Discovering the Foundations of Theoretical Computer Science

(Fernando Granha Jeronimo)

Under heavy construction

Last update: 10/12/24

Inspired by Babai's approach and the hungarian school

Van Gogh prize

a symbolic prize for any student in the course that solves an important open problem

(like van Gogh you are not going to receive anything other than have done something amazing)

Warning: these open problems can be challenging

Spectral Lens

Let $G = (V, E)$ be a d-regular graph on n vertices.

Let A be its adjacency matrix, i.e.,

$$A \in \mathbb{R}^{n \times n}, \quad A_{u,v} = 1_{[\{u,v\} \in E]}.$$

Study the spectral theorem.

Let $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ be the eigenvalues of A with corresponding orthonormal eigenvectors $\varphi_1, \dots, \varphi_n \in \mathbb{R}^n$.

$$(A\varphi_i = \lambda_i \varphi_i)$$

1] Prove that d is an eigenvalue of A.

Def $\langle x, x \rangle = \sum_{i=1}^{n} \bar{x}_i x_i$

Ex $x \in \mathbb{R}^n$ and $\varphi_1, \dots, \varphi_n \in \mathbb{R}^n$ ONB (orthonormal basis)

We can write $x = \sum_{i=1}^{n} \alpha_i \varphi_i$ with $\alpha_i = \langle \varphi_i, x \rangle$.

Ex $\langle x, x \rangle = \sum_{i=1}^{n} \alpha_i^2$ [Parseval]

Ex: $\langle x, Ax \rangle = \sum_{i=1}^{n} \alpha_i^2 \lambda_i$

Ex A sym $\Rightarrow$ A has real eigenvalues

Def Rayleigh quotient $\frac{\langle x, Ax \rangle}{\langle x, x \rangle}$ (for $x \neq 0$)

Ex $\mathrm{Tr}(A) = \sum_{i=1}^{n} \lambda_i$

Ex $\mathrm{Tr}(A^k) = \sum_{i=1}^{n} \lambda_i^k$

Ex $\mathrm{Tr}(A^2) = 2|E|$

Ex If G is simple with deg ≥ 1

$\Downarrow$

$\lambda_n < 0$

Ex Prove that $\frac{1}{n} \sum_{i=1}^{n} \lambda_i^2 = d$

Def $J_n = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ all ones $n \times n$ matrix

Ex Compute eigenvalues of J_n/n

Def K_n complete graph on n vertices

Def $K_{a,b}$ complete bipartite graph
$G = (V = L \cup R, E)$ with $|L| = a, |R| = b$

Ex Compute the spectrum of K_n

Ex Compute the spectrum of $K_{n,n}$

Ex Compute " " of $K_{1,d}$

Ex " " " of $K_{a,b}$

Ex $\lambda_1 \geq \max_{i \geq 2} |\lambda_i|$

Ex G bipartite $\iff$ $\text{Spec}(G) = -\text{Spec}(G)$.

Some Notions of Expansion

Def $\partial(S) = E(S, \bar{S})$ "Edge boundary"

Def $\Phi(S) = \frac{|\partial(S)|}{d|S|}$ "Conductance"

Def $\Phi(G) = \min_{\emptyset \neq S \subseteq V, |S| \leq \frac{n}{2}} \Phi(S)$ "Cheeger's constant"

Def: $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$

two-sided spectral expansion

Def $\lambda^{\text{one-sided}} = \lambda_2$ one-sided spectral expansion

Def $e(S,T) = |\{(s,t) \mid \{s,t\} \in E\}|$

Ex Prove that

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

[Expander Mixing Lemma]

Ex Improve the error bound $\lambda\sqrt{|S||T|}$.

Def $\alpha(G)$ = independence number

Ex Prove that $\frac{\alpha(G)}{n} \leq \frac{-\lambda_n}{d-\lambda_n}$

[Hoffman's bound]

Ex Prove that $d_{avg} \leq \lambda_1 \leq \Delta(G)$

Def $\chi(G)$ is the chromatic number

Ex Prove that $\chi(G) \leq \lambda_1 + 1$

[Wilf's bound]

Mixing Bounds

Def $\vec{1}$ is the all ones vector

Def $R = \frac{1}{d} A$ is the random walk matrix

Ex $R \frac{\vec{1}}{n} = \frac{\vec{1}}{n}$

Ex Prove $\| R^r p - \frac{\vec{1}}{n} \|_1 \leq \left(\frac{\lambda}{d}\right)^r \sqrt{n}$ for any distribution p.

[Mixing bound in l_1]

Study the Perron-Frobenius theorem (useful for understanding more general Markov chains)

Eigenvectors as an optimization problem

Let $V_k = \text{span}\{e_1, \dots, e_k\}$

$W_k = \text{span}\{e_k, \dots, e_n\}$

Ex $\lambda_k = \min_{0 \neq x \in V_k} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \max_{0 \neq x \in W_k} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}$

Ex Prove the min-max variational theorem

$$\lambda_k = \max_{\substack{V \subseteq \mathbb{R}^n \\ \dim(V) = k}} \min_{0 \neq x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \min_{\substack{V \subseteq \mathbb{R}^n \\ \dim(V) = n-k+1}} \max_{0 \neq x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}$$

[Courant-Fischer-Weyl]

The Magic of Interlacing

Ex Eigenvalue Interlacing

Let $A \in \mathbb{R}^{n \times n}$ be real symmetric matrix and B be a $(n-1) \times (n-1)$ principal submatrix

$$\text{eig}(A) = \{\lambda_1 \geq \dots \geq \lambda_n\}$$

$$\text{eig}(B) = \{\tilde{\lambda}_1 \geq \dots \geq \tilde{\lambda}_{n-1}\}$$

Prove $\lambda_1 \geq \tilde{\lambda}_1 \geq \lambda_2 \geq \dots \geq \tilde{\lambda}_{n-1} \geq \lambda_n$

Hint: use min-max theorem for eigenvalues

Extend to $r \times r$ principal submatrix B with $1 \leq r < n$

Ex: $\lambda_j \geq \tilde{\lambda}_j \geq \lambda_{j+n-r}$ for $j \in \{1, \dots, r\}$

[Cauchy Interlacing Thm]

Reminder on PSD matrices

Def A real sym matrix M is <u>positive semi-definite</u> (PSD) if

$$\forall x \in \mathbb{R}^n, \quad x^t M x \geq 0.$$

Ex Prove: The following are equivalent

1) M is PSD
2) M has non-negative eigenvalues
3) $\exists$ a matrix W s.t. $M = W^t W$

<u>Notation</u> We write $M \succcurlyeq 0$ if M is PSD

We write $M_1 \succcurlyeq M_2$ if $M_1 - M_2 \succcurlyeq 0$.

This gives a partial order (Loewner order)

Laplacian Matrix

Def $L = dI - A$ [Laplacian Matrix]

Let $\mu_1 \le \mu_2 \le \dots \le \mu_n$ be the eigenvalues of L

Ex For d-regular G, we have

$$\mu_1 = \underset{\substack{\| \\ 0}}{d - \lambda_1}, \quad \dots, \quad \mu_n = d - \lambda_n.$$

Ex Prove that $\langle x, Lx \rangle = \sum_{i \sim j} (x_i - x_j)^2$

Ex Conclude that $L \succeq 0$ (PSD)

Ex Prove that $\langle 1_S, L 1_S \rangle = |E(S, \bar{S})|$

Ex G connected $\iff$ $\mu_2 > 0$

Ex If G is connected, then $\mu_2 \ge \frac{1}{n \operatorname{diam}(G)}$

Ex $|\{k \mid \mu_k = 0\}| =$ # of connected components

Ex G bipartite iff $\mu_n = 2$

Ex Prove that $\frac{\mu_2}{2} \leq \Phi(G)$

CH* Prove that $\Phi(G) \leq O\left(\sqrt{\frac{\mu_2}{d}}\right)$

Hint: use eigenvector to μ_2 to find a cut ["rounding"].

[Cheeger's Inequality]

$$\frac{\mu_2}{2} \leq \Phi(G) \leq \sqrt{2\mu_2}$$

Characteristic Polynomial

Def Characteristic polynomial $\det(\lambda I - A) =: ch(\lambda)$

The roots of $ch(\lambda)$ are the eigenvalues of A

Cayley-Hamilton Theorem: $ch(A) = 0$

Ex G has diam $= K \Rightarrow A$ has at least $K+1$ distinct eigenvalues
connected

Hint: [Cayley-Hamilton] minimal polynomial

Ex Let A, B be two real sym matrices with $\operatorname{sig}(\lambda_1 \geq \cdots \geq \lambda_n)$, $(\tilde{\lambda}_1 \geq \cdots \geq \tilde{\lambda}_n)$

Compute the eigenvalues of $A \otimes B$.

Def $s : E \to \{\pm 1\}$ is an edge signing

Def $(A_s)_{u,v} \begin{cases} s(\{u,v\}) & \text{if } \{u,v\} \in E \\ 0 & \text{otherwise} \end{cases}$

Ex Prove $\lambda_1(A_s) \leq \Delta(G)$ for any signing s.

Limitations on Spectral Expansion

Ex G d-regular $\Rightarrow \lambda \geq \sqrt{d}\left(1 - o_n(1)\right)$

Ex If G has diam $\geq 4 \Rightarrow \lambda_2 \geq \sqrt{d}$

[Hint: look for the stars]

Ex $\lambda_2 < 0 \iff G = K_n$

[Hint: interlacing]

Ex Suppose G is connected. G has a unique positive eigenvalue iff G is a complete k-partite graph

[Hint: interlacing]

[h*] $\lambda_2 \geq 2\sqrt{d-1}\left(1 - O\left(\frac{1}{diam}\right)\right)$

[Alon-Boppana bound]

(cor) If $d = O(1)$

$$\Downarrow$$

$$\lambda_2 \geq 2\sqrt{d-1}\left(1 - O\left(\frac{1}{\log n}\right)\right)$$

Def G is Ramanujan if $\lambda \leq 2\sqrt{d-1}$

a.k.a. "Optimal" Spectral Expanders

OP [van Gogh Prize]

Construct infinite families of Ramanujan graphs for every $d \geq 3$

Vertex Expansion

Def $N(S) = \{u \mid \exists s \in S, \{u,s\} \in E\}$

Def Vertex (or Lossless) Expansion

$$\Phi^V(S) = \frac{|N(S)|}{d|S|}$$

$$\Phi^V_\varepsilon(G) = \min_{\substack{\emptyset \neq S \subseteq V \\ |S| \leq \varepsilon n}} \Phi^V(G).$$

OP [Van Gogh prize]

Construct explicit family with

$$\Phi^V_\varepsilon(G) > 1/2 \quad \text{for } \varepsilon = \Omega(1)$$

(an two-sided bipartite graph)

On the Complexity of Expansion

(Hypothesis) $\forall \eta \in (0,1)$ $\exists \delta \in (0,1)$ s.t. it is NP-hard to distinguish given input graph $G=(V,E)$

(Yes) $\exists S \subseteq V$ with $|S| \leq \delta n$ and $\Phi(S) \leq \eta$.

(No) $\forall S \subseteq V$ with $|S| \leq \delta n$, we have $\Phi(S) \geq 1-\eta$

OP van Gogh prize

Prove or refute the above hypothesis

Def: Boolean n-hypercube is the graph $H_n = (V, E)$ where

$$V = \mathbb{Z}_2^n$$

$$E = \{\{u, v\} \mid |u - v| = 1\}$$

or equivalently

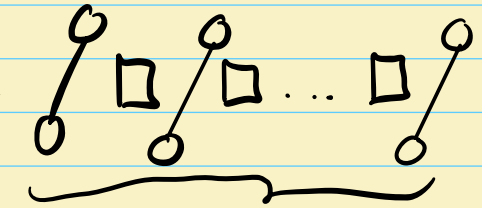
$$E = \{\{u, u + e_i\} \mid u \in \mathbb{Z}_2^n, i \in [n]\}$$

Ex Show that the adjacency matrix of H_n can be defined recursively as

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_n = \left(\begin{array}{c|c} A_{n-1} & I_{2^{n-1}} \\ \hline I_{2^{n-1}} & A_{n-1} \end{array}\right).$$

Def The cartesian product of graphs $G = (V(G), E(G))$ and $H = (V(H), E(H))$ is defined as

$$G \square H = (V = V(G) \times V(H),$$
$$E = \{\{(g_1, h_1), (g_2, h_2)\} \mid$$
$$(\{g_1, g_2\} \in E(G) \text{ and } h_1 = h_2) \text{ or}$$
$$(g_1 = g_2 \text{ and } \{h_1, h_2\} \in E(H))\})$$

Ex Prove that $H_n =$ 

Ex Prove that "the" adjacency matrix of $G \square H$ can be written as

$$A_{G \square H} = A_G \otimes I_{|V(H)|} + I_{|V(G)|} \otimes A_H$$

Ex Prove that

$$\mathrm{Spec}(A_{G \square H}) = \{ \lambda + \tilde{\lambda} \mid \lambda \in \mathrm{Spec}(G), \ \tilde{\lambda} \in \mathrm{Spec}(H) \}$$

Ex Compute $\mathrm{Spec}(H_n)$

Ex Consider the recursive edge signing of H_n

$$B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B_n = \left(\begin{array}{c|c} B_{n-1} & I_{2^{n-1}} \\ \hline I_{2^{n-1}} & -B_{n-1} \end{array}\right)$$

Prove that B_n has eigenvalues $\pm\sqrt{n}$ each with multiplicity 2^{n-1}.

[Hint: show $B_n B_n = n I_{2^n}$]

Def The induced subgraph of $G=(V,E)$ on $S \subseteq V$ is defined as

$$G[S] = (S, E' = \{\{u,v\} \in E \mid u,v \in S\})$$

Ex Prove that

$$(\forall\, S \subseteq V(H_n) \text{ with } |S| \geq 2^{n-1}+1)$$

$$(\Delta(H_n[S]) \geq \sqrt{n})$$

[Hint: Cauchy interlacing on B_n and $\lambda_1(G) \leq \Delta(G)$]

[Huang's theorem] implies the Sensitivity Conjecture via a known connection of Gotsman and Linial

Recall

OP van Gogh prize

Show that (families) of Ramanujan graphs exist for <u>every</u> degree $d \geq 3$.

OP van Gogh prize

Signing Conjecture [Bilu-Linial]

Every d-regular graph $G=(V,E)$ has an edge signing $S: E \to \{\pm 1\}$ such that the signed adjacency matrix satisfies $eig(A_S) \subseteq [-2\sqrt{d-1}, 2\sqrt{d-1}]$.

(Positive answer would resolve the first OP on this page.)

Fourier Analysis

Def Let $S \subseteq [n]$. The character $\chi_S : \mathbb{Z}_2^n \to \{\pm 1\}$ is defined as

$$\chi_S(x) = \prod_{i \in S} (-1)^{x_i}.$$

Let $f, g : \mathbb{Z}_2^n \to \mathbb{R}$.

Def $\langle f, g \rangle = \mathbb{E}_{x \in \mathbb{Z}_2^n} f(x) g(x)$

(This is just a convenient normalization for Fourier analysis (different from before).)

Ex $\langle \chi_S, \chi_T \rangle = \begin{cases} 1 & S = T \\ 0 & \text{o/w} \end{cases}$

Ex $\{\chi_S\}_{S \subseteq [n]}$ form an ONB for the space of functions $\{f : \mathbb{Z}_2^n \to \mathbb{R}\}$.

Ex ∃! Fourier decomposition

$$f = \sum_{S \subseteq [n]} \hat{f}(S)\, \chi_S$$

where $\hat{f}(S) := \langle f, \chi_S \rangle$.

Ex $\chi_S(x+y) = \chi_S(x)\,\chi_S(y)$

[homomorphism $\mathbb{Z}_2^n \to \{\pm 1\}$]

Ex $\langle f, f \rangle = \sum_{S \subseteq [n]} \hat{f}(S)^2$

[Parseval]

Ex $\chi_\emptyset = 1$

Ex $\hat{f}(\emptyset) = \mathbb{E}_{x \in \mathbb{Z}_2^n} f(x)$

Ex $\mathrm{Var}[f] = \sum_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \hat{f}(S)^2$

Def The convolution of f and g is defined as

$$f * g(x) = \mathbb{E}_{y \in \mathbb{Z}_2^n} f(y) g(x-y).$$

Ex $\widehat{(f*g)}(S) = \hat{f}(S) \cdot \hat{g}(S)$

Def The degree of f is

$$\deg(f) = \max_{S : \hat{f}(S) \neq 0} |S| .$$

Def $\operatorname{dist}(f,g) = \Pr_{x \in \mathbb{Z}_2^n} [f(x) \neq g(x)]$

Ex If $f, g : \mathbb{Z}_2^n \to \{\pm 1\}$, then

$$\langle f, g \rangle = 1 - 2 \operatorname{dist}(f,g) .$$

Ex Let A be the adjacency matrix of H_n. Prove that

$$A \chi_S = (n - 2|S|) \chi_S$$

[Characters as eigenvectors]

Def 1 $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is linear if

$$f(x) = \sum_{i=1}^{n} c_i x_i \quad \text{for some } c \in \mathbb{Z}_2^n.$$

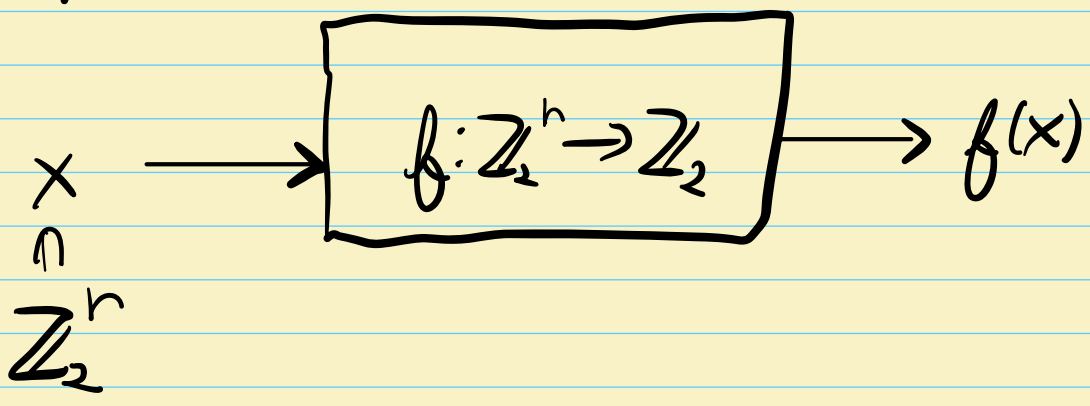
Def 2 $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is linear if

$$f(x) + f(y) = f(x+y) \quad \forall x, y \in \mathbb{Z}_2^n$$

Ex Def 1 $\iff$ Def 2.

Property Testing Model

Query



Def A property is a subset P of functions from $\{f : \mathbb{Z}_2^n \to \mathbb{Z}_2\}$

E.g. $P_{Lin} = \{$ linear functions $\}$

Def $dist(f, P) = \min_{g \in P} dist(f, g)$

Meta Question: Decide

(1) f has property P or

(2) f is ϵ-far from P.

Consider the following 3-query tester for linearity

(1) Sample $x, y \in \mathbb{Z}_2^n$ uniformly

(2) Accept iff $f(x) + f(y) = f(x+y)$.

Ex If f is linear, then tester accepts with probability 1.

For convenience let's think f maps to $\{\pm 1\}$ instead of $\mathbb{Z}_2$.

Def $\text{Prej}(f) = \Pr[\text{Tester rejects } f]$

Ex $\mathbb{E}_{x,y \in \mathbb{Z}_2^n} f(x) f(y) f(x+y) = 1 - 2\rho_{rej}(f)$

Ex $\rho_{rej}(f) \geq dist(f, P_{Lin})$

[Hint: Fourier analysis and convolution]

[BLR linearity testing]

Ex $\chi_S \cdot \chi_T = \chi_{S \Delta T}$

Complexity Measures

Let $f: \mathbb{Z}_2^n \to \{\pm 1\}$, $x \in \mathbb{Z}_2^n$

Def sensitivity of f at x

$$s(f,x) = |\{i \in [n] \mid f(x) \neq f(x+e_i)\}|$$

Def sensitivity of f

$$s(f) = \max_{x \in \mathbb{Z}_2^n} s(f,x)$$

Notation Let $B \subseteq [n]$. $x^B = x + \sum_{i \in B} e_i$

Def block sensitivity of f at x

$$bs(f,x) = \max\{k \mid \exists \text{ disjoint } B_1, \dots, B_k \subseteq [n] \text{ s.t. } f(x) \neq f(x^{B_i}) \ \forall i \in [k]\}$$

Def block sensitivity of f

$$bs(f) = \max_{x \in \mathbb{Z}_2^n} bs(f,x)$$

Ex $bs(f) \geq s(f)$

Ex* find f satisfying $bs(f) \geq \Omega(s(f)^2)$

Recall $deg(f) = \max_{S : \hat{f}(S) \neq 0} |S|$

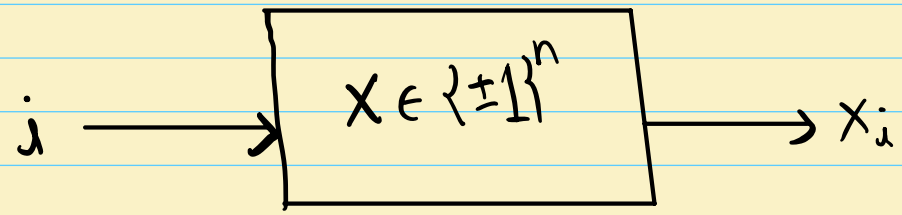
We say a polynomial $p(x_1, \dots, x_n)$ $\frac{1}{3}$-approximates $f : \{\pm 1\}^n \to \{0,1\}$ if

$$|p(x) - f(x)| \leq \frac{1}{3} \quad \forall x \in \{\pm 1\}^n$$

Def Approximate degree

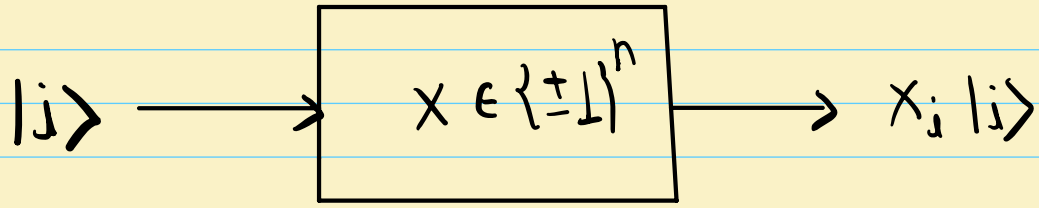
$$\widetilde{deg}(f) = \min \{ \text{degree}(p) \mid p \text{ } \tfrac{1}{3}\text{-approximates } f \}$$

Classical query model (viewed as a string)



[Think of n as very large]

Quantum query model (//)



O_x unitary

$O_x |i\rangle = x_i |i\rangle$

Decision Tree: Simplified computational model

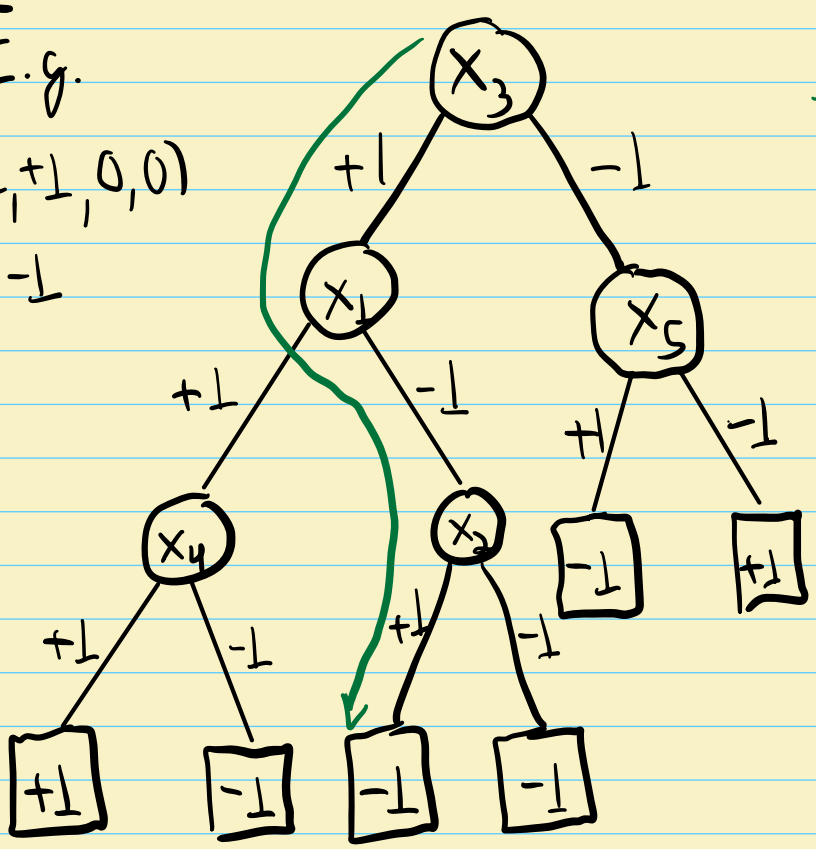
Input: $x = (x_1, \ldots, x_n)$

Internal nodes label query variables

E.g.

$x = (-1, +1, +1, 0, 0)$

output: -1



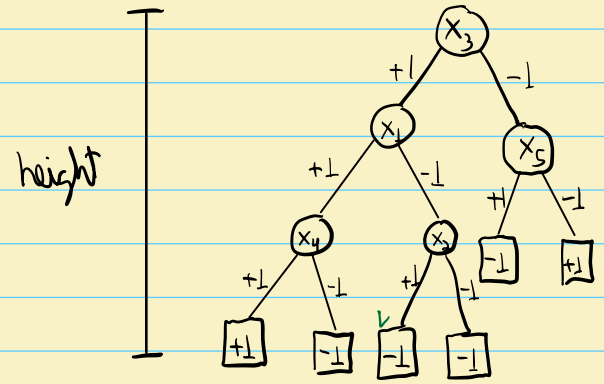
Start at the root and query input variables until leaf is reached

Leaves are labelled with output value of a computational path

Output: value of leaf reached by evaluating the decision tree

Def height(Tree) = length of a longest path from root to a leaf

E.g. for the previous example the height is 3



Def Decision tree complexity of f
(or classical query complexity)

$D(f) = \min\{\text{height}(T) \mid T \text{ is a tree computing } f\}$

Ex $D(f) \geq \deg(f)$

Quantum Query Model

Given $f: \Sigma_2^n \to \{0,1\}$, a t-query protocol specifies $t+1$ unitaries $U_0, \dots, U_t$,

$$\left(U_t O_x \cdots O_x U_1 O_x U_0 |0\rangle \right),$$

($|0\rangle$: starting state; t queries to the oracle)

Π_{acc} : projector onto accepting subspace,

$$p_{acc}(x) := \| \Pi_{acc} U_t O_x \cdots O_x U_1 O_x U_0 |0\rangle \|^2$$

such that

$$|p_{acc}(x) - f(x)| \leq 1/3 \quad \forall x \in \Sigma_2^n$$

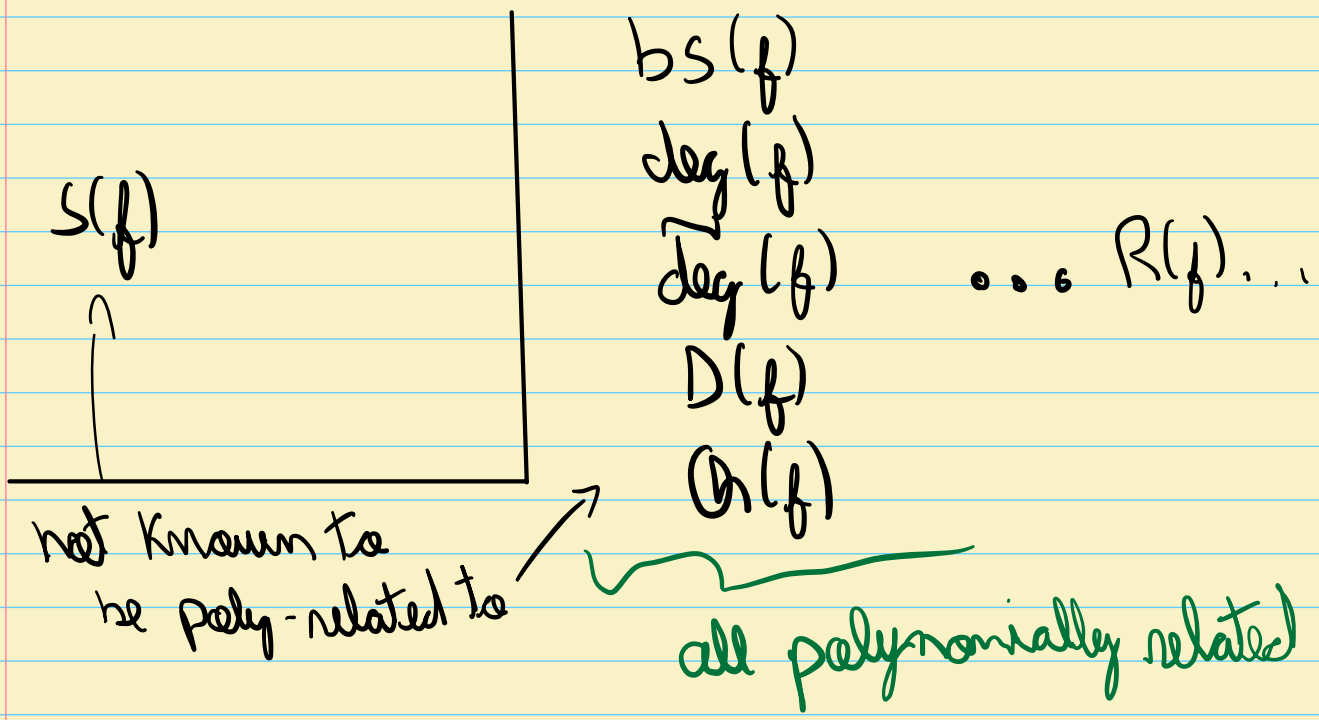
Ex $p_{acc}(x)$ is a polynomial of degree $\leq 2t$ in x.

Def Quantum query complexity of f

$$Q(f) = \min\{t \mid \exists \text{ quantum } t\text{-query protocol for } f\}$$

Ex $Q(f) \geq \frac{\widetilde{deg}(f)}{2}$

Before 2018



NS'90 [Sensitivity Conjecture]

$$bs(f) \leq poly(s(f))$$

Proved by Huang in 2018

Ex $D(f) \geq Ch(f)$

No superpolynomial quantum speed-up for total functions in the query model of computation

CH If f is a total function, then

$$Q(f) \geq D(f)^{\Theta(1)}.$$

OP Van Gogh prize

Find other efficient quantum algorithms for "useful" tasks with no known efficient classical algorithm (give "evidence" that none exist)

Group Theory Refresher

A group $(G, \cdot)$ is a set G with [notation overload]

a binary operation $\cdot$ satisfying

1) $g_1 \cdot g_2 \in G \quad \forall\, g_1, g_2 \in G$

2) $\exists\, 1 \in G$ s.t. $1 \cdot g = g \cdot 1 = g \quad \forall\, g \in G$

(existence of identity)

3) $\forall\, g \in G \;\exists\, g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = 1$

(existence of inverse)

4) $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3 \quad \forall\, g_1, g_2, g_3 \in G$

(associativity)

(We may use $g_1 g_2$ to denote $g_1 \cdot g_2$)

We say that $(G, \circ)$ is <u>Abelian</u> if

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \forall\ g_1, g_2 \in G.$$

(commutativity)

In this case, we may use '+' instead of '$\circ$'.

We may simply say G is group.

Cayley Graphs

Let G be a group and $S \subseteq G$.

$Cay(G, S)$ is the graph with vertex set $V = G$ and (directed) edge set

$$E = \{(g, sg) \mid g \in G, s \in S\}$$

Ex $H_n = Cay(\mathbb{Z}_2^n, \{e_1, \dots, e_n\})$

Ex $Cay(G, G)$ is the complete graph with self-loops

Ex $Cay(G, G \setminus \{1\})$ is $K_{|G|}$

Ex $Cay(G, \{1\})$ is the graph with only self-loops

Ex If $S = S^{-1}$, then $Cay(G, S)$ is undirected.

Ex The cycle graph C_n on n vertices is $Cay(\mathbb{Z}_n, \{\pm 1\})$.

Ex Generalize the definition of a character from $\mathbb{Z}_2$ to $\mathbb{Z}_3$ defining maps $\chi : \mathbb{Z}_3 \to \mathbb{C}$ that are homomorphisms to the complex unit circle

Ex Same question from before but now from $\mathbb{Z}_3$ to $\mathbb{Z}_n$

Ex If χ and ψ are characters, then so is $\chi \cdot \psi$.

Ex $\chi = 1$ is a (trivial) character

Ex If $\chi \neq 1$, then $\sum_{g \in G} \chi(g) = 0$.

Ex $\chi(g^{-1}) = \overline{\chi}(g)$

Ex $\frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, \psi(g) = \begin{cases} 1 & \text{if } \chi = \psi \\ 0 & \text{o/w} \end{cases}$

Ex* Generalize the definition of character to finite Abelian groups

Let A be the adjacency matrix of $Cay(G, S)$ for some Abelian group G.
Let $f : G \to \mathbb{C}$.

$$\text{Ex } (Af)(x) = \sum_{s \in S} f(sx)$$

Ex If χ is a character, then χ is an eigenvector

$$A\chi = \lambda \chi$$

with eigenvalue

$$\lambda = \sum_{s \in S} \chi(s) .$$

Ex Compute the eigenvalues of C_n

Ex Compute $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$ of C_n

Is it a good expander or not? (for large n)

Ex Compute the Cheeger constant of C_n.

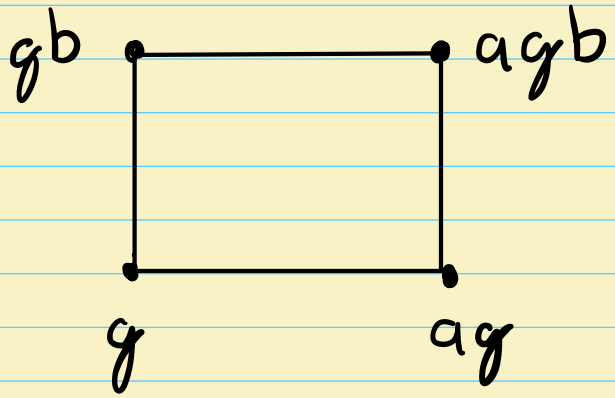
Ex Define a "right" Cayley graph with multiplication by a generator on the right

Ex Given two sets of generators $A, B \subseteq G$ define a "left-right" Cayley graph

$$\mathrm{Cay}(A, G, B)$$

Ex Find a "square" in $Cay(A, G, B)$

Hint:



$g \in G$

$a \in A$

$b \in B$

Pseudorandom Distributions

$\mathcal{F} \subseteq \{ f : \mathbb{F}_2^n \to \mathbb{F}_2 \}$ be a collection of functions to be "fooled"

Def We say that a distribution $\mathcal{D}$ on $\mathbb{F}_2^n$ ε-fools $\mathcal{F}$ if $\forall f \in \mathcal{F}$

$$\left| \Pr_{x \in \mathbb{F}_2^n} [f(x) = 1] - \Pr_{x \sim \mathcal{D}} [f(x) = 1] \right| \leq \varepsilon / 2.$$

Def We say that a distribution $\mathcal{D}$ on $\mathbb{F}_2^n$ is ε-biased if it ε-fools $\mathcal{F} = \{\chi_S \mid S \subseteq [n]\}$ (all characters).

Equivalently

$$\left| \mathop{\mathbb{E}}_{x \sim \mathcal{D}} \chi_S(x) \right| \leq \varepsilon \quad \forall \; \substack{S \neq \emptyset \\ S \subseteq [n]}.$$

Suppose $\mathcal{D}$ is an ε-biased distribution that is uniform on some multiset of $\mathbb{F}_2^n$

Ex Use $\mathcal{D}$ to define

$$Cay(\mathbb{Z}_2^n, \underbrace{?}_{\text{generating set}})$$

s.t. $\lambda(Cay(\mathbb{Z}_2^n, ?)) \leq \varepsilon$.

↑ (normalized) two-sided spectral expander

Ex Provide a converse transformation

Equivalent pseudorandom objects

ε-biased dist. $\Longleftrightarrow$ ε-expander

Coding Theory

$\Sigma = \{1, \dots, q\}$ alphabet (q-ary)

Def Any $\mathcal{C} \subseteq \Sigma^n$ is a code

n is the <u>blocklength</u>

Def (Normalized Hamming Distance) $x, y \in \Sigma^n$

$$\Delta(x,y) = \frac{1}{n} \sum_{i=1}^{n} 1_{[x_i \neq y_i]} \in [0,1]$$

Fundamental Parameters of $\mathcal{C}$

Def (Minimum Distance of $\mathcal{C}$)

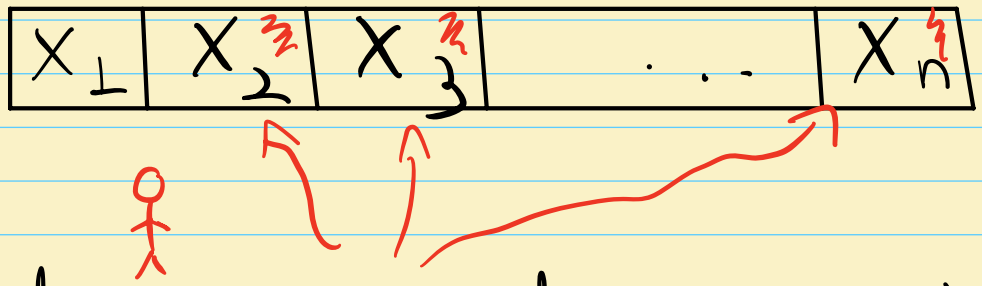
$$\Delta(\mathcal{C}) = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} \Delta(x,y) \in [0,1]$$

Def (Rate)

$$r(\mathcal{C}) = \frac{\log_q(|\mathcal{C}|)}{n} \in [0,1]$$

Error Model (Hamming)

$x \in \mathcal{C} \subseteq \Sigma^n$



Adversary can change symbols of x leading to some corrupted $\tilde{x} \in \Sigma^n$.

Def (Error) $x_i \neq \tilde{x}_i$

Ex If $\Delta(\mathcal{C}) = d/n$, then $\mathcal{C}$ can correct $\leq \lfloor \frac{d-1}{2} \rfloor$ adversarial errors

Coding Theory "Wish list"

Want $\mathcal{C} \subseteq \Sigma^n$ satisfying

- Both $\Delta(\mathcal{C})$ and $r(\mathcal{C})$ as large as possible (best rate-vs-distance trade-off)
- Efficient encoding
- Efficient (list) decoding
- Explicit construction
- Over small alphabets (ideally binary)
- Local properties (local testability, decodability, etc)

Achieving subsets of these wishes is wide open in many cases!

Def (Linear Code)

We say $\mathcal{C}$ is a linear code if $\Sigma = \mathbb{F}_q$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a <u>linear subspace</u>

Ex If $\mathcal{C}$ is linear and $\dim(\mathcal{C}) = k$, then $r(\mathcal{C}) = \frac{k}{n}$

Def (Normalized Hamming Weight) $x \in \Sigma^n$

$$|x| = \frac{1}{n} \sum_{i=1}^{n} 1_{[x_i \neq 0]}$$

Ex If $\mathcal{C}$ is linear, then

$$\Delta(\mathcal{C}) = \min_{\substack{x \in \mathcal{C} \\ x \neq 0}} |x|$$

Def $G \in \mathbb{F}_q^{n \times k}$ is a generating matrix of $\mathcal{C}$ if

$$\mathcal{C} = \text{im}(G)$$

Def $H \in \mathbb{F}_q^{(n-k) \times n}$ is a parity check matrix of $\mathcal{C}$ if

$$\mathcal{C} = \text{Ker}(H)$$

Ex If $\mathcal{C}$ is linear, $\mathcal{C}$ admits both a generating matrix and a parity check matrix.

Notation

$$\mathbb{F}_2^n = \{\alpha_1, \alpha_2, \dots, \alpha_{2^n}\}$$

Def (Hadamard Code)

$$\mathcal{H}_n = \{(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_{2^n})) \mid$$

$$f : \mathbb{F}_2^n \to \mathbb{F}_2 \text{ is linear}\}$$

$$N = 2^n$$

Ex $\mathcal{H}_n \subseteq \mathbb{F}_2^N$ is a linear code

Ex $\Delta(\mathcal{H}_n) = \frac{1}{2}$

Ex $r(\mathcal{H}_n) = \frac{n}{N}$

Ex Write a generating matrix for $\mathcal{H}_n$

Ex Write a parity check matrix for $\mathcal{H}_n$

[Hint: BLR]

Ex Show that $|\mathcal{H}_n|$ is optimal among binary linear codes with $\Delta(C) = \frac{1}{2}$.

Def (Dual Code) $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear

$$\mathcal{C}^\perp = \{ y \in \mathbb{F}_q^n \mid \langle y, x \rangle = 0 \ \forall x \in \mathcal{C} \}$$

Ex $\mathcal{C}^\perp$ is a linear code

Ex $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = n$

Ex If H is the parity check of $\mathcal{C}$, then $\mathcal{C}^\perp = \text{row span}(H)$

Ex H^T is the generating matrix of $\mathcal{C}^\perp$

Def (Polynomials of degree $\leq t$)

$$\mathbb{F}_q^{\leq t}[X] = \{ c_0 + c_1 X + \dots + c_t X^t \mid c_0, \dots, c_t \in \mathbb{F}_q \}$$

Let $k \leq n \leq q$

$$\Gamma = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq \mathbb{F}_q$$

(distinct)

Def (Reed - Solomon Code)

$$RS_\Gamma(k, n) = \{ (p(\alpha_1), \dots, p(\alpha_n)) \mid p \in \mathbb{F}_q^{\leq k-1}[X] \}$$

Extremely Important Fact

"Low degree polynomials have few roots"

Ex If $p \in \mathbb{F}_q^{\leq t}[X]$, then

$$|\{\alpha \in \mathbb{F}_q \mid p(\alpha) = 0\}| \leq t.$$

Ex $RS_\Gamma(K, n) \subseteq \mathbb{F}_q^n$ is a linear code

Ex $\Delta(RS_\Gamma(K, n)) \geq \frac{n-K+1}{n}$

Ex $r(RS_\Gamma(K, n)) = \frac{K}{n}$

Ex Write a generating matrix for $RS_q(k,n)$

[Hint: Vandermonde]

Ex Prove a rank lower bound on $l \times l$ submatrices (of the previous matrix) for $l \leq k$.

Ex Given $p \in \mathbb{F}_q^{k-1}[X]$, how many evaluation points are needed to interpolate it?

A General Code Upper Bound

Ex Any $\mathcal{C}$ with

$\Delta(\mathcal{C}) = d/n$ and

$r(\mathcal{C}) = k/n$ must

satisfy $k + d \leq n + 1$

(Singleton Bound)

Ex $RS_{\mathbb{F}}(k, n)$ meets this bound

(optimality of RS codes)

Finite Fields: Properties

Ex $\alpha^q = \alpha \quad \forall \alpha \in \mathbb{F}_q$

$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

Ex $\exists \gamma \in \mathbb{F}_q^*$ s.t.

$$\mathbb{F}_q^* = \{\gamma^i \mid i \in \mathbb{N}\}$$

(Cyclic Property)

Ex $\sum_{\alpha \in \mathbb{F}_q} \alpha^i = 0$ for $1 \leq i < q-1$

Ex Compute $RS_\Gamma(k,n)^\perp$

Ex Write the parity check of $RS_\Gamma(k,n)$

Def (Good codes)

We say that a family of codes (with $n \to \infty$) is <u>good</u> if

$$\Delta(\mathcal{C}) \geq \delta_0 = \Omega(1)$$

$$r(\mathcal{C}) \geq r_0 = \Omega(1)$$

for every $\mathcal{C}$ in the family

Def (ε-balanced code)

We say a linear binary code $\mathcal{C}$ is ε-balanced if $\forall\, 0 \neq x \in \mathcal{C}$

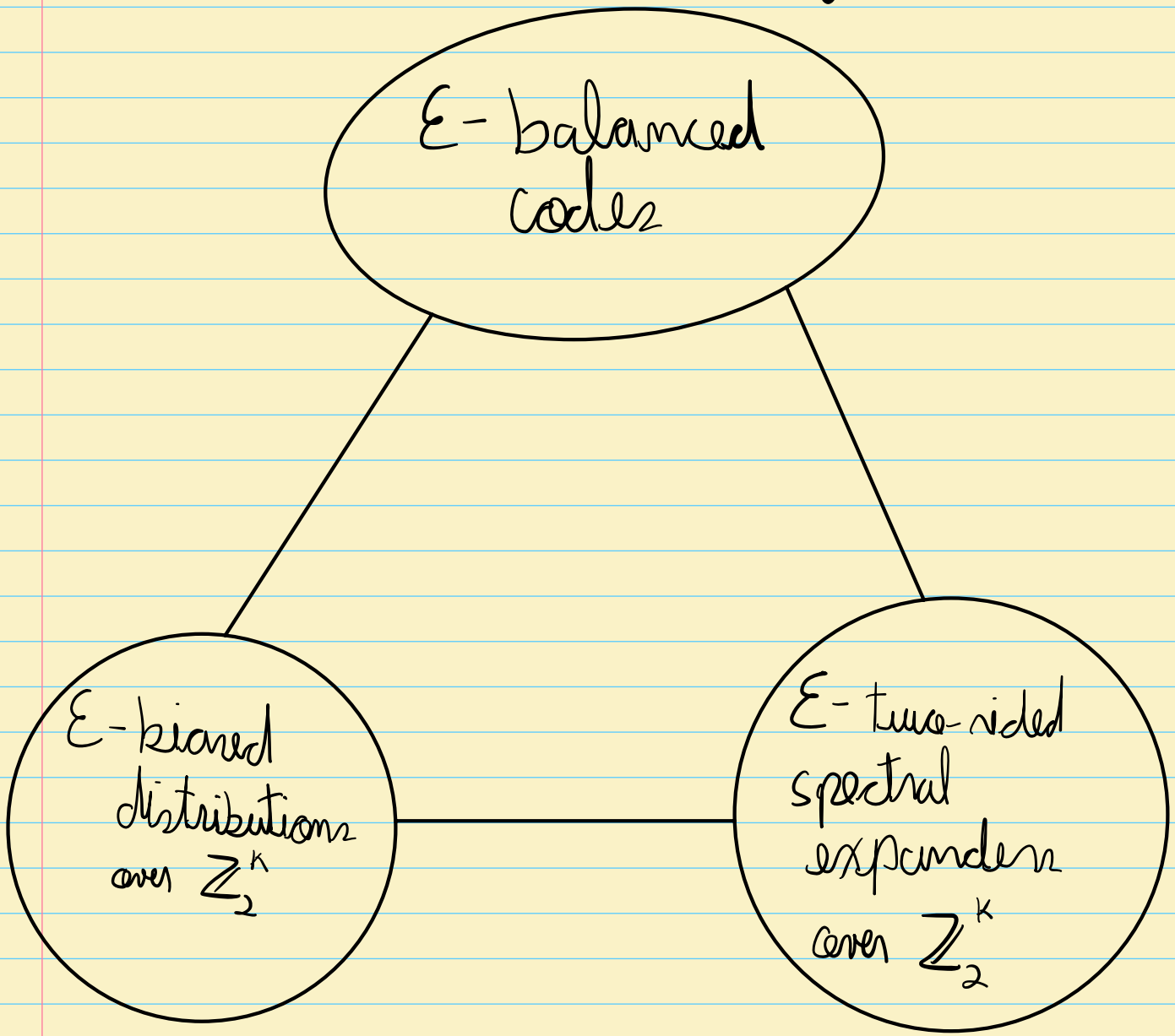
$$|X| \in \left[\frac{(1-\varepsilon)}{2}, \frac{(1+\varepsilon)}{2} \right].$$

Ex Starting from an ε-biased distribution $\mathcal{D}$ on $\mathbb{F}_2^k$ define an ε-balanced code $\mathcal{C} \subseteq \mathbb{F}_2^n$.

[Hint: $\dim(\mathcal{C}) = k$]

Equivalence Triad of Pseudorandom Objects

Ex Formalize all the equivalences:



Entropy and Volume

Def (Hamming Ball) $x \in \Sigma^n, \delta \in [0,1]$

$$B_q(x, \delta \cdot n) = \{ y \in \Sigma^n \mid \Delta(x,y) \leq \delta \}$$

$$\text{Ex } |B_q(0, \delta \cdot n)| = \sum_{i=0}^{\lfloor \delta \cdot n \rfloor} \binom{n}{i} (q-1)^i$$

Ex Fix $\delta \in (0, \frac{1}{2}]$, find

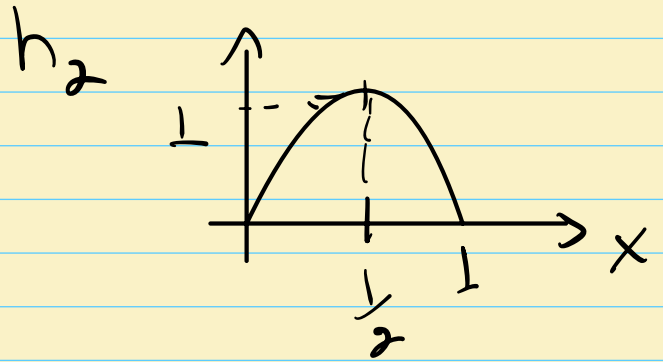
a function $f : [0,1] \to [0,1]$ s.t.

$$\lim_{n \to \infty} \frac{\log |B_2(0, \delta \cdot n)|}{f(\delta)\, n} = 1$$

[Hint: look ahead if very stuck]

Def (Binary Entropy) $h_2 : [0,1] \to [0,1]$

$$h_2(x) = x \log_2\left(\frac{1}{x}\right) + (1-x)\log_2 \frac{1}{(1-x)}$$



Ex

$$2^{(h_2(\delta) - o_n(1))n} \leq |B_2(0, \delta \cdot n)| \leq 2^{h_2(\delta) n}$$

Ex Define the q-ary entropy by analogy with the binary case

Another Code Upper Bound

Ex If $\mathcal{C} \subseteq \Sigma^n$ with $\Delta(\mathcal{C}) \geq d/n$, then

$$|\mathcal{C}| \leq \frac{q^n}{|B(0, L\frac{d-1}{2}\rfloor)|}.$$

(Hamming Bound)

$d = \delta \cdot n$ for $\delta \in [0, 1 - \frac{1}{q})$

Ex $r(\mathcal{C}) \leq 1 - h_q(\delta/2) + o_n(1)$

(Asymptotic Hamming Bound)

A Code Lower Bound

Ex Show that $\exists\ \mathcal{C} \subseteq \Sigma^n$ with

$$\Delta(\mathcal{C}) \geq d/n \quad \text{and}$$

$$r(\mathcal{C}) \geq 1 - \frac{\log_q(|B_q(0, d-1)|)}{n}$$

(Gilbert-Varshamov Bound)
or
GV Bound

Give two different proofs:

(1) Greedy Construction

(2) Random Construction

$d = \delta \cdot n \qquad \delta \in [0, 1 - 1/q)$

Ex $\exists\, \mathcal{C}$ with $A(\mathcal{C}) \geq \delta$ and

$$r(\mathcal{C}) \geq 1 - h_q(\delta) - o_n(1)$$

(Asymptotic GV Bound)

Ex Show that a random linear code achieves the GV bound whp

(Hint: sample a generating matrix)

Ex If $\delta = \frac{(1-\varepsilon)}{2}$, then the code from the previous problem is ε-balanced whp

OP van Gogh Prize

Construct <u>explicit</u> binary codes achieving the GV bound ($\delta \in [0, \frac{1}{2})$, $n \to \infty$)

OP van Gogh Prize

In the GV bound asymptotically (up to $o_n(1)$ additive term) the best possible rate-vs-dist. trade-off for binary codes?

(Again for fixed $\delta \in [0, 1/2)$ and $n \to \infty$)

Tensor Codes

Let $C_A \subseteq \mathbb{F}_q^{n_A}$ and $C_B \subseteq \mathbb{F}_q^{n_B}$ be linear codes

Def (Tensor Code)

$$C_A \otimes C_B = \{ M \in \mathbb{F}_q^{n_A \times n_B} \mid \text{every col of } M \text{ belongs to } C_A \text{ and every row of } M \text{ belongs to } C_B \}$$

Ex $C_A \otimes C_B$ is linear

Ex Compute $\Delta(C_A \otimes C_B)$ in terms of $\Delta(C_A)$ and $\Delta(C_B)$

Ex Compute $r(C_A \otimes C_B)$ // $r(C_A)$ and $r(C_B)$

Def (LDPC)

We say that $\mathcal{C}$ is a low-density parity check code if it admits a parity check matrix H with at most $b_0 = O(1)$ non-zero entries per row and per column.

(of course, this is for a family of codes)

To be continued...