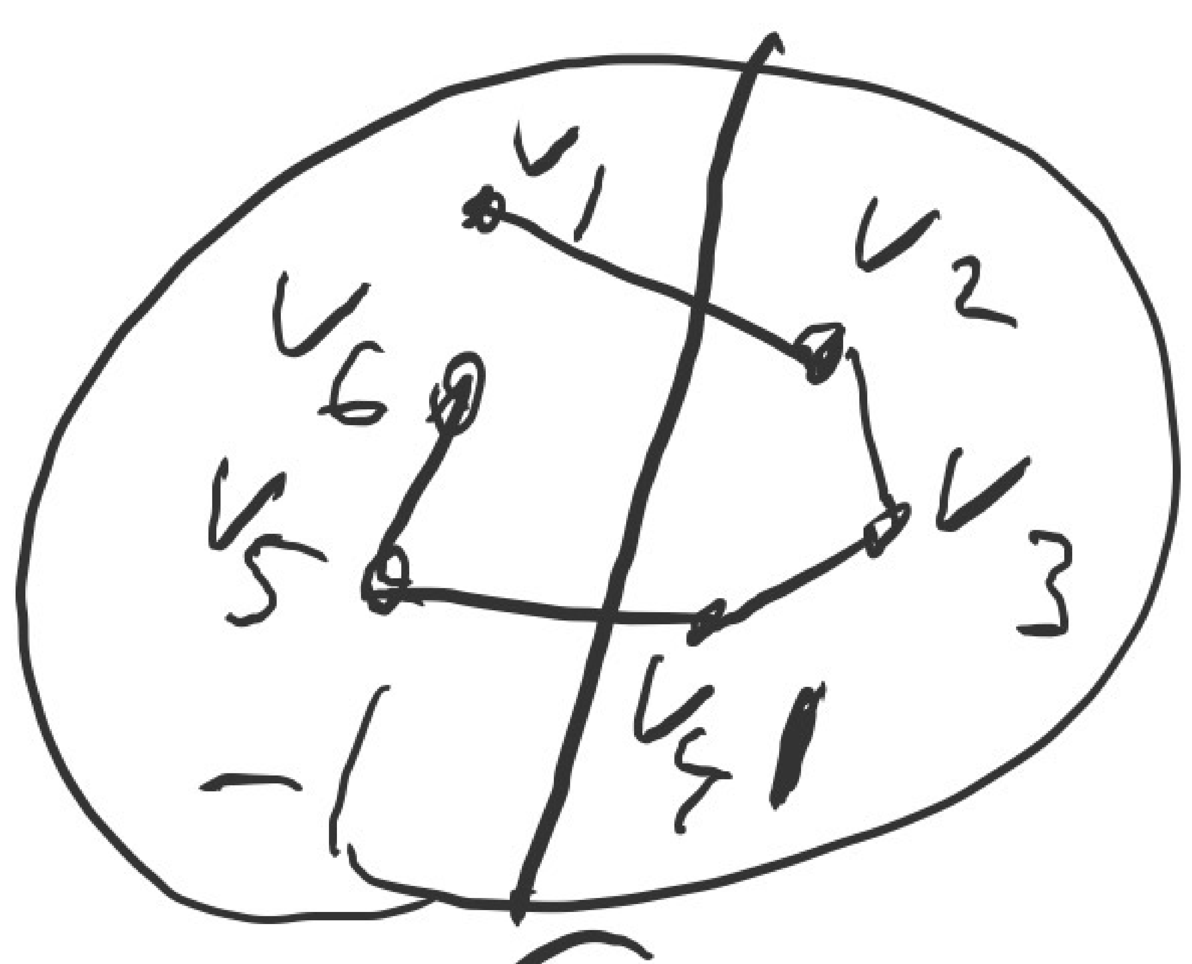
Expander Random Walks: A Fourier Analytic Approach

Gil Cohen, Noam Peri, and Amnon Ta-Shma

Overall question: Let's say we have a d-regular expander G and we take a pseudo-random sequence as follows:

1. Label half of the vertices of G -1 and label the other half 1
2. Take a $(t-1)$ step random walk $v_1, v_2, \ldots, v_t$ and output the labels of the vertices

G 

$-1, 1, 1, 1, -1, -1$

Q: For which functions does this behave like a random $x \in \{-1,1\}^t$?

This paper uses Fourier analysis to show that

Symmetric functions, functions in AC^0, and functions computable by a low width read once branching program are fooled.

Preliminaries: λ-spectral expanders

For a d-regular graph G, we'll also use G to denote the normalized adjacency matrix.

$$G_{ij} = \begin{cases} \frac{1}{d} & \text{if } (i,j) \in E(G) \\ 0 & \text{otherwise} \end{cases}$$

Definition: We say that G is a λ-spectral expander if for all eigenvectors except for $\vec{1}$, the magnitude of its eigenvalue is at most λ.

Definition: Define J to be $\frac{1}{n} \cdot$(all ones matrix) $\forall i,j \; J_{ij} = \frac{1}{n}$

Key property: $G = J + E$ where $\|E\| \le \lambda$ and $EJ = JE = 0$.

Preliminaries: Fourier Analysis Over $\{-1,1\}^t$

Fourier characters: $\chi_S = \prod_{j \in S} x_j$

Fourier Coefficients: $\hat{f}_S = \mathop{E}_{x \in \{-1,1\}^t} [f(x)\chi_S(x)]$

Fourier decomposition: $f = \sum_{S \subseteq [t]} \hat{f}_S \chi_S$

Parseval's Theorem: $\sum_{S \subseteq [t]} \hat{f}_S^2 = \mathop{E}_{x \in \{-1,1\}^t} [f^2]$

We'll be analyzing ± 1-valued functions so this will be 1.

Preliminaries: Difference from Random

Def: Given a graph G and a labeling $val: V(G) \to \{-1,1\}$ (where half of the vertices are labeled 1) define $RW_{G,val,t}$ to be the distribution obtained by taking the labels of a $(t-1)$ step random walk

Definition: Given a function $f: \{-1,1\}^t \to \{-1,1\}$, define $\mathcal{E}_{G,val}(f) = E_{x \sim RW_{G,val,t}}[f(x)] - E_{x \sim \{-1,1\}^t}[f(x)]$

Define $\mathcal{E}_\lambda(f) = \max_{\substack{\lambda\text{-spectral expanders } G \\ val}} |\mathcal{E}_{G,val}(f)|$

Idea: Bound $\mathcal{E}_\lambda(f)$ by analyzing $\mathcal{E}_{G,val}(X_S)$

Results on Symmetric Functions

Definition: We say that a function $f: \{-1,1\}^t \to \{-1,1\}$ is <u>symmetric</u> if $f(x_1, x_2, \ldots, x_t)$ only depends on the number of -1s and 1s in $x_1, \ldots, x_t$.

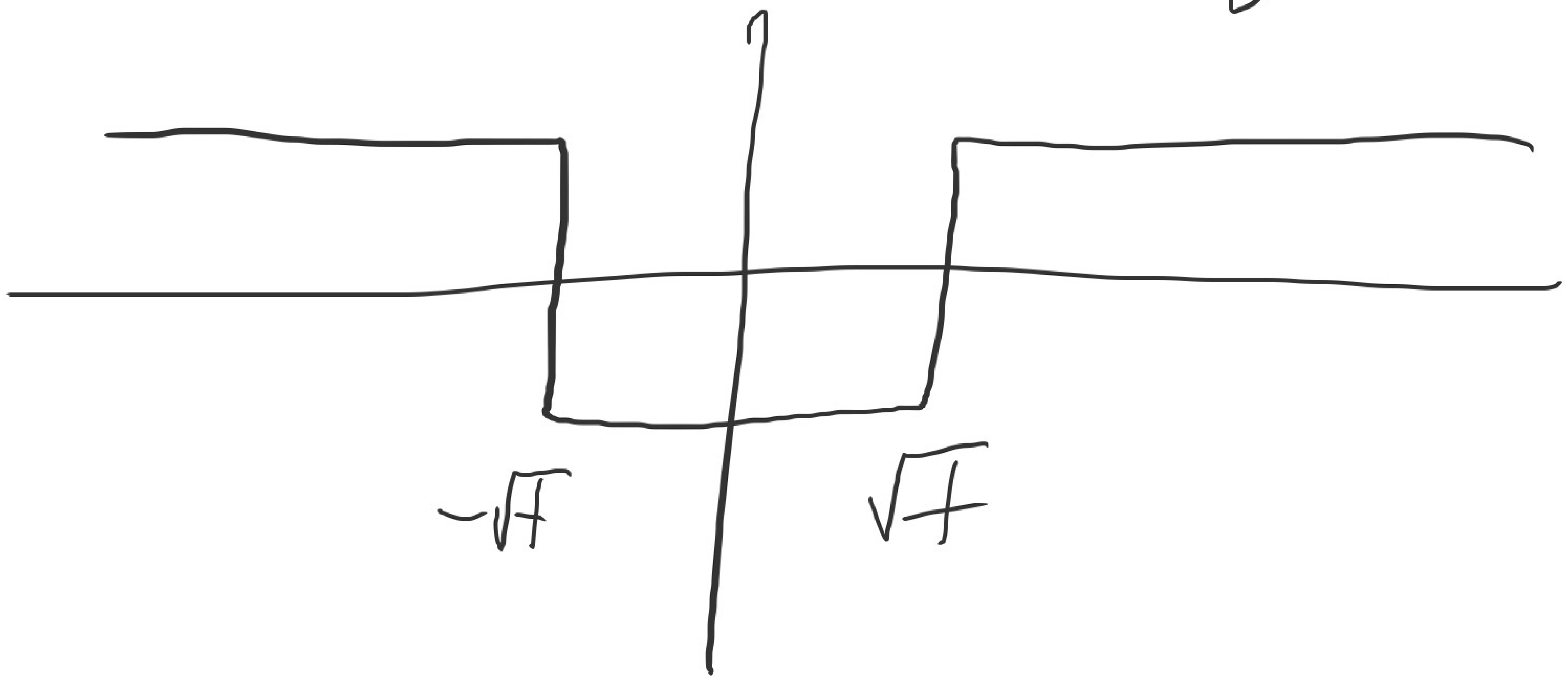
Theorem 1.1': For all symmetric functions f,

$$\varepsilon_\lambda(f) \text{ is } O(\lambda).$$

Restatement: If we only consider the number of 1s and -1s in x, the total variation distance between $RW_{G,val,t}$ and U_t = uniform dist on $\{-1,1\}^t$ is $O(\lambda)$

Theorem 1.4: $\varepsilon_\lambda(MAJ_t)$ is $O\left(\frac{\lambda^2}{\sqrt{t}}\right)$

I think $O(\lambda)$ is tight. I think



is an example.

Note: $RW_{G,val,t}$ does not necessarily fool all functions

If $Pr(\text{crossing}) = \frac{1}{2} + \Omega(\lambda)$ then

for $RW_{G,val,t}$, $E[\#\text{ of crossings}]$

is $\frac{t}{2} + \Omega(\lambda t)$

For U_t, # of crossings is $\frac{t}{2} \pm O(\sqrt{t})$.

Results on General Functions

Definition: Given a function $f:\{-1,1\}^t \to \{-1,1\}$, define $L_{1,k}(f) = \sum_{\substack{S \subseteq [t] \\ |S|=k}} |\hat{f}_S|$

Definition: Define $L_1^t(b)$ to be the family of functions $f:\{-1,1\}^t \to \{-1,1\}$ such that

$$\forall k \quad L_{1,k}(f) \le b^k$$

Claim 5.2': For any function $f \in L_1^t(b)$, $\varepsilon_t(f)$ is $O(\lambda b^2)$

Avishay Tal

Tight Bounds on the Fourier Spectrum of AC^0

Theorem: Any function computable by a size s depth d AC^0 circuit is in $L_1^+(b)$ for $b = O((\log s)^{(d-1)})$

$E_\lambda(f)$ is $O(\lambda(\log s)^{2(d-1)})$

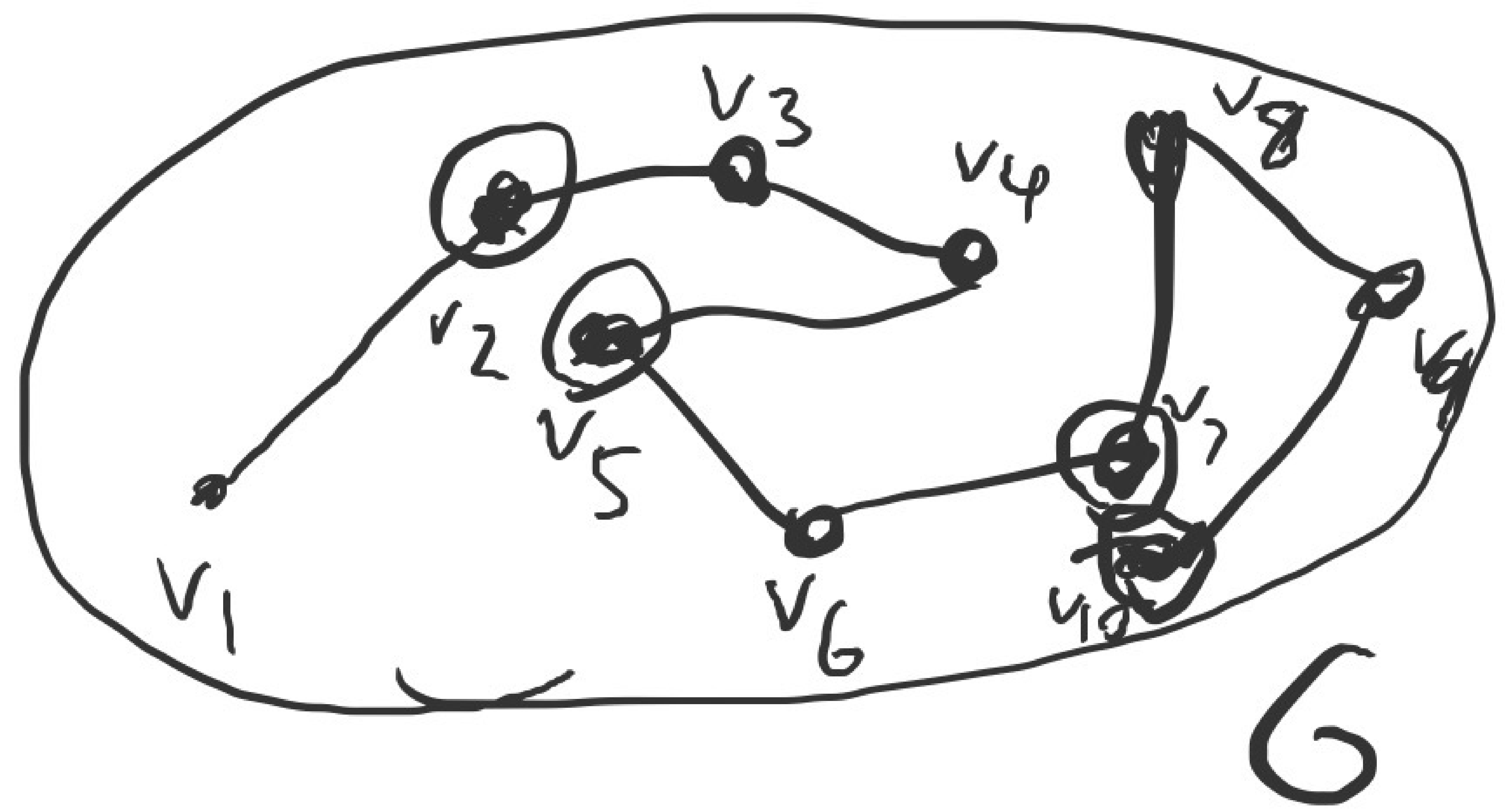
Eshan Chattopadhyay, Pooya Hatami, Omer Reingold, and Avishay Tal   Improved Pseudorandomness for Unordered Branching Programs Through Local Monotonicity

Theorem: If f can be computed by a width w read once branching program, $b = O((\log t)^w)$

$E_\lambda(f)$ is $O(\lambda(\log t)^{2w})$

$t \leq DT(f)$ $\qquad$ $\mathcal{E}_\lambda(f)$ is $O(\lambda\, DT(f)^2)$.

Analysis:



Consider $\mathcal{E}_{G,val}(X_S)$
$= \underset{RW_{G,val,t}}{E}[X_S(x)]$

$S = \{2, 5, 7, 10\}$
$\Delta_0 = 1$ $\Delta_1 = 3$ $\Delta_2 = 2$ $\Delta_3 = 3$

Define P to be the diagonal matrix where $P_{ii} = val(i)$.

$$\mathcal{E}_{G,val}(X_S) = \vec{1}^T (PG^{\Delta_{t-1}}) \ldots (PG^{\Delta_1})(PG^{\Delta_0})\frac{\vec{1}}{n}$$

Idea: We'll analyze this by breaking G^{Δ_j} up into $G^{\Delta_j} = J + E^{\Delta_j}$ (recall $G = J + E$ wher $\|E\| \leq \lambda$)

$$E_{G_{ral}}(X_S) = \vec{1}^T (PG^{\Delta_{t-1}}) \dots (PG^{\Delta_2})(PG^{\Delta_1}) P \frac{\vec{1}}{n}$$

Idea: Consider which E^{Δ_j} terms we have.

Proposition: $\vec{1}^T P \vec{1} = 0$. Since $J = \frac{1}{n}\vec{1}\cdot\vec{1}^T$,

$JP\vec{1} = 0 \quad \vec{1}^T P J = 0 \quad JPJ = 0$.

Claim: If we don't have E^{Δ_1} or $E^{\Delta_{t-1}}$, this part is 0.

If we don't have E^{Δ_j} and $E^{\Delta_{j+1}}$ for some j, this part is 0.

Definition: Define F_k to be the set of $I \subseteq [k-1]$ such that

1. $1 \in I$, $k-1 \in I$,
2. $\forall j \in [k-2]$ $j \in I$ or $j+1 \in I$.

Proposition 4.2: $\left|E_{G_{ral}}(X_S)\right| \leq \sum_{I \in F_k} \lambda^{\sum_{j \in I} \Delta_j(S)}$

Proposition 4.2: $\left|\mathcal{E}_{G,val}(X_S)\right| \leq \sum_{I \in F_k} \lambda^{\sum_{i \in I} \Delta_i(S)}$

Examples: $|S| = 2$ $\quad \leq \lambda^{\Delta_1}$ $\quad F_2 = \{\{1\}\}$

$|S| = 3$ $\quad \leq \lambda^{\Delta_1 + \Delta_2}$ $\quad F_3 = \{\{1,2\}\}$

$|S| = 4$ $\quad \leq \lambda^{\Delta_1 + \Delta_3} + \lambda^{\Delta_1 + \Delta_2 + \Delta_3}$ $\quad F_4 = \{\{1,3\},\{1,2,3\}\}$

$|S| = 6$ $\quad F_6 = \{\{1,3,5\},\{1,2,4,5\},\{1,2,3,5\},\{1,3,4,5\},$
$\{1,2,3,4,5\}\}$

Proposition: $\forall I \in F_k$, $|I| \geq \lceil \frac{k}{2} \rceil$

Proposition: If $|S| = 0$ or 1 $\quad \mathcal{E}_{G,val}(X_S) = 0$

Corollary: $\forall S : |S| \geq 2$, $\left|\mathcal{E}_{G,val}(X_S)\right| \leq 2^k \cdot \lambda^{\lceil \frac{k}{2} \rceil} \leq (4\lambda)^{\frac{k}{2}}$

Corollary: If $f \in L_1^+(b)$ then

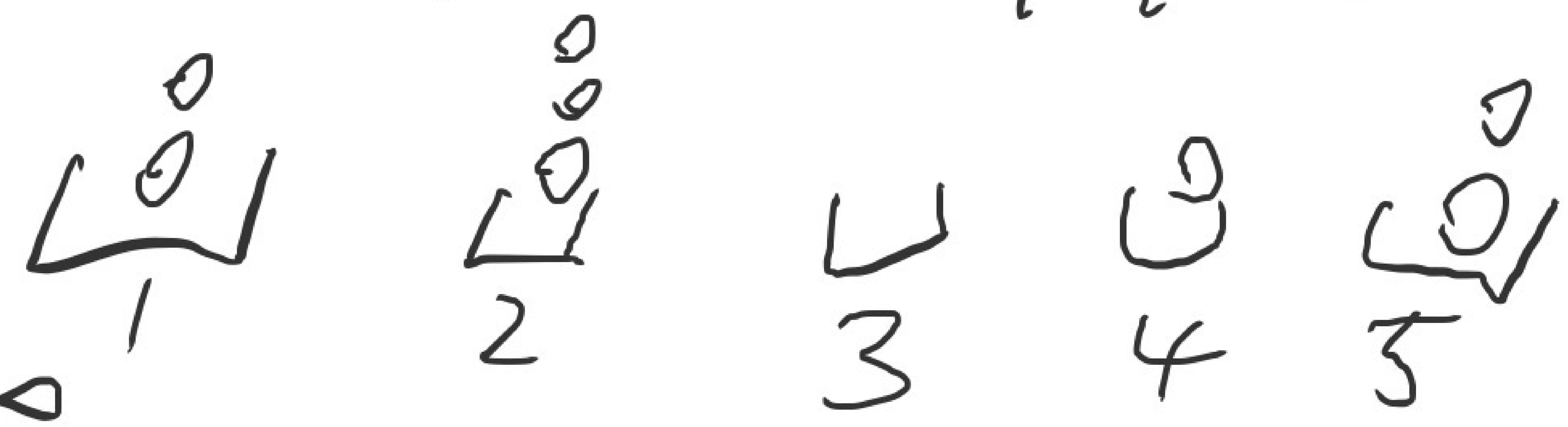
$\mathcal{E}_\lambda(f) \leq \sum_{k=2}^{\infty} (4\lambda)^{\frac{k}{2}} \cdot b^k$ which is $O(\lambda b^2)$.

Review: Unlabeled Balls in Labeled Bins

Proposition: There are $\binom{n+k-1}{k-1}$ ways to put n unlabeled balls in k labeled bins.

Trick: Imagine putting $k-1$ dividing lines among the n balls

$$\circ \ \circ \ | \ \circ \ \circ \ \circ \ | \ | \ \circ \ | \ \circ \ \circ$$



Claim 3.1: $\displaystyle\sum_{j=r}^{\infty} \binom{j}{r} \lambda^j = \frac{\lambda^r}{(1-\lambda)^{r+1}}$ if $|\lambda|<1$

Proof: $\dfrac{1}{1-\lambda} = 1+\lambda+\lambda^2+\lambda^3+\dots$

What is the coefficient of λ^j in $\dfrac{\lambda^r}{(1-\lambda)^{r+1}}$? Claim: This is like putting $j-r$ balls in $r+1$ labeled bins. There are $\binom{j-r+r+1-1}{r+1-1} = \binom{j}{r}$ ways to do this.

Definition: Define $\beta_k = \sum_{\substack{S \subseteq [t]: \\ |S| = k}} \Sigma_{\sigma, val}(x_S)$

Lemma 4.4: $|\beta_k| \leq 2^k \binom{t-1}{\lfloor \frac{k}{2} \rfloor} \left(\frac{\lambda}{1-\lambda}\right)^{\lceil \frac{k}{2} \rceil}$

Claim 4.5: $|\beta_k| \leq 2^k \sum_{m=\lceil \frac{k}{2} \rceil}^{t-\lfloor \frac{k}{2} \rfloor} \binom{m-1}{\lceil \frac{k}{2} \rceil - 1} \binom{t-m}{k-\lceil \frac{k}{2} \rceil} \lambda^m$

By symmetry, this only depends on $|I|$ and is decreasing in I.

Proof: $|\beta_k| \leq \sum_{\substack{S \subseteq [t] \\ |S| = k}} \sum_{I \in F_k} \lambda^{\sum_{j \in I} \Delta_j(S)} = \sum_{I \in F_k} \sum_{\substack{S \subseteq [t] \\ |S| = k}} \lambda^{\sum_{j \in I} \Delta_j(S)}$

Choosing a particular $I^* \in F_k$ where $|I^*| = \lceil \frac{k}{2} \rceil$, $|\beta_k| \leq 2^k \sum_{\substack{S \subseteq [t] \\ |S| = k}} \lambda^{\sum_{j \in I^*} \Delta_j(S)}$

Q: What is the coefficient of λ^m in this expression?
We need to split m factors of λ among $|I^*|$ Δ_j where each Δ_j is at least 1. This is $=$ putting $m - |I^*|$ balls in $|I^*|$ labeled bins.
We also need to divide the remaining $t-1-m$ steps of the path among $k+1-|I^*|$ other Δ. The middle Δ must be at least 1.

This is $=$ putting $t-1-m-(k+1-|I^*|-2)$ unlabeled balls in $k+1-|I^*|$ labeled bins.

This gives a coefficient of $\binom{m-1}{|I^*|-1}\binom{t-m}{k-|I^*|}$ for λ^m

Claim 4.5: $|\beta_k| \le 2^k \sum_{m=\lceil \frac{k}{2} \rceil}^{t-\lfloor \frac{k}{2} \rfloor} \binom{m-1}{\lceil \frac{k}{2} \rceil - 1}\binom{t-m}{k-\lceil \frac{k}{2} \rceil} \lambda^m$

$$\le 2^k \binom{t-1}{k-\lceil \frac{k}{2} \rceil} \lambda \sum_{m=\lceil \frac{k}{2} \rceil}^{\infty} \binom{m-1}{\lceil \frac{k}{2} \rceil - 1} \lambda^{m-1}$$

Claim 3.1: $\sum_{j=r}^{\infty} \binom{j}{r} \lambda^j = \frac{\lambda^r}{(1-\lambda)^{r+1}}$ $\quad = \frac{\lambda^{\lceil \frac{k}{2} \rceil - 1}}{(1-\lambda)^{\lceil \frac{k}{2} \rceil}}$

$r = \lceil \frac{k}{2} \rceil - 1$

Lemma 4.4

$$|\beta_k| \le 2^k \binom{t-1}{k-\lceil \frac{k}{2} \rceil} \cdot \frac{\lambda^{\lceil \frac{k}{2} \rceil}}{(1-\lambda)^{\lceil \frac{k}{2} \rceil}}$$

Lemma 4.4: $|\beta_k| \le 2^k \binom{t-1}{\lfloor \frac{k}{2} \rfloor} \left(\frac{\lambda}{1-\lambda}\right)^{\lceil \frac{k}{2} \rceil}$

For a symmetric function f, defining $\hat{f}_k$ to be $\hat{f}_S$ for some S of size k

$$\mathcal{E}_\lambda(f) \le \sum_{k=2}^{t} |\beta_k| \cdot \hat{f}_k$$

How large can $\hat{f}_k$ be?

There are $\binom{t}{k}$ subsets S of size k.

Since $\sum_{S:|S|=k} \hat{f}_S^2 = \binom{t}{k} \hat{f}_k^2 \le 1$ $\quad \hat{f}_k \le \frac{1}{\sqrt{\binom{t}{k}}}$

$$\mathcal{E}_\lambda(f) \le \sum_{k=2}^{t} 2^k \frac{\binom{t-1}{\lfloor \frac{k}{2} \rfloor}}{\sqrt{\binom{t}{k}}} \left(\frac{\lambda}{1-\lambda}\right)^{\lceil \frac{k}{2} \rceil}$$

$O\left(\frac{\lambda^{\lceil \frac{k}{2} \rceil}}{\sqrt{t}}\right)$ k is odd

$O\left(\lambda^{\frac{k}{2}}\right)$ k is even