = |S| \cdot |\bar{S}| \cdot (|\bar{S}| + |S|) = n \cdot |S| \cdot |\bar{S}|$$



$$x^T A x = d\,|E(S)| \cdot |\bar{S}|^2 + d\,|E(\bar{S})| \cdot |S|^2 - 2\,|E(S,\bar{S})| \cdot |S| \cdot |\bar{S}|$$

$$= d \cdot |S| \cdot |\bar{S}|^2 - |E(S,\bar{S})| \cdot |\bar{S}|^2 +$$
$$d \cdot |\bar{S}| \cdot |S|^2 - |E(S,\bar{S})| \cdot |S|^2 +$$
$$- 2\,|S| \cdot |\bar{S}| \cdot |E(S,\bar{S})|$$

$$= d \cdot |S| \cdot |\bar{S}| \cdot n - \left(|S| + |\bar{S}|\right)^2 \cdot |E(S,\bar{S})|$$

$$= d \cdot |S| \cdot |\bar{S}| \cdot n - n^2 \cdot |E(S,\bar{S})|$$

$$\Rightarrow \lambda_2 \geq \frac{x^T A x}{\|x\|_2^2} = d - \frac{n}{|S| \cdot (n - |S|)} \cdot |E(S,\bar{S})|$$

$$\geq d - 2\,\frac{|E(S,\bar{S})|}{|S|} = d - 2h(G)$$

□

$= d - \lambda \frac{}{|S|} - d - \lambda \cdot u(0)$

Expander mixing lemma

thm: $\forall$ d-regular G, $\lambda(G) = \max(|\lambda_2|, |\lambda_n|)$

$\forall S, T \subseteq V(G)$

$$\left| E(S,T) - \frac{d\,|S| \cdot |T|}{n} \right| \leq \lambda \sqrt{|S| \cdot |T|}$$

Pf: $v_1, v_2, \dots v_n$ ... orthonormal eigenvectors of $A(G)$
$\lambda_1, \dots \lambda_n$ eigenvalues of $A(G)$

let χ_S, χ_T ... characteristic vectors of $S \subseteq T$

$$\chi_S = \sum_{i=1}^{n} \alpha_i v_i \qquad \chi_T = \sum_{i=1}^{n} \beta_i v_i$$

$$|E(S,T)| = \chi_S^T A \chi_T$$
$$= \left(\sum_{i=1}^{n} \alpha_i v_i \right)^T A \sum_{i=1}^{n} \beta_i v_i$$
$$= \sum_{i=1}^{n} \alpha_i \beta_i \lambda_i$$

$$\alpha_0 = \left\langle \chi_S, \underbrace{\frac{\mathbb{1}}{\sqrt{n}}}_{v_1} \right\rangle = \frac{|S|}{\sqrt{n}} \qquad \beta_0 = \frac{|T|}{\sqrt{n}}$$

$$\Rightarrow |E(S,T)| = \lambda_1 \frac{|S| \cdot |T|}{n} + \sum_{i=2}^{n} \lambda_i \beta_i \alpha_i$$

$$= d \frac{|S| \cdot |T|}{n} + \sum_{i=2}^{n} \lambda_i \beta_i \alpha_i$$

$$\Rightarrow \left| |E(S,T)| - \frac{d\,|S| \cdot |T|}{n} \right| = \left| \sum_{i=2}^{n} \lambda_i \beta_i \alpha_i \right|$$
$$\leq \sum_{i=2}^{n} |\lambda_i \beta_i \alpha_i| \leq \lambda \sum_{i=2}^{n} |\beta_i| \cdot |\alpha_i|$$
$$\leq \lambda \sqrt{\sum_{i=2}^{n} \beta_i^2 \cdot \sum_{i=2}^{n} \alpha_i^2}$$

$$\le \lambda \sqrt{\sum_{i=2}^{n} \beta_i^2 \cdot \sum_{i=2}^{n} \alpha_i^2}$$

$$\le \lambda \sqrt{|S| \cdot |T|}$$

∎

- a d-regular graph on n vertices is (n,d)-graph.
  an (n,d)-graph with $\lambda \le \alpha d$ is (n,d,α)-graph.

Ex:

- the maximum independent set of (n,d,α)-graph has size at most αn

– indeed, $|E(S,S)| = 0$ exp. mixing

S independent set of G

$$\Rightarrow \left| d \frac{|S|^2}{n} \right| \le \lambda \cdot |S| \le \alpha d |S|$$

$$\Rightarrow |S| \le \alpha n$$

∎

$\Rightarrow$ the chromatic number $\ge \frac{1}{\alpha}$.

- Sampling $(v,d) \in V \times d$ instead of $(v,u) \in U^2$.

thm: $\lambda \ge 2\sqrt{d-1} - o_n(1)$

a weaker statement: $\lambda \ge \sqrt{d}\,(1 - o_n(1))$

Pf: $\operatorname{trace}(M) = \sum_{i=1}^{n} M_{ii} = \sum \lambda_i$

M ... matrix

Fact

$\operatorname{trace}(A^2) \ge dn$ (easy)

$\operatorname{trace}(A^2) = \sum \lambda_i^2 \le d^2 + (n-1)\lambda^2$

λ_i^2 ... eigenvalues of A^2

$$\Rightarrow dn \le d^2 + (n-1)\lambda^2$$

$$\Rightarrow \lambda^2 \ge d\,\frac{n-d}{n-1}$$

∎

$$\Rightarrow \lambda^2 \geq d\,\frac{n-d}{n-1}$$

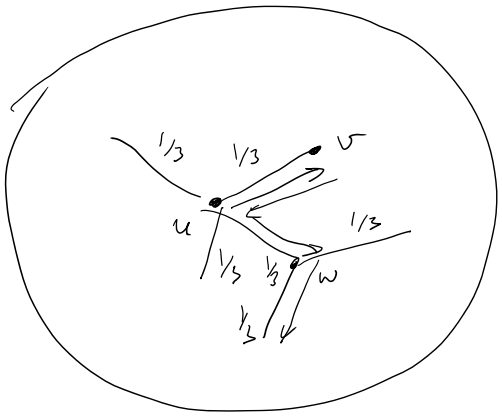
Michal Koucky v 14/11/2017 16:14

Random walk on a graph

$\|x\|_1 = \sum |x_i|$

$\|x\|_2 = \sqrt{\sum x_i^2}$

$\|x\|_\infty = \max_i |x_i|$



at the current vertex pick a neighbor uniformly at random & move to that neighbor

$\tilde{A} = \frac{1}{d} A$ ... normalized adjacency matrix of a d-reg. graph G, (n,d,λ)-graph

$p^0 = (p_1, \dots p_n)$ ... probability distribution on vertices

$\sum p_i = 1 \qquad p_i \geq 0$

- $\tilde{A} p^0 = p^1$ ... distribution after one step of the walk
- $\tilde{A}^t p^0 = p^t$ ... distribution after t steps of the walk

Claim: $\tilde{A}^t p^0 \xrightarrow[t\to\infty]{} \pi$ ... a stationary distribution s.t. $A\pi = \pi$

clearly $\pi = (\frac{1}{n}, \frac{1}{n}, \dots \frac{1}{n})$ for d-regular graphs

Pf: $\|\tilde{A}p - \pi\|_2 = \|\tilde{A}p - \tilde{A}\pi\|_2 = \|\tilde{A}(p-\pi)\|_2$

$= v$

$v \perp \pi = \langle v, \pi \rangle = \langle p-\pi, \pi \rangle = \frac{1}{n} - \frac{1}{n} = 0$

Let $v_1, v_2, \dots v_n$ be orthonormal basis of $\tilde{A}$

$\lambda_1 \quad \lambda_2 \quad \dots \quad \lambda_n$

Let $v_1, v_2, \dots v_n$ be orthonormal basis of A

$\lambda_1 \geq \dots \geq \lambda_n$

$v_1 = \pi$

$\Rightarrow \quad v = \sum_{i=2}^{n} \alpha_i v_i$

$\tilde{A} v = \sum_{i=2}^{n} \lambda_i v_i \alpha_i$

$$\| \tilde{A} v \|_2 \leq \sqrt{\langle (\tilde{A} v)^T \tilde{A} v \rangle} = \sqrt{\left\langle \sum_{i=2}^{n} \lambda_i \alpha_i v_i^T \sum_{i=2}^{n} \alpha_i v_i \lambda_i \right\rangle} =$$

$$= \sqrt{\sum_{i=2}^{n} \lambda_i^2 \alpha_i^2} \leq \max_{i \in \{2,\dots n\}} \lambda_i \sqrt{\sum \alpha_i^2} = \lambda \cdot \|v\|$$

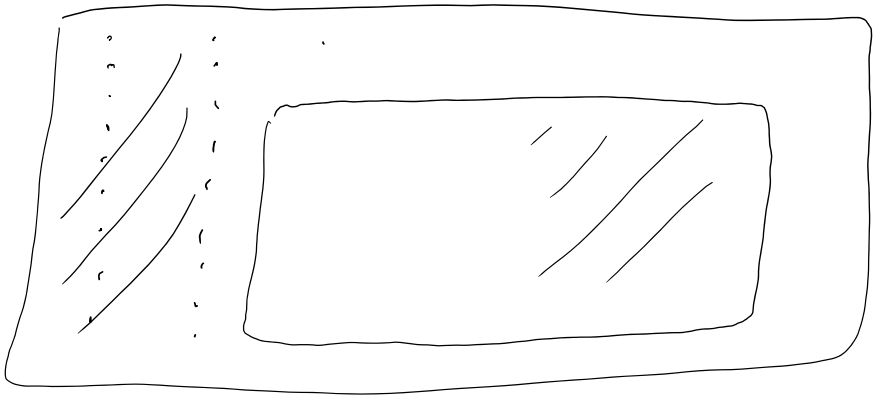
$\lambda_1 = 1 \qquad \lambda = \max\{|\alpha_2|, |\alpha_n|\}$

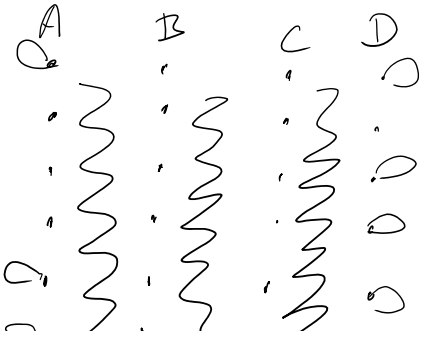
$\rightarrow \quad \| \tilde{A} p - \pi \|_2 \leq \lambda \| p - \pi \|_2$

$\rightarrow \quad \| \tilde{A}^t p - \pi \|_2 \leq \lambda^t \| p - \pi \|_2$

$\lambda < \lambda_1 = 1 \quad \Rightarrow \quad \tilde{A}^t p \to \pi$ ∎

Ex: $\| \tilde{A} p - \pi \|_1 = \| p - \pi \|_1$ in l_1-norm the difference might not shrink





expander, consisting of 4 parts, self-loops long white

$n \quad n \quad n \quad n$

very where p

Vertices in B, C get prob. $\frac{1}{4n}$

A $\frac{1}{4n} + \varepsilon$

D $\frac{1}{4n} - \varepsilon$

$\| p - \pi \| = 2n\varepsilon \qquad \| \hat{A} p - \pi \| = 2n\varepsilon$ ▨

since $\| \tilde{A}^t p - \pi \|_2 \leq \lambda^t \cdot 2$, after $O(\lg n)$ steps

$\| \tilde{A}^t p - \pi \|_2 \leq \frac{1}{e}$

... time $O(\lg n)$

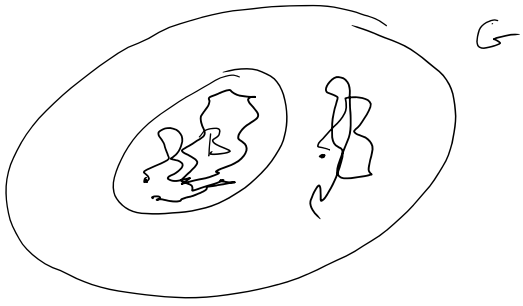
<u>Claim</u>: $\| \tilde{A}^t p - \pi \|_1 \leq 2\sqrt{n} \cdot \lambda^t$

<u>Pf</u>: $\|x\|_1 = \sum_i |x_i| \leq \sqrt{\sum_i x_i^2 \cdot \sum_i 1^2} \leq \sqrt{n} \cdot \sqrt{\sum_i x_i^2} = \sqrt{n}\, \|x\|_2$ ▨

(↑ Cauchy-Schwarz)

$G = (V, E)$ (n, d, λ)- graph

pick $B \subseteq V$ $|B| = \beta n$



Start a random walk from a random vertex.

What's the probability we stay in B for t steps?

(B, t) ... event that the walk stays in B for t steps.

<u>Thm</u>: $\Pr[(B, t)] \leq (\beta + \lambda)^t$

<u>Pf</u>: Set $P_B = \begin{pmatrix} 0 & & \\ & \boxed{1,1,0} & \\ & & 0 \end{pmatrix} B$ i.e. $(P_B)_{ij} = \begin{cases} 1 & i=j \in B \\ 0 & \text{o/w} \end{cases}$

Pf: Set $P_B = \begin{pmatrix} 0 & & \\ & \boxed{1,1,0} & \\ & & 0 \end{pmatrix}_B$ i.e. $(P_B)_{ij} = \begin{cases} 1 & i=j \le B \\ 0 & \text{o/w} \end{cases}$

$\tilde{A}$ ... normalized adjacency matrix of G

Claim: $\Pr[(B,t)] = \left\| \left(P_B \tilde{A}\right)^t P_B u \right\|_1$

Pf: trio. (M)

↳ P_B zeroes out entries not in B in any vector.

Claim: $\| P_B \tilde{A} P_B v \|_2 \le (\beta + \alpha) \cdot \|v\|_2 \quad \forall v \in \mathbb{R}^n$

Pf: w.l.o.g v is supported only on entries in B

(this would only decrease the right-hand side

& $P_B (P_B v) = P_B v$)

w.l.o.g $v \ge 0$ (doesn't change R.H.S & may increase LHS)

w.l.o.g $\sum v_i = 1$ (by linearity)

$v = u + z$ where $u = (\frac{1}{n}, \frac{1}{n}, \dots \frac{1}{n})$

& z is orthogonal to u. $(z = v - u.)$

$$P_B \tilde{A} P_B v = P_B \tilde{A} v = P_B \tilde{A} u + P_B \tilde{A} z = P_B u + P_B \tilde{A} z$$

$$\| P_B \tilde{A} P_B v \|_2 \le \| P_B u \|_2 + \| P_B \tilde{A} z \|_2$$

enough to show: $\| P_B u \|_2 \le \beta \cdot \|v\|_2$ and $\| P_B \tilde{A} z \|_2 \le \lambda \|v\|_2$ $\Rightarrow$ claim

Since $\sum v_i = 1$ & support of v has $\le \beta n$ coordinates

Since $\sum v_i = 1$ & support of v has $\leq \beta n$ coordinates

by cauchy-Schwarz $\quad 1 = \sum v_i \leq \sqrt{\beta n}\, \|v\|_2$.

Also $\|P_B u\|_2 = \sqrt{\beta/n}$ $\Rightarrow$ $\|P_B u\|_2 \leq \sqrt{\frac{\beta}{n}}\sqrt{\beta n}\,\|v\|_2 = \beta\|v\|_2$

- $\|P_B \widetilde{A} z\|_2 \leq \|\widetilde{A} z\|_2 \leq \lambda \|z\|_2$ as $z \perp u$.

Also $\|z\|_2 \leq \|z+u\|_2 = \|v\|_2$

$z \perp u$ $\quad \langle z+u, z+u\rangle = \langle z,z\rangle + \langle u,u\rangle$

Thus: $\left\| \left(P_B \widetilde{A}\right)^t P_B u \right\|_1 \leq \sqrt{n}\, \left\| \left(P_B \widetilde{A}\right)^t P_B u \right\|_2$

$= \sqrt{n}\, \left\| \left(P_B \widetilde{A} P_B\right)^t u \right\|_2$

$\leq \sqrt{n}\, (\beta+\lambda)^t \|u\|_2$

$= (\beta+\lambda)^t$

For uniformly chosen $t+1$ vertices, the probability of falling into B is β^{t+1}. For vertices generated by the walk it is at most $(\beta+\lambda)^t$.

Thm [Alon-Feige-Wigderson-Zuckerman]
If $\beta \geq 6\lambda$ then $\beta\cdot(\beta-2\lambda)^t \leq \Pr[(B,t)] \leq \beta(\beta+2\lambda)^t$

(no proof)

Thm: $\forall K \subseteq \{0,\dots t\}$ & $\forall B \subseteq V$ $\quad |B| = \beta n$

$\Pr[X_i \in B \quad \forall i \in K] \leq (\beta+\lambda)^{|K|-1}$

where $X_0, X_1 \dots X_t$ is the random walk

where $X_0, X_1 \dots X_t$ is the random

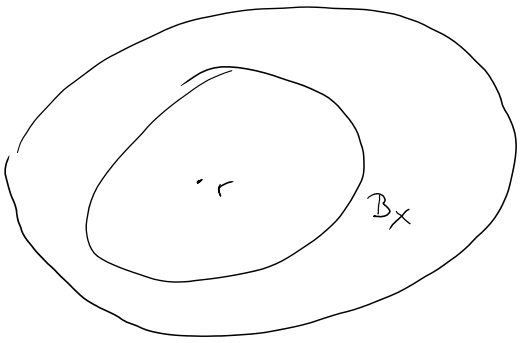
Error amplification

- randomized alg A

$A(x, r)$ — e.g. poly-time alg.

- input of length n
- random bits $\ell = \text{poly}(n)$

$x \in \{0,1\}^n$



$B_x = \{ r \in \{0,1\}^\ell, A(x,r) \text{ gives incorrect answer} \}$

$$\Pr_r [A(x,r) \text{ gives incorrect answer}] = \frac{|B_x|}{2^\ell}$$

want: $\forall x \quad \Pr_r [A(x,r) \text{ is incorrect}] \leq \varepsilon$

$0 \leq \varepsilon < \frac{1}{2}$ say ε is a constant

Error amplification A'

1) pick $r_1, r_2, \dots r_k$ independently at random
2) run $A(x, r_i)$, for $i = 1, \dots, k$
   output the majority answer

- If $\varepsilon < \frac{1}{2}$ is constant
  then A' has probability of error $\leq 2^{-O(k)}$
  (depends on ε)

then A' has probability of error $\leq 2^{-\Omega(k)}$ ↑ depends on ε

- similar amplification works even for $\varepsilon \approx \frac{1}{2} - \frac{1}{\mathrm{poly}(n)}$.

A' requires $\ell \cdot k$ random bits

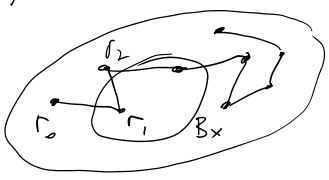
Q: Can we save random bits?

YES - using expander walks.

Pick a $(2^\ell, d, \lambda)$-graph. (The graph is unrelated to either A or x.)

In step 1) of A', pick A_1 at random and each successive A_{i+1} pick as a random neighbor of A_i.

continue with A' as before.



→ needs only $\ell + O(k)$ random bits

Say $\varepsilon < \frac{1}{10}$ (which can be achieved by amplifying A $O(1)$ times.)

$\lambda \leq \frac{1}{10}$ by our choice

- A makes an error on x if $> k/2$ steps of the random walk stay in B_x.

For given subset $K \subseteq \{1, \dots k\}$

$$\Pr\left[\forall i \in K,\ r_i \in B_x\right] \leq (\varepsilon + \lambda)^{|K|-1}$$

$$\Rightarrow \Pr\left[A \text{ is incorrect on } x\right] \leq \sum_{\substack{K \subseteq \{1,\dots k\} \\ |K| \geq k/2}} (\varepsilon+\lambda)^{|K|-1}$$

$$\leq 2^k \cdot \left(\frac{1}{5}\right)^{k/2-1}$$

$= 2^{-\Omega(k)}$

$$\leq 2^{k} \cdot \left(\frac{1}{5}\right)^{k/2}$$

$$\leq \left(\frac{4}{5}\right)^{k/2-1} \leq 2^{-O(k)}$$ ☐

Hardness of approximation

MAX-CLIQUE PROBLEM

Input: G ... graph on n vertices

Output: the size of the largest clique in G ... $\omega(G)$

Fact: MAX-CLIQUE is NP-hard [well known]

Q: Can we at least approximate the size of the largest clique?

No, unless $P = NP$

Thm [Feige - Goldwasser - Lovász - Safra - Szegedy]

There are constants $1 > \delta_1 > \delta_2 > 0$ s.t.
it is NP-hard to decide whether the largest clique $\omega(G)$ satisfies $\omega(G) \geq \delta_1 n$ or $\omega(G) \leq \delta_2 n$.

Note: If one could approximate $\omega(G)$ within a factor δ_1/δ_2 then we could decide.

Thm: There is $\varepsilon > 0$ s.t. if there is a poly-time algorithm A that on input G of size n outputs # s.t. $n^{-\varepsilon} \leq A(G)/\omega(G) \leq n^{\varepsilon}$ then $P = NP$.

Pf: first we present a probabilistic reduction which we will derandomize using expander walks.
(later)

$H = (V^t, E')$ $t = \log n$

Exer

Given $G=(V,E)$ define $H=(V^t, E')$ $t=\log n$

where $(v_1,\dots v_t) \sim_H (u_1,\dots u_t)$

iff $\{v_1,\dots v_t, u_1,\dots u_t\}$ is a clique in G

Claim: Every clique in H is a subgraph of S^t for some $S \subseteq V$, S is a clique of G.

Hence $\omega(H) = \omega(G)^t$.

Pf: If S is a clique in G then S^t is a clique in H so $\omega(H) \geq \omega(G)^t$.

If S' is a clique in H, then the union of the entries of G appearing in S' forms a clique in G. Hence $|S'| \leq |S|^t \Rightarrow \omega(G)^t \geq \omega(H)$. ∎

Alg on G

1) Pick a random subset of $V(H)=V^t$ of size $m=\text{poly}(n)$. and the induced subgraph H' on that subset of H

2) Run alg A on H'. If it outputs $\# > \frac{1}{2}\delta_1^t m$, then return 1 o/w return 0.

For correctness of this algorithm we want to show that:

a) If $\omega(G) \geq \delta_1 n$ then w.h.p. $\omega(H') \geq \frac{1}{2}\delta_1^t m$.

b) If $\omega(G) \leq \delta_2 n$ then w.h.p. $\omega(H') \leq 2\delta_2^t m$.

This proves the lemma for a right choice of $m=\text{poly}(n)$, $t=\log n$.

$\omega(G) \geq \delta_1 n \Rightarrow \omega(H) \geq (\delta_1 n)^t$

$\Rightarrow \omega(G) \geq \delta_1 n \Rightarrow \omega(H) \geq (\delta_1 n)^t$

Let S be a clique from H of maximum size.

The expected number of vertices from S that are in H' is $|S| \cdot \frac{V(H')}{V(H)} \geq \delta_1^t n^t \frac{n}{n^t} = \delta_1^t n$.

By the Chernoff bound this is at least $\frac{1}{2}\delta_1^t n$ with probability $\geq 1 - 2e^{-\frac{\delta_1^t n}{12}}$.

Each clique in H' is a subclique of S^t for some clique S in G. Each $|S| \leq \delta_2 n$ so $|S^t| \leq (\delta_2 n)^t$. The expected # of vertices from S^t in H' is $\leq \delta_2^t n^t \cdot \frac{n}{n^t} = \delta_2^t n$.

The probability that $\geq 2\delta_2^t n$ vertices of S^t are in H' is by the Chernoff bound $\leq 2e^{-\delta_2^t n/3}$.

There are $\leq 2^n$ sets (cliques) S in G so the probability of any of them creating clique of size $\geq 2\delta_2^t n$ in H' is $\leq 2^n \cdot 2e^{-\delta_2^t n/3} < \frac{1}{10}$

for n large enough polynomial of n.

(Note, even if S is smaller than $\delta_2^t n$, we can add "fake" elements to S to be of size $= \delta_2^t n$, take the subset & remove from it the "fake" elements. Hence we can apply the Chernoff bound as if S were exactly of size $\delta_2^t n$.)

• deterministic construction

- take an (n, d, λ)-graph G'. As the vertex set V' of H' we take the set of random walks of length $t-1$ on G':

$$V' = \{(u_1, u_2, \dots u_t) \in V(H);\ u_1 \text{ is arbitrary}, * \text{ for } i > 1,\ u_i \text{ is connected by an edge to } u_{i-1} \text{ in } G'\}$$

$m = |V'| = n \cdot d^{t-1}$ as G' is d-regular on n vertices

vertices in V' correspond to random walks on G' of length $t-1$.

- H' is the induced subgraph of H on V'.

Claim: If $\omega(G) \le \delta_2 n$ then $\omega(H') \le (\delta_2 + 2\lambda)^t m$.

Pf: A clique in H' corresponds to random walks on G' that are confined to a vertex set of G which is a clique.

The probability that random walks stay in a set of size $\le \delta_2 n$ is at most $(\delta_2 + 2\lambda)^t$.

So the # of such walks is $\le m \cdot (\delta_2 + 2\lambda)^t$ ☐

Claim: If $\omega(G) \ge \delta_1 n$ then $\omega(H') \ge (\delta_1 - 2\lambda)^t m$.

Pf: As above, the probability of a random walk on G' to stay within a clique S of G, $|S| \ge \delta_2 n$, is at least $(\delta_1 - 2\lambda)^t$, so the # of walks staying in S is $\ge (\delta_1 - 2\lambda)^t m$ ☐

Construction of expanders

- iterative construction using graph operations

Goal: construct a sequence of graphs

$G_0, G_1, G_2, \ldots$

where G_i is (n_i, d, λ)-graph

for some fixed d & λ & $n_i > n_{i-1}$.

- we will start from G_0 to be some fixed (n_0, d, λ)-graph for suitable d & λ.
- we will apply on G_i certain graph operations to get G_{i+1}

- **graph squaring**

$\tilde{A}$ is the normalized adjacency matrix of (n, d, λ)-graph G

$\rightarrow \tilde{A}^2$ is the —"— of (n, d^2, λ^2)-graph

in general $\tilde{A}^t \rightarrow (n, d^t, \lambda^t)$-graph

$(\tilde{A}^t)_{i,j}$ = prob of going from vertex i to j in G by a random walk.

$\tilde{A}^2$ corresponds to a graph with the same vertices as G where edges represent paths of length 2 in G.

(we allow multiple edges & self-loops)

graph squaring improves the expansion $\lambda \rightarrow \lambda^2$ but increases degree $d \rightarrow d^2$.

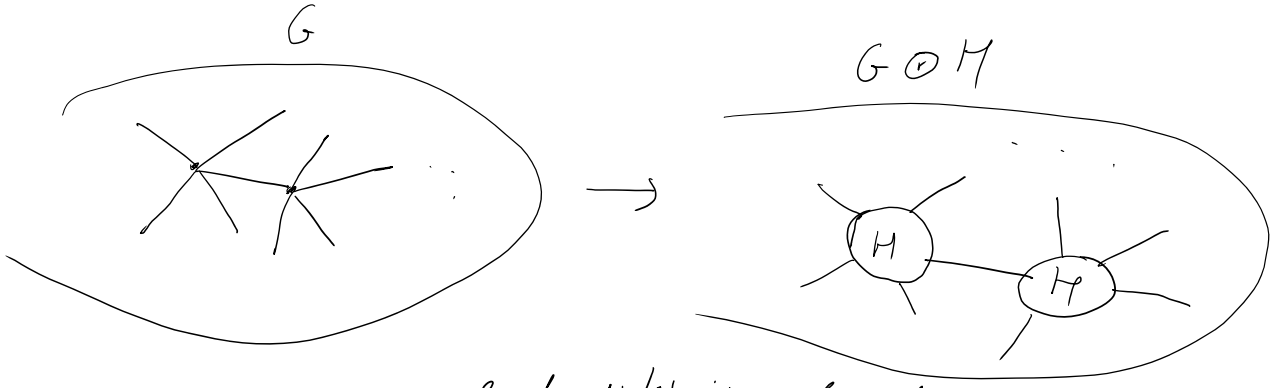
but increases degree $d \to d^2$.

- graph replacement

(n, D, α)-graph
G

(D, d, β)-graph
H

$G \textcircled{r} H$ ... $(nD, d+1, ?)$-graph



each vertex is replaced by a copy of H $\to nD$ vertices

edges of $G \textcircled{r} H$ are the internal edges of H & the external edges between clouds corresp. to vertices connected in G.

$\lambda(G \textcircled{r} H)$ depends on $\lambda(G)$ & $\lambda(H)$, better depending gives zig-zag product.

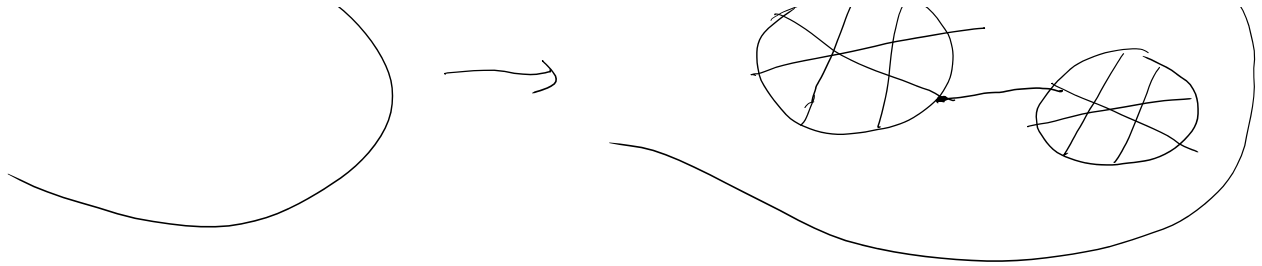
- zig-zag product

(n, D, α)
G

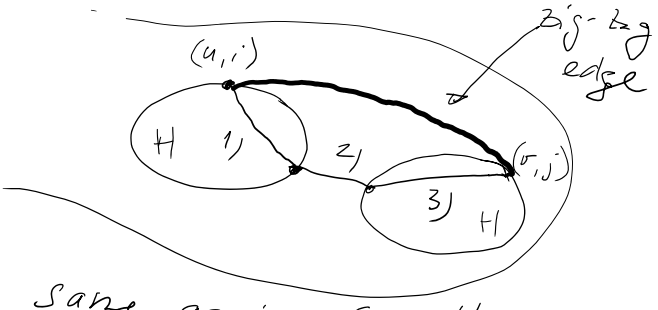
(D, d, β)
H

$\downarrow$

$G \textcircled{z} H$ $(nD, d^2, ?)$



$G \textcircled{z} H$



$(u,i) \sim_{G \textcircled{z} H} (v,j)$

- Vertices in $G \textcircled{z} H$ same as in $G \textcircled{r} H$
- but edges correspond to paths of length 3 in $G \textcircled{r} H$ where the first step is internal in H, the second is external step between clouds & the third is an internal step in H.

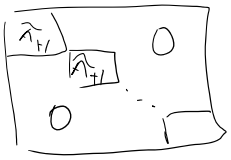
uniquely determined by the current vertex

d choices
$\Rightarrow d^2$ degree in $G \textcircled{z} H$

$$\widetilde{A}_{G \textcircled{z} H} = B A B$$

where $$B((u,i),(v,j)) = \begin{cases} 0 & \text{if } u \neq v \\ \widetilde{A}_H & \text{if } u = v \end{cases}$$

i.e. $B = I \otimes \widetilde{A}_H$.



$$A((u,i),(v,j)) = \begin{cases} 1 & \text{if } v \text{ is the } i\text{th neighbor of } u \\ & \text{\& } u \text{ is the } j\text{th neighbor of } v \\ 0 & \text{o/w.} \end{cases}$$

Thus, A is a permutation matrix.

claim: $\lambda(G \textcircled{z} H) \leq \lambda(G) + 2\lambda(H) + \lambda(H)^2$

$(\alpha + 2\beta + \beta^2)$

- using the claim to construct G_{i+1} from G_i:

$$G_{i+1} = \left(G_i^2\right) \textcircled{z} H$$

where G_i is $(n_i, d^2, \frac{1}{2})$-graph
H is $(d^4, d, \frac{1}{10})$-graph

$$\lambda(G_{i+1}) \leq \frac{1}{4} + \frac{2}{10} + \frac{1}{10^2} < \frac{1}{2}$$

$$n_i = n_0 d^{4i}$$

We need to prove the claim.

Recall: $\lambda(M) = \max_{\substack{x \in \mathbb{R}^n \\ x \perp \mathbb{1}}} \frac{\|Mx\|_2}{\|x\|_2} = \max_{\substack{x \in \mathbb{R}^n \\ x \perp \mathbb{1} \\ \|x\|_2 = 1}} \|Mx\|_2$

For $M \in \mathbb{R}^{n \times n}$
doubly stochastic
symmetric

Def.: spectral norm of a matrix $M \in \mathbb{R}^{n \times n}$

$$\|M\| = \max_{\substack{x \in \mathbb{R}^n \\ \|x\|_2 = 1}} \|Mx\|_2$$

Note: if M is symmetric with eigenvalues $\lambda_1, \lambda_2, \dots \lambda_n$,
then $\|M\| = \max_i |\lambda_i|$.

Properties: $\forall A, B \in \mathbb{R}^{n \times n}$

1) $\|A + B\| \leq \|A\| + \|B\|$
2) $\|\alpha A\| \leq |\alpha| \cdot \|A\|$ $\quad \forall \alpha \in \mathbb{R}$
3) $\|A \cdot B\| \leq \|A\| \cdot \|B\|$

Pf: 1), 2) trivial
3) $\forall x \in \mathbb{R}^n$ $\quad \|A \cdot \underbrace{B \cdot x}_{y}\|_2 \leq \|A\| \cdot \|\underbrace{Bx}_{y}\|_2 \leq \|A\| \cdot \|B\| \cdot \|x\|_2$ □

Lemma: Let G be a d-regular graph on n vertices & $\widetilde{A_G}$ be its normalized adjacency matrix.

Thm: $\lambda(G) = \| \widetilde{A_G} - \frac{1}{n} J \|$

(J ... all-one $n \times n$ matrix)

Pf: Let $\lambda_1 \geq \lambda_2 \dots \lambda_n$ be the eigenvalues of $\widetilde{A_G}$

$\lambda_1 = 1$

$v_1, v_2, \dots v_n$ be the orthonormal eigenbasis

$v_1 = \frac{1}{\sqrt{n}} \mathbb{1}$

s.t. $M = \widetilde{A_G}$

$$\left(M - \tfrac{1}{n} J\right) v_1 = M v_1 - \tfrac{1}{n} J v_1 = v_1 - \tfrac{1}{n} \tfrac{n}{\sqrt{n}} \mathbb{1} = 0$$

($\tfrac{1}{n} \tfrac{n}{\sqrt{n}} \mathbb{1} = v_1$)

for $i > 1$ $\left(M - \frac{1}{n} J\right) v_i = M v_i - \frac{1}{n} J v_i = M v_i = \lambda_i v_i$

($\frac{1}{n} J v_i = 0$ as $\langle \mathbb{1}, v_i \rangle = \langle v_1, v_i \rangle = 0$)

$\Rightarrow$ $\left(M - \frac{1}{n} J\right)$ has eigenvalues $0, \lambda_2, \dots \lambda_n$

& eigenbasis $v_1, v_2, \dots v_n$.

$$\| M - \tfrac{1}{n} J \| = \max_{i>1} \{ |\lambda_i|, 0 \} = \lambda(G). \qquad \square$$

($M - \frac{1}{n} J$ is real symmetric)

Lemma: G ... (n, D, α)-graph H ... (D, d, β)-graph

then $\lambda(G \circledcirc H) \leq \alpha^2 + 2\beta + \beta^2$.

Pf: Let $\widetilde{A_{G \circledcirc H}}$ be the normalized adjacency matrix of $G \circledcirc H$.

Recall $\widetilde{A_{G \circledcirc H}} = B A B$

A is a permutation matrix

$B = I \otimes \widetilde{A_H}$.

Let $E = \widetilde{A}_H - \frac{1}{D} J$

So $B = \underbrace{I \otimes \frac{1}{D} J}_{\overline{J}} + \underbrace{I \otimes E}_{\overline{E}}$

Denote

Thus $BAB = (\overline{J} + \overline{E}) A (\overline{J} + \overline{E})$

$= \overline{J}A\overline{J} + \overline{J}A\overline{E} + \overline{E}A\overline{J} + \overline{E}A\overline{E}$

$$\lambda(G \circledast H) = \max_{\substack{x \in \mathbb{R}^{nD} \\ \|x\|_2 = 1 \\ x \perp \mathbb{1}}} \| \widetilde{A}_{G \circledast H} x \|_2$$

$$\| \widetilde{A}_{G \circledast H} x \|_2 = \| BAB x \|_2 \le \|\overline{J}A\overline{J}x\|_2 + \|\overline{J}A\overline{E}x\|_2 + \|\overline{E}A\overline{J}x\|_2 + \|\overline{E}A\overline{E}x\|_2$$

$$\le \|\overline{J}A\overline{J}x\|_2 + \|\overline{J}A\overline{E}\| + \|\overline{E}A\overline{J}\| + \|\overline{E}A\overline{E}\|$$

we will bound $\|\overline{J}A\overline{J}x\| \le \alpha$

$\|\overline{E}\| \le \beta$

then $\| \widetilde{A}_{G \circledast H} x \| \le \alpha + \|\overline{J}A\overline{E}\| + \|\overline{E}A\overline{J}\| + \|\overline{E}A\overline{E}\|$

$\le \|E\| \le \|\overline{E}\| \le \|\overline{E}\|^2$

$\le \beta \le \beta \le \beta^2$

$\le \alpha + 2\beta + \beta^2$

Take any $z \in \mathbb{R}^{nD}$ $\quad z = (\underbrace{z_1 \dots z_D}_{z_1}, \underbrace{z_{D+1} \dots z_{2D}}_{z_2}, \dots, \underbrace{\dots z_{nD}}_{z_n})$

$$\|\overline{E} \cdot z\|_2^2 = \| I \otimes E \cdot z \|_2^2 = \sum_{i=1}^{n} \|E \overline{z}_i\|_2^2 \le \sum_i \|E\|^2 \cdot \|\overline{z}_i\|_2^2$$

$$= \|E\|^2 \cdot \|z\|_2^2$$

$$\Rightarrow \quad \| I \otimes E \| \le \|E\| = \lambda(\widetilde{A}_H) \le \beta . \quad \checkmark$$

$\overline{J}A\overline{J} = \widetilde{A}_G \otimes \frac{1}{D} J$ sum row $\overline{J}A\overline{J}$ acts on $(0,0,\dots 1,0,0\dots)$ $(u,:)$

let $x = (x_1 \dots x_D, x_{D+1}, \dots x_{2D}, \dots \quad x_{nD})$

$\overline{x_1}$ $\overline{x_2}$ $\cdots$ $\overline{x_n}$

Let $y_u = \sum_{i=1}^{D} \frac{x_{u,i}}{D}$

$$\|y_u\|_2^2 = \sum \left(\sum \frac{1}{D} \cdot x_{u,i}\right)^2 \le \sum_u \left(\sum \frac{1}{D^2}\right) \cdot \left(\sum x_{u,i}^2\right) = \frac{1}{D} \|x\|_2^2$$

$$\|\bar{J} A \bar{J} x\|_2^2 = \left\| \left(\tilde{A}_G \otimes \frac{1}{D} J\right) x \right\|_2^2$$

$$= \sum_{u,i} \left(\sum_{v,j} \frac{1}{D} \left(\tilde{A}_G\right)_{v,u} x_{u,i} \right)^2 \qquad u \sim v$$

$$= \sum_{u,i} \left(\sum_v \left(\tilde{A}_G\right)_{v,u} y_u \right)^2$$

$$= D \sum_u \left(\sum_v \left(\tilde{A}_G\right)_{v,u} y_u \right)^2$$

$$= D \|\tilde{A}_G \cdot y\|_2^2 \le D \cdot \alpha^2 \|y\|_2^2 \le \alpha^2 \|x\|_2^2$$

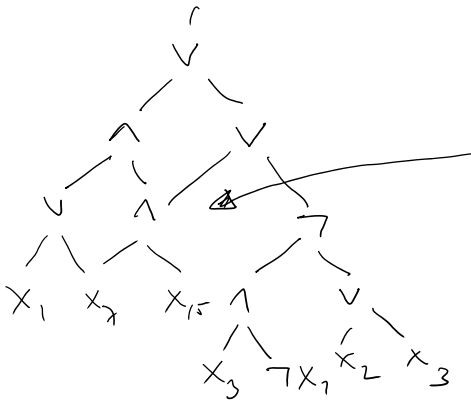
$y \perp \mathbb{1}$

Note: Reingold's USTCONN algorithm.

Michal Koucky v 02/01/2018 14:24

Super Concentrators

- Boolean circuits – generalization of bool. formulas



– can reuse already computed value multiple times

$f: \{0,1\}^n \to \{0,1\}$

or more generally

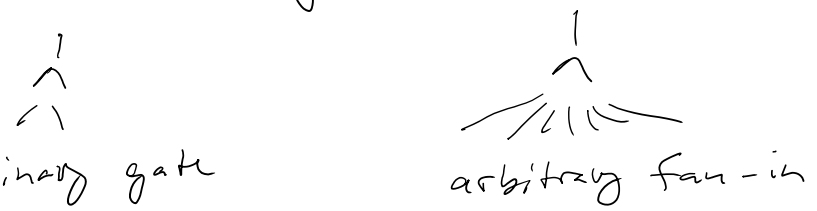
$f: \{0,1\}^n \to \{0,1\}^m$

n inputs m outputs

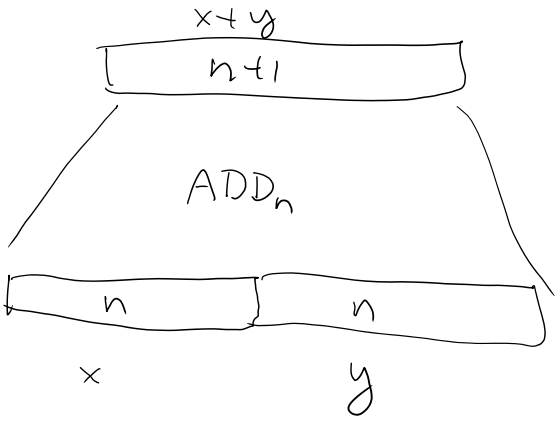
↑ depth,

depth corresponds to time necessary for evaluation

constant depth → allow gate of arbitrary fan-in



Ex: integer addition $ADD_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{n+1}$



- can be computed by ckts of depth 10 & size $O(n^3)$.
  ↑ # of gates or # of wires

(Exc): determine by constant depth ckt, where carry bit starts & how far it propagates.
using the carry into & x & y, determine the output.

Size of a ckt: # of wires ... $w(n)$
# of gates ... $s(n)$

Fact: For ckt's consisting of AND & OR, NOT gates,
$w(n) \leq s(n)^2$.

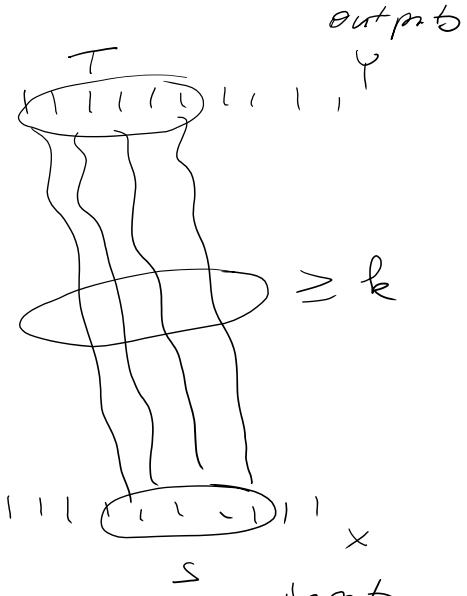
Q: Can addition be done by constant depth circuits of linear size? (I.e., $s(n) \in O(n)$?)

Valiant ≃ '70s: Perhaps not, the circuit must contain some weak super-concentrator.

(Later Valiant shows the linear size construction of super-concentrators from the 1st lecture. This construction has depth $O(\lg n)$.)

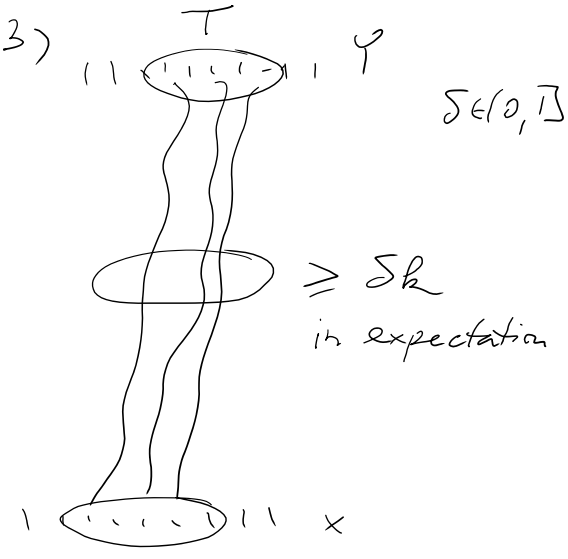
three variants of superconcentrators

1)



$\forall k$
$\forall S \subseteq X, |S| = k$
$\forall T \subseteq Y, |T| = k$
$\exists$ k vertex disjoint paths from S TO T.

3)



$\forall k$ the expected number of vertex disjoint paths between $S \subseteq X$ & $T \subseteq Y$, $|S| = |T| = k$, sampled at random is $\geq \delta k$.

2) middle ground: $\forall k$ $\forall S \subseteq X, |S| = k$ the expected # of vertex disjoint paths between S & $T \subseteq Y$, $|T| = k$, T sampled at random, is $\geq \delta k$.

Ex.: • circuits for addition satisfy 3)
• circuits for good error correcting codes satisfy 2)

Ex: • circuits for addition satisfy 3)
• circuits for good error correcting codes satisfy 2)

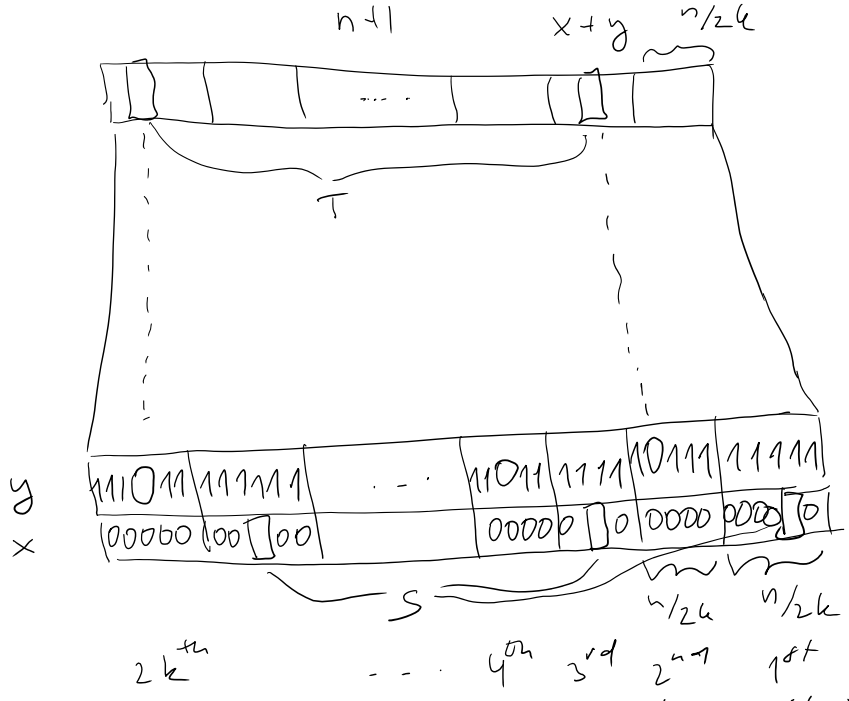
1) ⇒ 2) ⇒ 3)

↳ weakening of 3) ... S, T don't have to be sampled uniformly from $\binom{X}{k} \times \binom{Y}{k}$ but can be sampled from a distribution on $\binom{X}{k} \times \binom{Y}{k}$ s.t.

$$\forall i \in X \quad \Pr_S[i \in S] \leq \frac{k}{\varepsilon n} \qquad \text{for fixed } \varepsilon \in (0,1].$$

$$\forall j \in Y \quad \Pr_T[j \in T] \leq \frac{k}{\varepsilon n}$$

Given $k \geq 1$



blocks of $\frac{n}{2k}$ bits

Pick from each odd block of x one position uniformly at random → S

Pick from each even block of $x+y$ —//— → T

Claim: There are at least k vertex disjoint paths between S & T.

↳ $\varepsilon = \frac{1}{4}$, $\delta = 1$ (we could trade ε for δ)

↳ Pf: set all bits of y to 1 except for positions in T
set all bits of x to 0 except for positions in S

as we vary over the 2^k choices w/i to positions of X in S, we observe 2^k different outputs at positions in T of $X+y$. If the claim were false, by Menger's thm (min-cut-max-flow thm), we could separate the positions of X in S from positions of $X+y$ in T by a cut of size $< k$. However, this cut is the only connection between those positions & it must be transmitting k bits of information. Impossible if it is of size $< k$. Hence the claim must be true ☐

Size of super concentrators

The # of edges in graphs satisfying 1), 2), 3)

depth	1)	2)	3)	
1	$\Omega(n^2)$	$\Omega(n^2)$	$\Omega(n^2)$	
2	$\Omega\left(n \frac{\lg^2 n}{\lg\lg n}\right)$	$\Omega\left(n\left(\frac{\lg n}{\lg\lg n}\right)^2\right)$	$\Omega(n \lg n)$	(Tashma–Radhakrishna GKKPV)
3	$\Omega(n \lg\lg n)$	$\Omega(n \lg\lg n)$	$\Omega(n \lg\lg n)$	
$2d$	$\longleftarrow$	$\Omega(n \lambda_d(n))$	$\longrightarrow$	(Dolev-Dwork-Pippenger-Wigderson Pudlák)
$d>2$ $2d+1$				
$O(\lg n)$		$\Omega(n)$	(Valiant)	

all bounds are tight as there are matching constructions where λ_d are defined as follows:

For $f : \mathbb{N} \to \mathbb{N}$ where $f(n) < n$ for $n > 1$

define $F^*(n) = \min\{ i ;\ f^{(i)}(n) \le 1 \}$

$$f^{(i)}(n) = \underbrace{f(f(f\cdots f(n))\cdots)}_{i\text{-times}}$$

then $\lambda_0(n) = \lfloor \sqrt{n} \rfloor$, $\lambda_{d+1} = \lambda_d^*$ $d \geq 0$

Notice: $\lambda_1(n) = \Theta(\lg \lg n)$ $\lambda_2(n) = \Theta(\lg^* n)$

Properties of λ_d: $\forall f : \mathbb{N} \to \mathbb{N}$ s.t. $f(n) \leq \lfloor n^{1/2} \rfloor$

1) $f^*(n) \leq f(n) \leq \lfloor n^{1/2} \rfloor$ $\forall n$

2) $f^{(i+1)}(n) \leq \dfrac{f^{(i)}(n)}{f^{(i+1)}(n)}$ $\forall i\ \forall n$

3) $\dfrac{f^*(n)}{2} \leq f^{(i)}(n)$ $\forall i \leq f^*(n)/2$

Pf: (Exc) ☒

Def: DAG G with n outputs Y & n inputs X is

$(\delta, \varepsilon, \eta)$-connected if $\forall k \in \{\eta n, \eta n+1, \ldots n\}$

there are distributions on X on $\binom{X}{k}$ and Y on $\binom{Y}{k}$

s.t. $\forall i \in X$ $\Pr_{S \sim X}[i \in S] \leq \dfrac{k}{\varepsilon n}$

$\forall j \in Y$ $\Pr_{T \sim Y}[j \in T] \leq \dfrac{k}{\varepsilon n}$

& $\mathbb{E}_{\substack{S \sim X \\ T \sim Y}}[\#\text{ of vertex disjoint paths between } S \text{ \& } T \text{ in } G] \geq \delta k$.

$D(n, d, \delta, \varepsilon, 1/r)$ = the minimum # of edges in a $(\delta, \varepsilon, 1/r)$-connected DAG G with n inputs & n outputs.

Thm: (Pudlák '94) For any fixed $d \geq 2$, and for every n & $r \leq n$

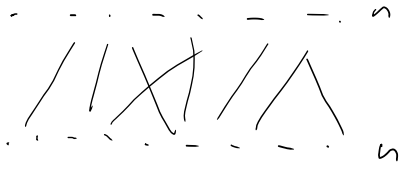
$$D(n, 2d, \delta, \varepsilon, 1/r) \geq \Omega(n \lambda_d(r))$$

(Pudlák '94)

$$D(n, 2d, \delta, \varepsilon, 1/r) \geq \Omega(n \lambda_d(r))$$
$$D(n, 2d+1, \delta, \varepsilon, 1/r) \geq \Omega(n \lambda_d(r))$$

Lemma: $D(n, 1, \delta, \varepsilon, 1/r) \geq \frac{\delta \varepsilon^2}{2} nr \geq \Omega(n \lambda_0(r))$

Pf: Consider a $(\delta, \varepsilon, 1/r)$-connecting graph with n inputs & n outputs of depth 1 with $\leq s$ edges.



Set $k = \lceil \frac{n}{r} \rceil$, let X & Y be the distributions given from $(\delta, \varepsilon, 1/r)$-connecting.

Given edge (i,j) connects $S \cap X$, $T \sim Y$ with probability at most $\frac{k^2}{\varepsilon^2 n^2}$

so the expected # of edges between S & T is at most $s \frac{k^2}{\varepsilon^2 n^2}$. By $(\delta, \varepsilon, 1/r)$-connecting

$$s \frac{k^2}{\varepsilon^2 n^2} \geq \delta k \Rightarrow s \geq \delta \varepsilon^2 n^2 / k \geq \frac{\delta \varepsilon^2 nr}{2}$$

$$\frac{n}{r} \geq 1 \Rightarrow k \leq 2\frac{n}{r}$$

Lemma: Let $f(n) \leq \lfloor n^{1/2} \rfloor$ for all $n \geq 0$.

$\forall \alpha, \delta, \varepsilon \ \exists \beta$ s.t.

if $\forall n \forall r \leq n \quad D(n, d, \frac{\delta}{2}, \varepsilon, 1/r) \geq \alpha n f(r)$ (a)

then $\forall n \forall r \leq n \quad D(n, d+2, \delta, \varepsilon, 1/r) \geq \beta n f^*(r)$ (b)

Pf: Assume $\alpha, \delta, \varepsilon$ are s.t. (a) is true.

We will show (b) holds for suitable β.

Take G with n inputs, n outputs of depth $d+2$

which is $(\delta, \varepsilon, 1/r)$-connected.

Let $V_0, V_1, V_2, \dots V_{d+2}$ be vertices at levels $0, \dots d+2$ in G.

Def: $A_0 = \{ v \in V_1 \cup V_{d+1} ; \deg(v) > f(r) \}$

$\forall i > 0$: $A_i = \{ v \in V_1 \cup V_{d+1} ; f^{(i+1)}(r) < \deg(v) \le f^{(i)}(r) \}$

<u>claim</u>: $\forall i$; $1 \le i \le \frac{f^*(r)}{2} - 3$ at least one of the following holds:

(1) $|A_0 \cup \dots \cup A_{i-1}| \ge \frac{\delta}{4} \frac{n}{f^{(i+1)}(r)}$

(2) $|\{(u,v); (u,v) \text{ incident with } A_i \cup A_{i+1} \cup A_{i+2}\}| \ge \frac{\varepsilon\delta}{4} n$

(3) $|\{(u,v); (u,v) \text{ not incident with } A_0 \cup \dots A_{i+2}\}| \ge \alpha n \frac{f^{(i+2)}(r)}{f^{(i+3)}(r)}$

<u>Pf:</u> Let i be given. Suppose $\neg(1)$ & $\neg(2)$. We will show that (3) is true.

Let k be arbitrary integer s.t. $\frac{n}{f^{(i+1)}(r)} \le k \le n$.

Let S, T be chosen according to the appropriate X, Y.

On average, there are $\ge \delta k$ vertex disjoint paths connecting them.

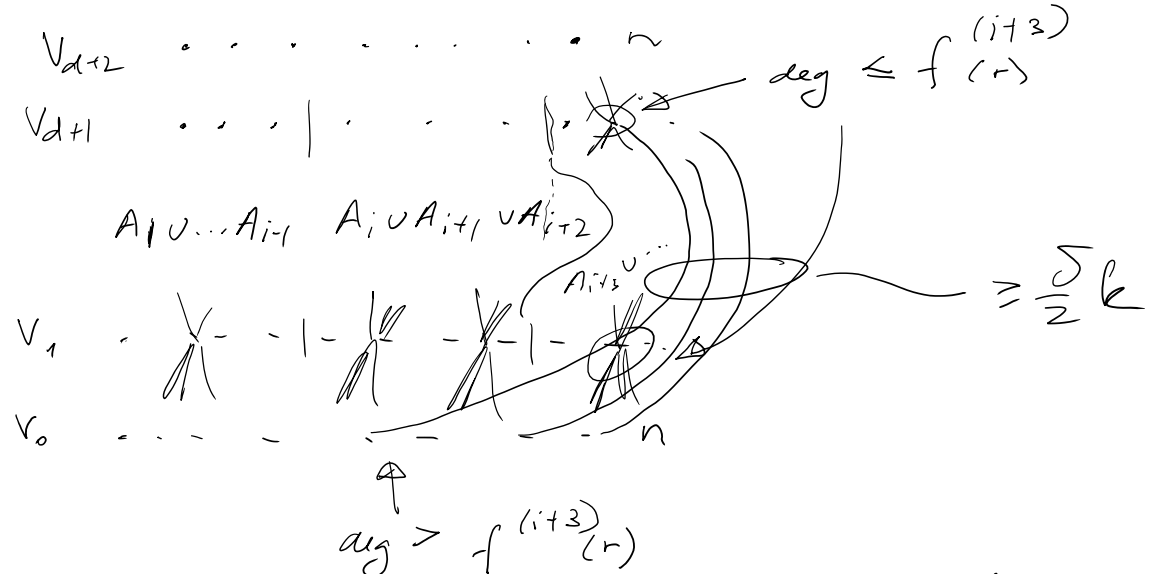
Among them there are at most $\frac{\delta}{4} \frac{n}{f^{(i+1)}(r)} \le \frac{\delta}{4} k$ paths through $A_0 \cup \dots \cup A_{i-1}$ by $\neg(1)$ &

at most $\frac{\varepsilon\delta}{4} n \cdot \frac{k}{\varepsilon n} = \frac{\delta}{4} k$ via $A_i \cup A_{i+1} \cup A_{i+2}$ by $\neg(2)$.

$\ge$ prob'ty of an edge connected to $A_i \cup A_{i+1} \cup A_{i+2}$ being incident with S or T.

Hence, on average at least $\frac{\delta}{2} k$ paths

must go through $A_{i+3} \cup A_{i+4} \dots$.



Create G' from G by removing $V_{d+1} \cup V_1$ with all incident edges and adding edge (u, v) for any two vertices $u \in V_2$, $v \in V_0$ which are connected via $A_{i+3} \cup A_{i+4} \cup \dots$ and similarly for $u \in V_d$ & $v \in V_{d+2}$.

G' has at most $f^{(i+3)}(r)$ - times more edges than G, it is of depth d & $(\frac{\delta}{2}, \varepsilon, \frac{1}{f^{(i+1)}(r)})$-connected.

By (a) G' is of size at least

$$D\left(n, d, \frac{\delta}{2}, \varepsilon, \frac{1}{f^{(i+1)}(r)}\right) \ge \alpha n f\left(f^{(i+1)}(r)\right) = \alpha n f^{(i+2)}(r).$$

Hence

$$|G| \ge \frac{|G'|}{f^{(i+3)}(r)} \ge \frac{\alpha n f^{(i+2)}(r)}{f^{(i+3)}(r)}$$

so (3)

To finish the lemma:

Case 1: $\exists i \le \frac{f^*(r)}{2} - 3$ s.t. (1) holds.

Then $|G| \geq f^{(i)}(r) \cdot |A_0 \cup A_1 \cup \dots \cup A_{i-1}|$

$\leq$ degree of vertices in g

$$\geq \frac{\delta}{4} \frac{n}{f^{(i-1)}(r)} \cdot f^{(i)}(r) \geq \frac{\delta}{4} n \cdot f^{(i+1)}(r)$$

$$\geq \frac{\delta}{4} n \cdot \frac{f^*(r)}{2}$$

$$\geq \frac{\delta}{8} n \cdot f^*(r)$$

Case 2: $\forall i \leq \frac{f^*(r)}{2} - 3$, (2) holds:

$$|G| \geq \frac{1}{3}\left(\frac{f^*(r)}{2} - 3\right) \frac{\varepsilon\delta}{4} n \geq \beta n f^*(r)$$

for suitable β.

Case 3: $\exists i \leq \frac{f^*(r)}{2} - 3$ s.t. (3) holds

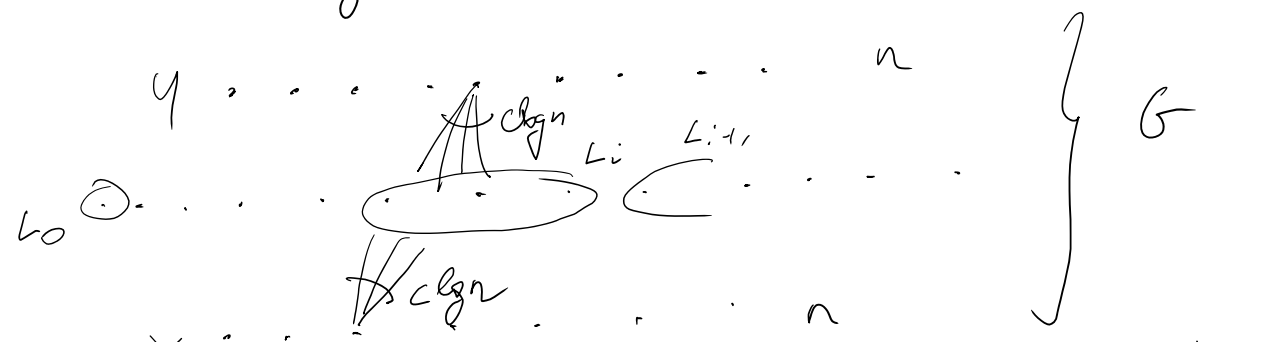
$$|G| \geq \alpha n \frac{f^{(i+2)}(r)}{f^{(i+3)}(r)} \geq \alpha n f^{(i+3)}(r) \geq \frac{\alpha}{2} n f^*(r).$$

The two lemmas imply the theorem

Michal Koucky v 10/01/2018 11:47

Construction of depth 2 superconcentrator

$\rightarrow O(n \lg^2 n)$ edges



G ... depth 2, n inputs, n inputs

middle layer $\dot{\cup} L_i$ $i = 0, \dots, t$

middle layer L_i $\quad i = 0, \dots, t$

$t = 1 + \log_{\frac{6}{5}} n$

$|L_i| = \ell_i$ where $\ell_0 = 1 \quad \ell_{i+1} = \frac{6}{5}\ell_i$

G ... for $i = 0, \dots t$, for each $u \in X \cup Y$, connect u to $c \log n$ random vertices in L_i (chosen uniformly, independently)

$\rightarrow$ G has $(t+1) \cdot 2n \, c \log n = O(n \log^2 n)$ edges

Claim: W.h.p. G is a superconcentrators s.t.

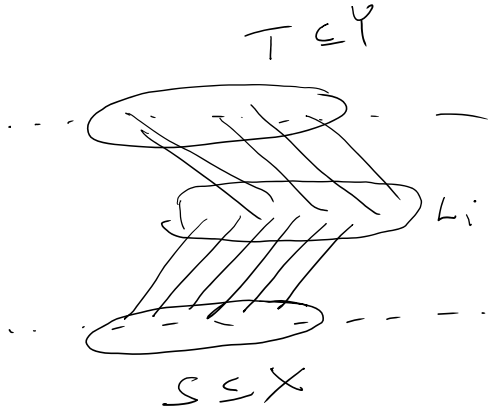
$\forall k \quad \forall S \subseteq X, \forall T \subseteq Y, \quad |S| = |T| = k \Rightarrow$ there are k vertex disjoint paths between S & T.

Pf: G is nice if $\forall S \subseteq X$ if i satisfies $\left(\frac{5}{6}\right)^2 \ell_i \le |S| \le \frac{5}{6}\ell_i$ then there is a matching between $S \& L_i$

& similarly for $\forall T \subseteq Y$.

Claim: If G is nice then G is superconcentrator.

Pf:



matching from S covers $\ge \left(\frac{5}{6}\right)|L_i|$ vertices of L_i

$\ge \frac{2}{3}|L_i|$. The same for T.

$\Rightarrow$ matching from S & T overlap on at least

$\geq \frac{2}{3}$ k vertices.

$\Rightarrow$ there are at least $\frac{2}{3}k$ vertex disjoint paths between S & T via L_i.

Let S' be the vertices of S not on those paths & T' be the vertices of T not on those paths.

$|S'| \leq \frac{1}{3}|S|$ & $|T'| \leq \frac{1}{3}|T|$

and we still need to connect vertices in S' & T' by vertex disjoint paths. This can be done in one step via $L_{i'}$, where $i' < i$, as the set S', T' are $\leq \frac{1}{3}$ of $|S|, |T|$.

($k \leq \frac{5}{6}\ell_i \Rightarrow |S'|, |T'| \leq \frac{1}{3}k \leq \frac{5}{6}\ell_{i'}$, $i' \leq i-1$)

We need to show that G is nice w.h.p.

Claim: $\forall k \in [n]$, let i be s.t. $\left(\frac{5}{6}\right)^2 \ell_i \leq k \leq \frac{5}{6}\ell_i$.

$\Pr[\exists S \subseteq X, |S| = k, \nexists \text{ matching between } S \text{ \& } L_i] \leq \frac{1}{n^2}$

Similar claim holds for $T \subseteq Y$.

By union bound, the claim implies $\Pr[G \text{ is not nice}] \leq 2n \cdot \frac{1}{n^2} \leq \frac{2}{n}$.

Pf: Let $S' \subseteq X$. $k' = |S'|$ $k' \leq k$

$\Pr[|\Gamma(S') \cap L_i| < |S'|] \leq$

$\Pr[\exists U \subseteq L_i, |U| < k', \Gamma(S) \cap L_i \subseteq U]$

$\leq \binom{\ell_i}{k'-1} \cdot \left(\frac{|U|}{|L_i|}\right)^{k' \cdot c \log n} \leq \left(\frac{6}{5}n\right)^{k'} \cdot \left(\frac{5}{6}\right)^{k' c \log n}$

of U's $\Pr[\Gamma(S) \cap L_i \subseteq U]$

choices of S' $\approx$

Let $k' \le k$ $\quad |S'| = k'$

$$\Pr[\exists S' \subseteq X,\ |\Gamma(S') \cap L_i| < |S'|] \le \binom{n}{k'} \cdot \left(\frac{6}{7}n\right)^{k'} \left(\frac{7}{6}\right)^{k' \log n}$$

$$\le \left(\frac{7}{6} \cdot \frac{1}{n^5}\right)^{k'}$$

by choice of $\subseteq$.

$$n^{k'} \cdot \left(\frac{6}{7}n\right)^{k'} \left(\frac{7}{6} \cdot \frac{1}{n^5}\right)^{k'}$$

$$\le \frac{1}{n^3}$$

$|S| \le k$

$$\Rightarrow \Pr[\underbrace{\exists S' \subseteq X,\ |\Gamma(S') \cap L_i| < |S'|}_{(*)}] \le k \cdot \frac{1}{n^3} = \frac{1}{n^2}$$

if $(*)$ doesn't happen, the by Hall's theorem, there is a matching between S & C_i for each $S \subseteq X$ of size k.

Codes based on expanders

code $C \subseteq \{0,1\}^n$

$|C| = 2^k$ $\qquad \delta \in (0,1)$ $\qquad \forall x \neq y \in C \quad \Delta_{Ham}(x,y) \ge \delta n$

Δ_{Ham} ↑ Hamming distance

want:

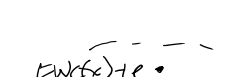
$$ENC : \{0,1\}^k \to \{0,1\}^n$$
$$DEC : \{0,1\}^n \to \{0,1\}^k$$

where $\forall x \in \{0,1\}^k, \forall e \in \{0,1\}^n,\ \Delta_{Ham}(e, 0^n) \le \tau n$

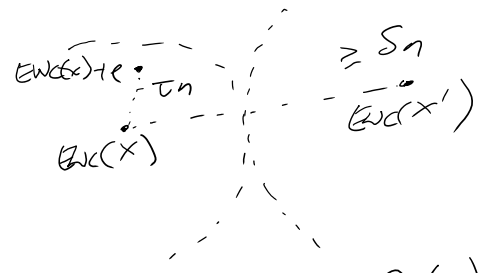
$$\Rightarrow \quad DEC(ENC(x) + e) = x$$

$+$ ↑ bit-wise XOR; e ↑ error

typically $\tau < \frac{\delta}{2}$

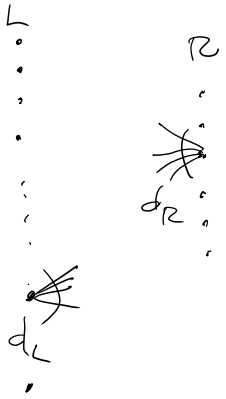


typically $\tau < \frac{\delta}{2}$



ideally: ENC, DEC computable in time $O(n)$
- can be achieved for $\delta, \tau, \varepsilon$ constants

[Spielman '94]



$G = (L \cup R, E)$

$|L| = n \quad |R| = (1-\varepsilon)n$

$L = \{1, \dots n\}$

$C = \{y \in \{0,1\}^n \text{ s.t. } \forall u \in R, \bigoplus_{i \in \Gamma(u)} y_i = 0\}$

$\rightarrow$ C is defined by $(1-\varepsilon)n$ linear equations (over GF_2, i.e., mod 2)

$\rightarrow \dim C \geq n - \#\text{eq's}$

$= \varepsilon n$

$\rightarrow |C| \geq 2^{\varepsilon n}$

C is a subspace of $\{0,1\}^n$ so $ENC: \{0,1\}^k \rightarrow \{0,1\}^n$ can be done using "generating" matrix A

rows of A ... basis of C.

$ENC(x) = xA$

(time nk but more involved construction gives $O(n)$)

DEC(y):

while $\exists i \in L$ s.t. more than $\frac{1}{2}$ of equations to which y_i contributes is not satisfied

flip y_i

output y

$\rightarrow$ can be implemented so that each iteration takes $O(1)$ time.

... $1 - \delta$ errors

- if G is a strong expander & the number of ... is small enough, the decoding step can be done in $O(n)$ time with the correct output.

$\gamma \in (0,1)$
$\forall\, U \subseteq L \quad |U| \le \gamma n \Rightarrow |\Gamma(U)| > \frac{3}{4} d_L |U|.$ (*)

By HW: $(*) \Rightarrow \forall\, U \subseteq L \quad |U| \le \gamma n$, $|\{v \in \Gamma(U) : \exists! u \in U, u \sim v\}| > \frac{d_L}{2}|U|$.

"unique neighbors"

$\Rightarrow$ if the # of errors in y is $\le \gamma n$, then there is a position with error s.t. more than $1/2$ of its lin. constraints are not satisfied. Hence the decoding algorithm can perform an iteration.

Cl.: If the # of errors in y is $\le \frac{\gamma}{2 d_L} n$ then the decoding alg. decodes correctly in $O(n)$ steps.

Pf: In each iteration the alg. decreases the # of unsat. constraints by at least one.
$\Rightarrow$ it cannot run for more than $\frac{\gamma}{2} n$ repetitions.
During each iteration it may or may not introduce an error to y, but the # of these errors is at most $\frac{\gamma}{2} n$. So during the run the word never reached γn errors in total, so it can always find a bit to flip. Hence it stops because all constraints are satisfied, i.e. it stops with a codeword.
As the distance of the code is $\ge \gamma n$, the

codeword must be the original codeword

for bits flips cannot give another codeword as some constraints will be unsatisfied. (the unique corrected)

a more involved construction give ENC & DEC in $O(n)$ time

END