Expansion, divisibility, parity

joint with M. Radziwiłł

(joint with M. Radziwiłł)

Motivation

As $x \to \infty$

λ Liouville function

$\lambda(p) = -1$

completely multiplicative

$$\frac{1}{x} \sum_{n \le x} \lambda(n) = o(1) \iff \text{PNT}$$

$$\frac{1}{x} \sum_{n \le x} \lambda(n)\lambda(n+1) = o(1)$$

open and very hard

(Chowla's conjecture in degree 2)

Tao 2015 (using M-R)

$$\frac{1}{\log x} \sum_{n \le x} \frac{\lambda(n)\lambda(n+1)}{n} = o(1) \quad (*)$$

as $x \to \infty$

2015: Matomäki-Radziwiłł

$\lambda(n)$ averages to 0 over most short interval:

For $H \to \infty$ as $N \to \infty$,

$$\frac{1}{NH} \sum_{x=N}^{2N-1} \left| \sum_{n=x+1}^{x+H} \lambda(n) \right| = o(1)$$

as $N \to \infty$

(known before for $H \ge N^{1/6}$)

(*) reduces to

$$\frac{1}{x\mathcal{L}} \sum_{n \leq x} \lambda(n) \sum_{\substack{p \mid n \\ p \in P}} \lambda(n+p) = o(1) \qquad (**)$$

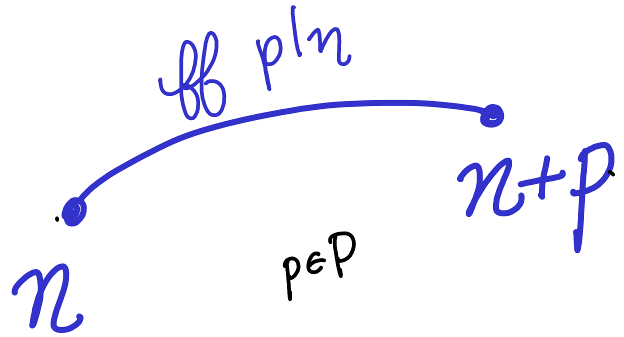
$$\mathcal{L} = \sum_{p \in P} \frac{1}{p} \to \infty$$

P a set of primes $\leq H$

I.2 A prime divisibility graph

vertices $V = \mathbf{N} = \{N+1, \ldots, 2N\}$

edges $E = \{\{n, n+p\},\ p \in P,\ p \mid n\}$, $n,\ n+p \in V$



equivalent to graph considered in M-R-T II, Tao

T is locally connected a.e.

"it may be possible to estimate expressions [...] by establishing some sort of expander graph property." "Unfortunately we were unable to establish such an expansion property, as the [...] standard methods of establishing expansion [do not] work."

Expander graphs

usually defined for <u>regular</u> graphs Γ (= graphs where every vertex has degree d)

Define a linear operator Ad: for $f: V \to \mathbb{C}$

$$(Ad\, f)(v) := \sum_{w:\{v,w\}\in E} f(w)$$

$Ad\, f: V \to \mathbb{C}$

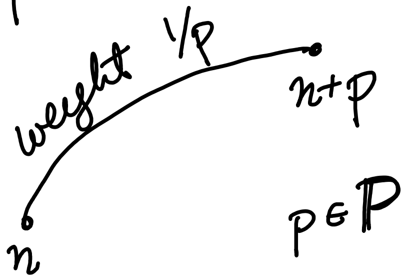
A regular graph of degree d is an (two-sided) ϵ-expander if every eigenvalue λ of Ad (except for one "copy" of $\lambda = d$, corresponding to constant functions) satisfies $|\lambda| \leq (1-\epsilon) d$

Lemma A graph is an ϵ-expander iff the endpoint of a random walk of length $\leq \frac{C}{\epsilon} \log|V|$ is almost perfectly <u>equidistributed</u> (in L^∞ norm)

Our Γ can only equidistribute locally

Aim for "local expansion a.e."

Γ'



$$A := Ad_\Gamma - Ad_{\Gamma'}$$

Is A an expander? Not quite $\mathcal{L} = \sum_{p \in P} 1/p$

is that enough?

· We want more:

we want every eigenvalue to be small, in fact: $o(\mathcal{L})$

· $\exists\, n$ with (too) many prime factors

We define $X \subset N = \{N+1, \ldots, 2N\}$, $N \setminus X$ very small

We will work with

$$(A_{|X} f) := (A(f|_X))|_X$$

so

$$(A f_{|X})_{|X}(n) = \sum_{p \in P} \sum_{\substack{\sigma \in \{-1,1\} \\ n,\, n+\sigma p \in X}} \left(1_{p|n} - \frac{1}{p} \right) f(n+\sigma p)$$

We will show that $A_{|X}$ has a strong expander property: every eigenvalue is $O(\sqrt{\mathcal{L}})$

O(Ramanujan)

Main Thm Let Γ, A be as above for $P \in [H_0, H]$. Let $\mathcal{L} = \sum_{p \in P} 1/p \geq e$

Assume $\log H_0 \geq (\log H)^{2/3} (\log\log H)^2$ and $\log H \leq \sqrt{\frac{\log N}{C\mathcal{L}}}$

Then: $\forall C > 0$ $\exists X \subset \mathbb{N}$ with $\geq (1 - e^{-C\mathcal{L}})N$ elements

s.t.

every eigenvalue of $A|_X$ is $O_C(\sqrt{\mathcal{L}})$

In fact,

$\forall K \geq 1$ $\exists X \subset N$ with $|X| = \left(1 - O\left(\frac{1}{e^{K\mathcal{L}\log K}} + \frac{1}{\sqrt{H_0}}\right)\right)N$

s.t. every eigenvalue of $A|_X$ is $O(\sqrt{K\mathcal{L}})$.

Cor.

For $f, g : N \to \mathbb{C}$ $\quad |f|_2, |g|_2 \leq 1$, $\quad |f|_4, |g|_4 \leq e^{C\mathcal{L}}$

$$\frac{1}{N\mathcal{L}} \left(\sum_{n \in N} \sum_{\substack{p \in P \\ p \mid n}} f(n)\overline{g(n \pm p)} - \sum_{n \in N} \sum_{p \in P} \frac{f(n)\overline{g(n \pm p)}}{p} \right)$$

$$= O_C\left(\frac{1}{\sqrt{\mathcal{L}}}\right)$$

Cor.

I.4 Consequences on parity

Cor For any $1 \le w \le X$

$$\frac{1}{\log w} \sum_{\frac{X}{w} < n \le X} \frac{\lambda(n)\lambda(n+1)}{n} = O\left(\frac{1}{\sqrt{\log\log w}}\right)$$

Comparison:
For $w = X$

Tao: $\dfrac{1}{(\log\log\log\log x)^{1/5}}$ made explicit by H^2-Ubis

Tao-Teräväinen $\dfrac{1}{(\log\log\log x)^{c}}$ $c < 1/3$

Stronger Cor

Tao-Teräväinen

$$\frac{1}{N} \sum_{N < n \le 2N} \lambda(n)\lambda(n+1) = o(1)$$

at almost all* scales $\frac{X}{W} < N < X$

* outside a set of log density $o(1)$

We replace $o(1)$ $\left(\begin{array}{c}\text{or rather} \\ o(1)\cdot o(1)\end{array}\right)$

by $\dfrac{1}{\sqrt{\log\log w}}$.

More corollaries!

Cor. For k a popular value of $\Omega(n)$, $n \sim x$
(i.e. $k = \log\log n + O(\sqrt{\log\log n})$)
and $e^{(\log x)^{\varepsilon}} \le w \le x$,

$$\sum_{\substack{t < n \le 2t \\ \Omega(n) = k}} \lambda(n+1) = o\Bigg(\sum_{\substack{t < n \le 2t \\ \Omega(n) = k}} 1\Bigg)$$

$O\left(\frac{1}{(\log\log)^{*}} \cdots\right)$

at almost all scales
$\frac{X}{w} \le N \le X$

| average of $\lambda(p+1)$ is 0: open and hard

$\Omega(n) = \#$ of prime factors w/ multiplicity

$\lambda(n) = (-1)^{\Omega(n)}$

Cor. w as above
$I_1(x), I_2(x) \subset \mathbb{Z}_{>0}$

$$\frac{1}{\log w} \sum_{\substack{\frac{X}{w} < n \le X \\ \Omega(n) \in I_1,\ \Omega(n+1) \in I_2}} \frac{\lambda(n)\lambda(n+1)}{n} = O_{\varepsilon}\left(\frac{\sqrt{s_1 s_2}}{\log\log x}\right)$$

where $s_i = \min(|I_i|, \sqrt{\log\log x})$

trivial bound: $\frac{s_1 s_2}{\log\log x}$

From now on:

Sketch of proof of Main Thm

If there is one large eigenvalue α, there are $\geq \frac{N}{H}$ of them (after restriction to some good X) because our edges are of lengths $\leq H$ (by Hölder)

$$\longrightarrow \operatorname{Tr} A^{2k}|_X \geq \frac{N}{H}\alpha^{2k}$$

(A is real symmetric)

Recall:

$$\sum_{\text{eigenvalues } \lambda} \lambda = \operatorname{Tr} A = \sum \text{diagonal entries}$$

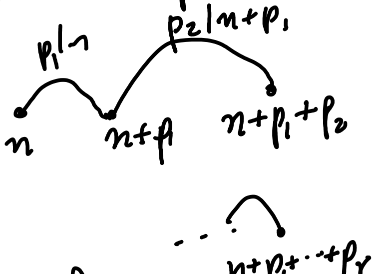
$$\sum \lambda^{2k} = \operatorname{Tr} A^{2k} = \sum_{\substack{\text{closed} \\ \text{paths of length } 2k}} \prod (\text{weights})$$

We will exclude from X:

(0) magic sauce

(1) all n with $\geq K\ell$ prime factors in $\mathbb{P}$

(2) all n s.t. $\exists\, p \mid n$, r small ($r \leq \ell$), $\exists\, p_1, \dots, p_r$ distinct from p and each other (except if consecutive) s.t. $\exists$ path in Γ



and $p \mid n$, $p \mid n+p_1+\dots+p_r$ (p is the "witness prime")

What is $\mathrm{Tr}(A|_X)^{2k}$ like?

Well, what is $\mathrm{Tr}\, A^{2k}$ like? sum over closed paths

$\mathrm{Tr}\, A^{2k}$ = sum over closed paths where each prime appears at least twice

lone prime $\Rightarrow$ total cancellation (as we vary n over N)

$n_i = n + \sigma_1 p_1 + \dots + \sigma_i p_i$

$p \mid n_i$ Prob $= \frac{1}{p}$ weight $1 - \frac{1}{p}$

$p \nmid n_i$ Prob $= 1 - \frac{1}{p}$ weight $-\frac{1}{p}$

$$\frac{1}{p} \cdot \left(1 - \frac{1}{p}\right) + \left(1 - \frac{1}{p}\right)\left(-\frac{1}{p}\right) = 0$$

effect of excluding integers from X with $\geq K\mathcal{L}$ factors in P

instead of total cancellation, contribution of a walk is divided by $\sqrt{\mathcal{L}}$ for each lone prime

Pf Kubilius model

+

Laplace transform of smooth version of truncation $\leq K\mathcal{L}$	Shifting multiple contour integral

Effect of excluding from X vertices n with ≥ 1 witness path of length $\leq l$

inclusion-exclusion ... too expensive

In $\mathbb{Z}$, (even with conditions mod p) inclusion-exclusion too expensive $\rightsquigarrow$ combinatorial sieve

Brun $\to$ abstract combinatorial sieve

having a particular witness path $\iff n \equiv a_i \bmod m_i$

m_i: composite

prove a combinatorial sieve for composite moduli

Problem: redundancy

$(6 \cdot 5 = 10 \cdot 3)$

$\to$ Rota's cross-cut thm $\to$ cancellation

So, in general:

$$1_{\text{sieved set}} = \text{main term} + O^*\Big(\sum_{R \in \partial \mathcal{D}} 2^{\omega(q(R))} 1_{n \in R}\Big)$$

i.e. $1_{n \notin P}\ \forall P \in \mathcal{Q}$

$\mathcal{Q}$ a set of arithmetic progressions)

being:

$$\sum_{R \in \mathcal{D}} c_R 1_{n \in R}$$

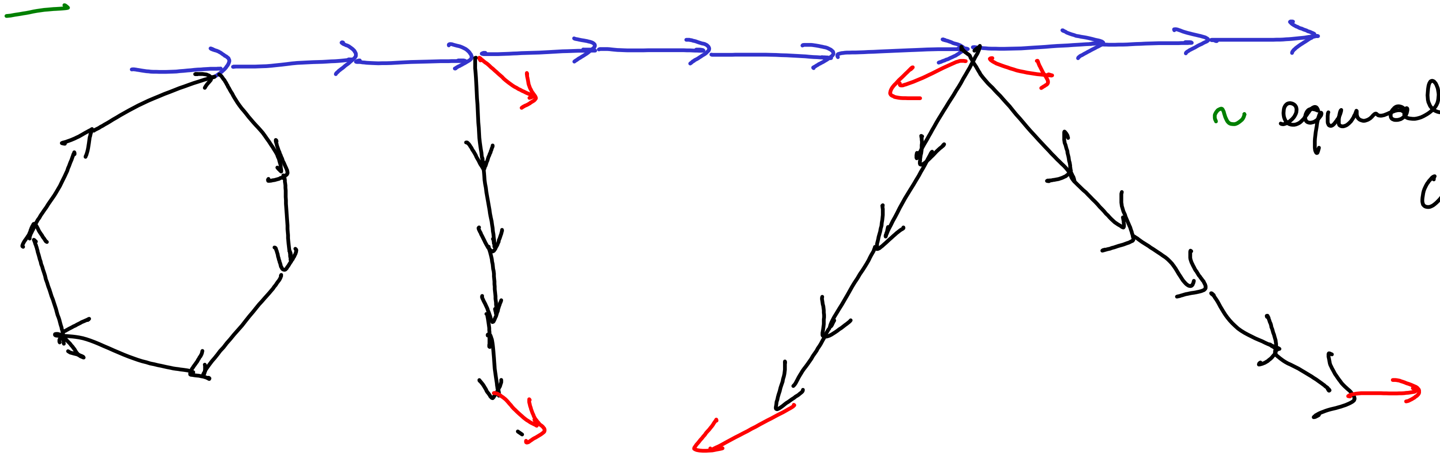
$|c_R| \leq 2^{\omega(q(R))}$

$\mathcal{D}$ = a subset of $\mathcal{Q}^\cap$ of your choice, closed under $\cap$

elements of $\mathcal{D}$ s.t. $\exists P \in \mathcal{Q}$ with $R \cap P \notin \mathcal{D}$

$q(R)$ = modulus of R

Ex. a condition in $\mathcal{Q}^\cap$:



simplifying, and skipping some steps:

$\sigma_i = \pm 1$

must bound sum of $\prod_{i: p_i \nmid n_i} \frac{1}{p_i}$

over closed walks of length $2k$

n, $n_1 = n + \sigma_1 p_1$, $n_2 = n + \sigma_1 p_1 + \sigma_2 p_2$

$n_3 = n + \sigma_1 p_1 + \sigma_2 p_2 + \sigma_3 p_3, \ldots$

with

(a) $\underbrace{\text{few lone primes}} < k/\log k$

(b) every n_i has $\leq K\mathcal{L}$ prime divisors

K a parameter

(c) $\underset{(<K)}{\text{few}}$ disjoint revenants

There are no indices

$1 \leq i_1 < i_1' \leq i_2 \leq i_2' \leq \ldots \leq i_K < i_K' \leq 2k$

note: this is morally true

s.t.

(i) $p_{i_r} = p_{i_r'}$ $\forall r$

We have already summed over n at this stage

(ii) $\exists\, i_r < j_r < i_r'$ with $p_{j_r} \neq p_{i_r}$

(iii) the walk between i_r and i_r' isn't trivial as a word

We consider the shape of a walk

$\vec{\sigma} = \{-1, 1\}^{2k}$

shape: $(\sim, \vec{\sigma})$

equivalence relation on $\{1, \ldots, 2k\}$

We will sum over all walks of that shape

$I \subset \{1, \ldots, 2k\}$ "bit" indices $\leftarrow p_i \mid n_i$

if $1 \sim 4$ and $1, 4 \in I$: $\Longrightarrow p_1 \mid p_2 + p_3$

in the example

$p_1 \mid n + p_1$, $p_1 = p_4 \mid n + p_1 - p_2 + p_3 + p_1$

if 1 or $4 \notin I$: pay penalty $\frac{1}{p_1}$ (or $\frac{1}{p_1^2}$)

$$\begin{array}{c|l} p_{[1]} & a_{11} p_{[1]} + a_{12} p_{[2]} + \cdots \\ p_{[1]} & \\ p_{[2]} & M = (a_{ij}) \end{array}$$

Idea: we will usually find in M a submatrix of large rank r with disjoint row and column indices

$\downarrow$ geometry of #s

few walks of that shape

Example:

$n \to n + p_1$

$\downarrow$

$n + p_1 - p_2$

$\downarrow$

$n + p_1 - p_2 + p_3$

$\downarrow$

$n + p_1 - p_2 + p_3 + p_1$

$\downarrow$

$n + 2p_1 - p_2 + p_3 + p_2$

$\downarrow$

$n + 2p_1 + p_3 - p_4 = n$

has shape $(\sim, \vec{\sigma})$:

$\vec{\sigma} = 1, -1, 1, 1, 1, -1$

equiv classes $i \sim j$ iff $p_i = p_j$

Sketch of proof

Let $\sim$ be an equiv. relation on $\{1,\dots,2k\}$, $\vec{\sigma}$ a tuple $\in \{-1,1\}^{2k}$

$(\sim,\vec{\sigma})$ induces a word

The indices not surviving reductions are colored yellow

graph $G_\sim :=$ vertices $=$ non-yellow equivalence classes

edges: between $[i_1]$ and $[i_2]$

s.t. every $i_1<j<i_2$ or $i_2<j<i_1$ is yellow

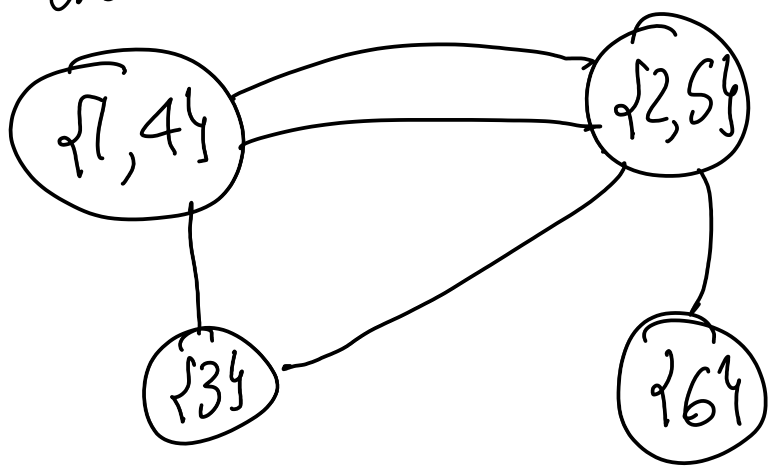
Example:

$\sim = \{\{1,4\},\{2,5\},\{3\},\{6\}\}$

$\vec{\sigma} = (1,-1,1,1,1,-1)$

$X_{[1]} X_{[2]}^{-1} X_{[3]} X_{[1]} X_{[2]} X_{[6]}^{-1}$

induce



Another example:

$$\sim \; = \{\{1,8\},\{2,9\},\{3\},\{4,7\},\{5,6,10\}\}$$

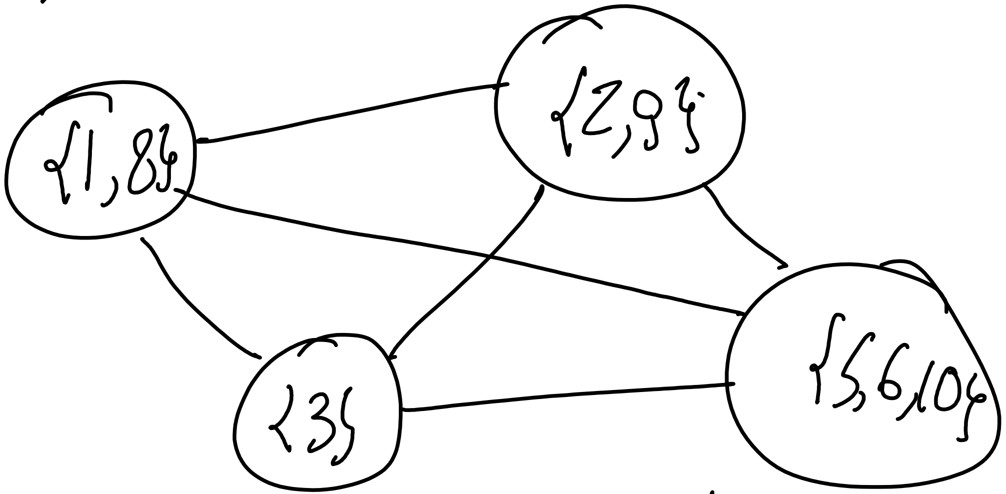
$$\vec{\sigma} = (1,-1,1,-1,1,-1,1,1,1,-1)$$

$$w = x_{[1]}\, x_{[2]}^{-1}\, x_{[3]}\, x_{[4]}^{-1}\, x_{[5]}\, x_{[5]}^{-1}\, x_{[4]}\, x_{[1]}\, x_{[2]}\, x_{[5]}^{-1}$$

reduction: $w' = x_{[1]}\, x_{[2]}^{-1}\, x_{[3]}\, x_{[1]}\, x_{[2]}\, x_{[5]}^{-1}$

So the class $[4] = \{4,7\}$ is yellow

vertices = non-yellow classes



$\sim', \vec{\sigma}' = (1,-1,1,1,1,-1)$: what you expect

Lemma Let $(\sim, \vec{6})$ be a shape of length $2k$

Let $\mathcal{G} = \mathcal{G}_\sim$.

Partition non-yellow vertices of $\mathcal{G}_\sim$ into red and blue so that $\mathcal{G}|_{blue}$ is connected

Let $x_{[j]}$ a formal variable for each red $[j]$

$$v(i) := \sum_{\substack{j < i \\ [j] \in \text{red}}} 6_j \, x_{[j]} \quad \text{for } 1 \le i \le 2k$$

Then the space V spanned by $v(i_2) - v(i_1)$ with $[i_1] = [i_2] \in$ blue

equals the space W spanned by $v(i_2) - v(i_1)$ with $[i_1] = [i_2] \in$ blue

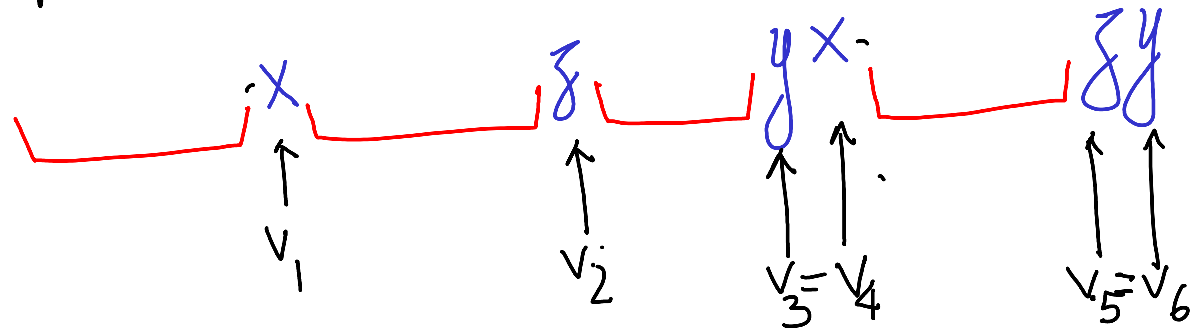
Easy linear algebra Lemma

Let A be an $n \times m$ matrix s.t.

- every row has at least one non-zero entry
- no column has $> k$ non-0 entries

Then $\operatorname{rank} A \ge \frac{n}{k}$

Example



because $\mathcal{G}_\sim$ blue is connected

rows in M: $P_x \mid \underbrace{\text{linear combination of red variables between first and second } x}_{= v_4 - v_1} + C$

$$V = \langle v_4 - v_1,\ v_6 - v_3,\ v_5 - v_2 \rangle$$

$$\|$$

$$W = \langle v_2 - v_1,\ v_3 - v_2,\ \underbrace{v_4 - v_3}_{=0},\ v_5 - v_4,\ \underbrace{v_6 - v_5}_{=0} \rangle$$

Prop Let $(\sim, \vec{\sigma})$, $\mathcal{G}_\sim$, V be as before. Let $(\sim', \vec{\sigma}')$ be the reduced shape. Assume $< k$ disjoint revenants in $(\sim', \vec{\sigma}')$ (i.e. can't have $1 \le i_1 < i_1' \le i_2 < i_2' < \dots \le i_r < i_r' \le 2k'$ with $i_\nu \sim' i_\nu'$ $\forall \nu$, $\exists\, i_\nu < j < i_\nu'$ with $j \not\sim i_\nu$)

Then $\dim W \geq \frac{s}{k} - 1$

where $s = \#$ of indices $1 \le j \le 2k'$ s.t. j is blue and $j+1$ is red

Idea of Pf

s counts red blocks

$<k$ disjoint revenants $\longrightarrow$ $<k$ of these blocks have trivial sums

$\downarrow$

each red letter appears in $<k$ blocks

So: use easy linear algebra lemma

So: want to choose blue $\subset V$ so that $G|_{\text{blue}}$ is connected and s is as large as possible.

Draw an arrow from $[i']$ to $[i+1']$ in G for each $1 \le i \le 2k'$ (draw each arrow only once) and from $[2k']$ to $[1']$

There's an arrow into every vertex

For $S \subset V$, $\vec{\partial} S := \{ v \in V \setminus S : \exists\, v' \in S \;\; v' \to v \}$. Then $s \geq |\vec{\partial} S| - 1$.

So choose blue $\subset V$ so that $G|_{\text{blue}}$ is connected & $\vec{\partial}$ blue is large. How?

How to choose connected blue $\subset V$

s.t. $\vec{\partial}$ blue is large

Graph theory result

(essentially Kleitman-West '91;
followed Storer '91,
Payan-Tchuente-Xuong '84,
Griggs-Kleitman-Shastri '89;
see also Gravin '11,
Bankevich-Karpov '12, Karpov '13)

For any connected graph with $\geq n$ vertices of degree >2,

$\exists$ spanning tree $\geq \frac{n}{4} + 2$ leaves. //

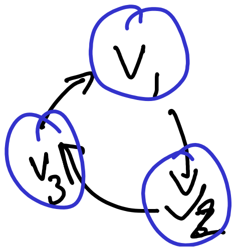
The undirected boundary of the set of $\underbrace{\text{non-leaves (internal vertices)}}_{\text{connected!!!}}$ is the set of leaves

directed boundary $\vec{\partial}$:

(0) put every internal vertex in blue

(1) if non-leaf → leaf v put v in red

(2) other leaves fall into cycles



odd
red

So:

- $G|_{\text{blue}}$ is connected
- $\vec{\partial}$ blue $> \frac{n}{12} + 1$

Good!

But what happens if n is small,
i.e., if few vertices v in G have degree >2 ?

degree 1 means:

wvw $\quad$ $w^{-1}vvvw^{-1}$

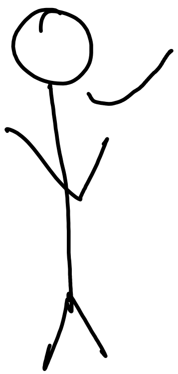
v always followed and preceded by w (or v)

degree 2:
same with w_1, w_2

$\longrightarrow$ words with few vertices of degree >2 can be described simply

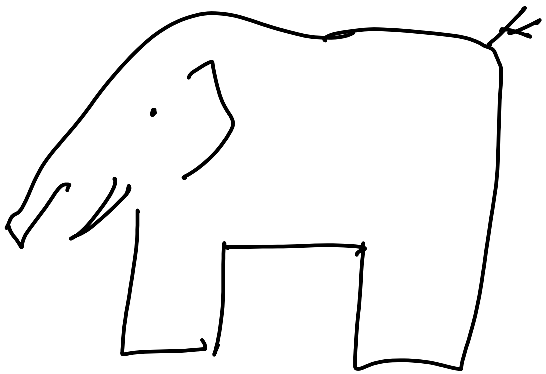
$\longrightarrow$ few such words

(meaning $O(1)^k \; (2k)^{kn}$ as opposed k^k)



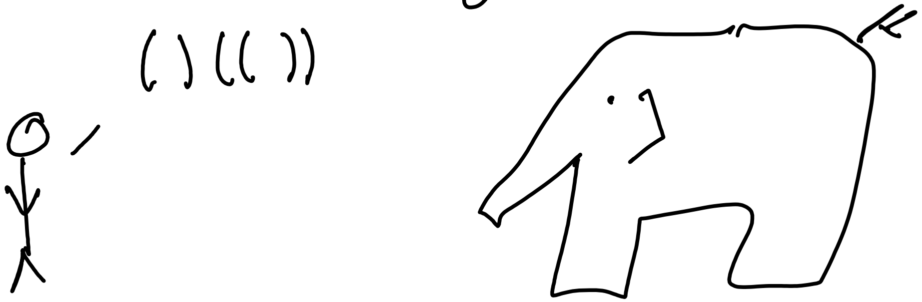
remember w_2?

that's the next letter



v

What about the part of the walk that got reduced?

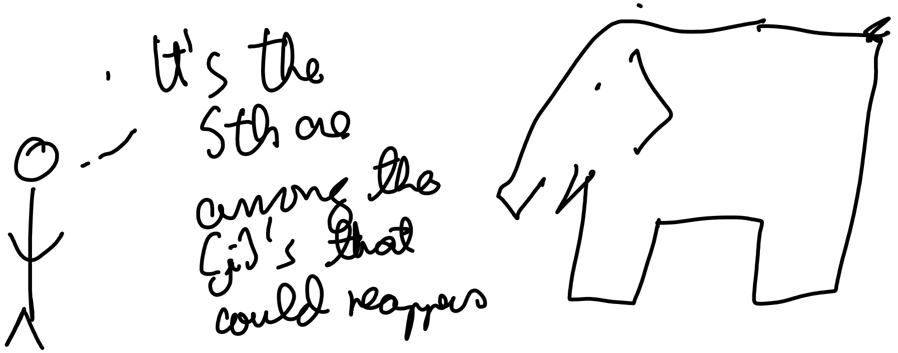


→ reconstructing $2m$ steps that were reduced has cost $O(KL)^m$.

still have to describe equivalence class of each (

If new, good. If not:

$\ldots P[j]\,\sigma_j\, P[j]^+ \cdots \sigma_{i-1}\, P[i-1]$



... and there are only $\leq KL$ possibilities

Choose your parameters:

$k = c_0 \log H$, $\ell \simeq \dfrac{\log H_0}{\log L \log 2k}$, $K \simeq \dfrac{\sqrt{\log H_0}}{\log 2k}$ → Main Thm proved. //

What next?

· graphs with composite edges

(perhaps without factors $< H_0$)

edges with 2 prime factors

$\Rightarrow$ a.e.

$\# n$ s.t. $\Omega(n) = k$
$\Omega(n+1) = k'$

k, k' popular

$\rightarrow$ bounds $\frac{1}{(\log x)^c}$ rather than $\frac{1}{\sqrt{\log \log}}$?

· higher-order Chowla?

unclear what to do

hypergraphs?