

Discovering the Foundations of Theoretical Computer Science

(Fernando Granha Jeronimo)

Under heavy construction

Last update: 10/11/24

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.,

$$A \in \mathbb{R}^{n \times n}, \quad A_{u,v} = \begin{cases} 1 & [u,v] \in E \\ 0 & \text{otherwise} \end{cases}.$$

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 .

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

Ex $x \in \mathbb{R}^n$ and $\ell_1, \dots, \ell_n \in \mathbb{R}^n$

We can write

$$x = \sum_{i=1}^n \alpha_i \ell_i \quad \text{with } \alpha_i = \langle \ell_i, x \rangle.$$

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

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

Ex A sym $\Rightarrow A$ has real eigenvalues

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

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

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

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

Ex If G is simple with $\deg \geq 1$

$$\downarrow \\ \lambda_n < 0$$

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

Def $J_n = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$ 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 $\Leftrightarrow \text{Spec}_{\parallel}(G) = \text{Spec}(G)$.

Some Notions of Expansion

$$\text{Def } \partial(S) = E(S, \bar{S})$$

"Edge boundary"

$$\text{Def } \Phi(S) = \frac{|\partial(S)|}{|S|}$$

"Conductance"

$$\text{Def } \Phi(G) = \min_{\substack{\emptyset \neq S \subseteq V \\ |S| \leq n/2}} \Phi(S)$$

"Cheeger's constant"

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

two-sided spectral expansion

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

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

Ex Prove that

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

[Expander Mixing Lemma]

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

Def $\alpha(G)$ = independence number

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

[Hoffmann's bound]

Ex Prove that $\text{clawy} \leq \lambda_1 \leq \Delta(G)$

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

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

[Witj's bound]

Mixing Bounds

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

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

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

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

[Mixing bound]
in l_1

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

Eigenvalues as an optimization problem

Let $V_K = \text{Span}\{\varphi_1, \dots, \varphi_K\}$

$W_K = \text{Span}\{\varphi_{K+1}, \dots, \varphi_n\}$

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

$$\lambda_K = \max_{V \subseteq \mathbb{R}^n} \min_{0 \neq x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \min_{V \subseteq \mathbb{R}^n} \max_{0 \neq x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}$$

$\dim(V) = K$ $\dim(V) = n - K + 1$

[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]

Refresher on PSDness

Def A real sym matrix M is positive semi-definite (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. $M = W^T W$

Notation We write $M \succ 0$ if M is PSD

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

This gives a partial order (Lacumon order)

Laplacian Matrix

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

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

Ex For d -regular G , we have

$$\mu_1 = d - \lambda_1, \dots, \mu_n = d - \lambda_n.$$

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

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

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

Ex G connected $\Leftrightarrow \mu_2 > 0$

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

$E \times K \times \{ \mu_k = 0 \} | = \# \text{ of connected components}$

Ex G bipartite iff $\mu_n = 2d$

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

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

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

[Cheeger's Inequality]

$$\frac{\mu_2}{2d} \leq \Phi(6) \leq \sqrt{\frac{2\mu_2}{d}}$$

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

Hint: [Cayley-Hamilton] minimal polynomial

Ex Let A, B be two real sym
matrices with $\text{eig}(A) \geq \dots \geq \lambda_n$
 $\text{eig}(B) \geq \dots \geq \tilde{\lambda}_n$

Compute the eigenvalues of $A \otimes B$.

Def $s: E \rightarrow \{-1\}$ 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 $\lambda_1(A_s) \leq \Delta(B)$ for any
signing s .

Limitations on Spectral Expansion

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

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]

 Ch*

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

[Alon-Boppana bound]

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

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

Def 6 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 Losslen) Expansion

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

$$\underline{\Phi}_\epsilon^V(\epsilon) = \min_{\substack{\emptyset \neq S \subseteq V \\ |S| \leq \epsilon n}} \underline{\Phi}^V(S).$$

OP [van Gogh prize]

Construct explicit family with

$$\underline{\Phi}_\epsilon^V(\epsilon) > \frac{1}{2} \quad \text{for } \epsilon = \Omega(1)$$

(on two-sided bipartite forest)

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
 $\bar{\Phi}(S) \leq \eta$.

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

OP Van Gogh ping

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

$$E = \{(u, u + e_j) \mid u \in \mathbb{Z}_2^n, j \in [n]\}$$

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

$$A_L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_n = \begin{pmatrix} A_{n-1} & I_{2^{n-1}} \\ I_{2^{n-1}} & A_{n-1} \end{pmatrix}.$$

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

$$G \square H = (V = V(G) \times V(H),$$

$$E = \{(g_1, h_1), (g_2, h_2) \mid$$

$(g_1, g_2) \in E(G)$ and $h_1 = h_2$ or

$(g_1 = g_2 \text{ and } h_1, h_2) \in E(H)\}$

Ex Prove that $H_n = \underbrace{\circ \square \circ \square \dots \square \circ}_{n \text{ times}}$

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

$$\text{Spec}(A_{G \square H}) = \left\{ \lambda + \tilde{\lambda} \mid \begin{array}{l} \lambda \in \text{Spec}(G), \\ \tilde{\lambda} \in \text{Spec}(H) \end{array} \right\}$$

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

Ex Consider the recursive edge

Signing of H_n

$$B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B_n = \begin{pmatrix} B_{n-1} & I_{2^{n-1}} \\ I_{2^{n-1}} & -B_{n-1} \end{pmatrix}$$

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
every degree $d \geq 3$.

OP van Gogh prize

Signing Conjecture [Bilu-Linial]

Every d -regular graph $G = (V, E)$

has an edge signing $S: E \rightarrow \{-1\}$

such that the signed adjacency matrix

satisfies $\text{eig}(A_S) \subseteq [-2\sqrt{d-1}, 2\sqrt{d-1}]$.

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

Fourier Analysis

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

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

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

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

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

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

$E_x \{X_S\}_{S \subseteq [n]}$ form an ONB

for the space of functions $\{f: \mathbb{Z}_2^n \rightarrow \mathbb{R}\}$.

$E_x \exists!$ Fourier decomposition

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

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

$$E_x X_S(x+y) = X_S(x) X_S(y)$$

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

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

[Parseval]

$$\mathbb{E}_x \chi_{\emptyset} = 1$$

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

$$\mathbb{E}_x \text{Var}[f] = \sum_{\substack{S \subseteq [n] \\ S \neq \emptyset}} \hat{f}(S)^2$$

Def The convolution of f and g is defined as

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

$$\mathbb{E}_x (\widehat{f * g})(S) = \hat{f}(S) \cdot \hat{g}(S)$$

Def The degree of f is

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

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

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

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

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

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

[Character as eigenvectors]

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

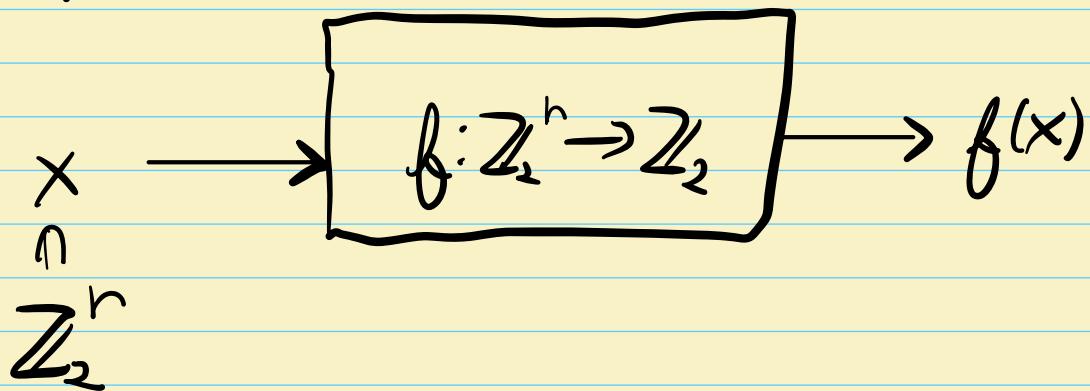
$$f(x) = \sum_{i=1}^n c_i x_i \quad \text{for some } c \in \mathbb{Z}_2^n.$$

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

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

Ex Def 1 \Leftrightarrow Def 2.

Property Testing Model
Query



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

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

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

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 $\{+1\}$ instead of \mathbb{Z}_2 .

If $\text{Proj}(f) = \Pr[\text{Tester rejects } f]$

$$\mathbb{E}_x \mathbb{E}_{\substack{x,y \in \mathbb{Z}_2^n \\ f(x), f(y) \neq f(x+y)}} f(x)f(y) = 1 - 2\text{Proj}(f)$$

$$\mathbb{E}_x \text{Proj}(f) \geq \text{dint}(f, P_{\text{Lim}})$$

[Hint: Fourier analysis and convolution]

[BLR linearity testing]

$$\mathbb{E}_x \chi_S \cdot \chi_T = \chi_{S \Delta T}$$

Complexity Measures

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

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

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

Def block sensitivity of f

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

$$\text{Ex } bs(f) \geq s(f)$$

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

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

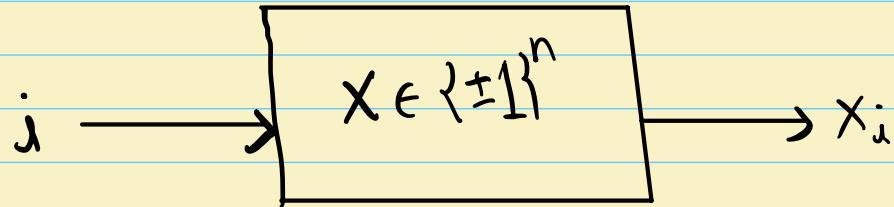
We say a polynomial $p(x_1, \dots, x_n)$ $\frac{1}{3}$ -approximates $f: \{-1\}^n \rightarrow \{0, 1\}$ if

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

Def Approximate degree

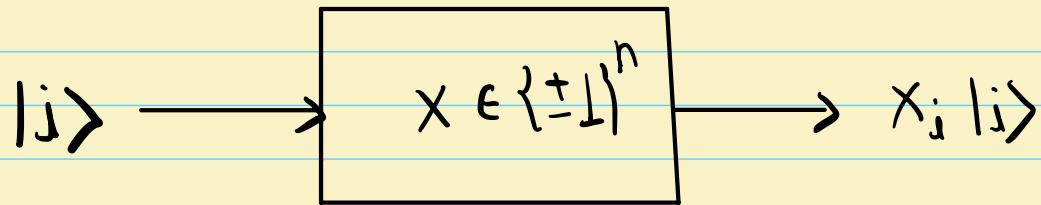
$$\tilde{\deg}(f) = \min \{ \deg(p) \mid p \text{ } \frac{1}{3}\text{-approximates } f \}$$

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

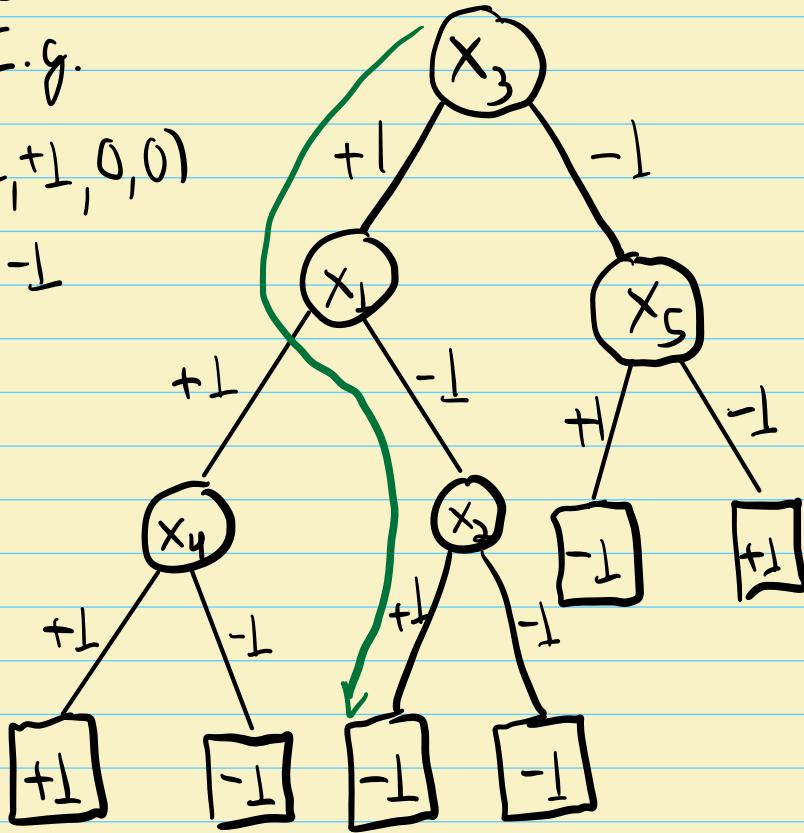
Input: $x = (x_1, \dots, x_n)$

Internal nodes label query variables

E.g.

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

output: -1



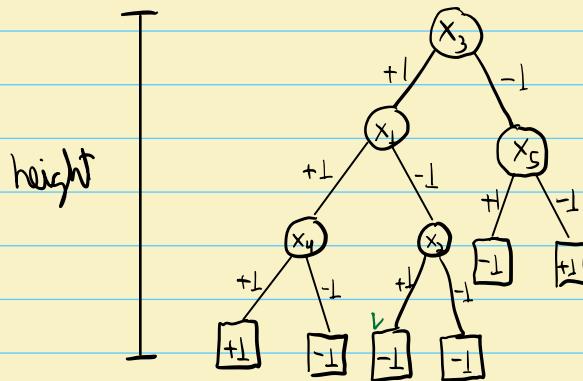
Start at the root
and query input
variables until
leaf is reached

Leaves are labelled with output value
of a computational path

Output: value of leaf reached by evaluating
the decision tree

Def $\text{height}(\text{Tree})$ = 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 $f: \mathbb{Z}_2^n \rightarrow \{0,1\}$, a t -query protocol
specifies $t+1$ unitaries U_0, \dots, U_t ,

$$\left(U_t O_x \dots O_x U_1 O_x U_0 |0\rangle \begin{array}{c} \\ \swarrow \quad | \quad \searrow \\ t \text{ queries to the oracle} \end{array} \right)$$

Starting state

Π_{acc} : projector onto accepting subspace,

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

such that

$$|p_{\text{acc}}(x) - f(x)| \leq \frac{1}{3} \quad \forall x \in \mathbb{Z}_2^n$$

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

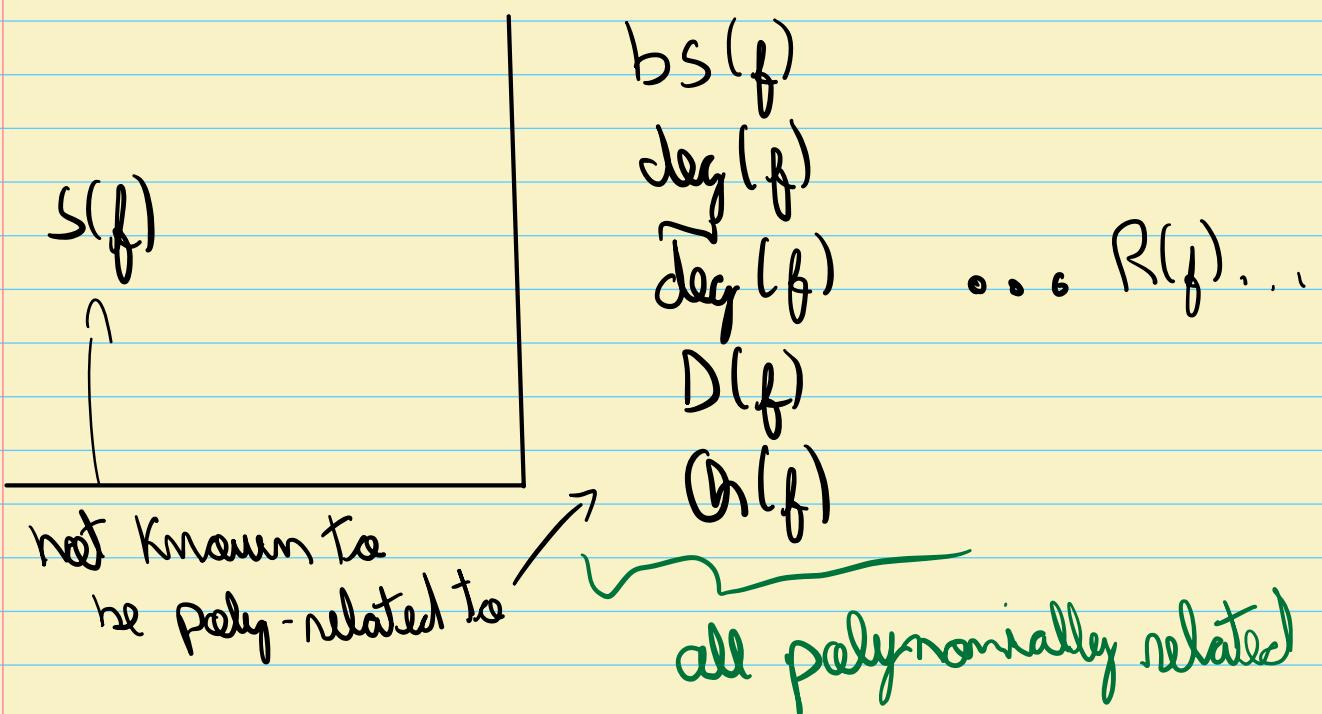
Def Quantum query complexity of f

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

for f

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

Before 2018



NS'90 [Sensitivity Conjecture]

$$bs(f) \leq \text{poly}(S(f))$$

Proved by Muraug in 2018

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

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

 If f is a total function, then

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

OP Van Graph prize

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

Group Theory Refresh

A group (G, \circ) is a set G with

a binary operation ' \circ ' satisfying

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

$$2) \exists 1 \in G \text{ s.t. } 1 \circ g = g \circ 1 = g \quad \forall g \in G$$

(existence of identity)

$$3) \forall g \in G \exists g^{-1} \in G \text{ s.t. } g \circ g^{-1} = g^{-1} \circ g = 1$$

(existence of inverse)

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

(associativity)

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

We say that (G, \circ) is Abelian 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 $S \subseteq G$.

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

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

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

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

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

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

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

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

Ex Generalize the definition of a character from \mathbb{Z}_2 to \mathbb{Z}_3 defining maps $\chi: \mathbb{Z}_3 \rightarrow \mathbb{C}$ 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 $\chi(g^{-1}) = \bar{\chi}(g)$

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

Ex* Generalize the definition of character to finite Abelian groups

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

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

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 .

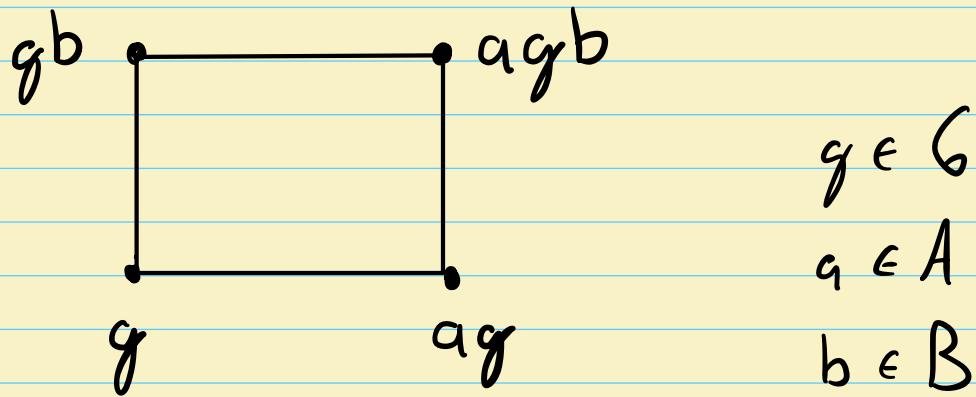
Ex Define a "right" Cayley graph with
multiplication by a generator on the right

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

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

Ex Find a "square" in $\text{Cay}(A, G, \beta)$

Hint:



$$g \in G$$

$$a \in A$$

$$b \in B$$

Pseudorandom Distributions

$\mathcal{F} \subseteq \{f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2\}$ be a collection
of functions to be
“foaled”

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

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

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

Equivalently

$$\left| \mathbb{E}_{x \sim \mathcal{D}} X_S(x) \right| \leq \epsilon \quad \forall S \neq \emptyset, S \subseteq [n].$$

Suppose \mathcal{D} is an ϵ -biased distribution that is uniform of

some multiset of \mathbb{F}_2^n

Ex Use \mathcal{D} to define

$$\text{Cay}(\mathbb{Z}_2^n, \underline{\square})$$

generating net

r.t. $\lambda(\text{Cay}(\mathbb{Z}_2^n, \underline{\square})) \leq \epsilon.$

\uparrow (normalized)

two-sided spectral
expander

Ex Provide a converse transformation

Equivalent pseudorandom objects
 ϵ -biased dist. \iff ϵ -expander

Coding Theory

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

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

n is the blocklength

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

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

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

Parameters
of \mathcal{C}

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

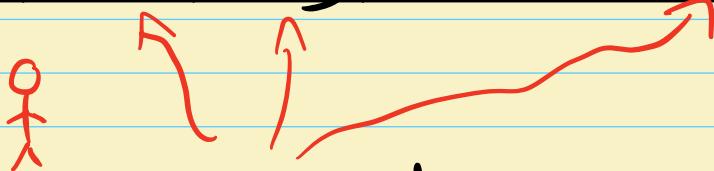
Def (Rate)

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

Error Model (Hamming)

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

x_1	x_2	x_3	\dots	x_n
-------	-------	-------	---------	-------



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

$$\text{Ref (Error)} \quad x_i \neq \tilde{x}_i$$

Ex if $\Delta(\mathcal{E}) = \frac{d}{n}$, then \mathcal{E}

can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ adversarial error

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 $\Sigma = \mathbb{F}_q^n$
and $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a linear subspace

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

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

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

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 ℓ if

$$\ell = \text{im}(G)$$

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

$$\ell = \text{Ker}(H)$$

Ex If ℓ is linear, ℓ 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)

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

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

$$N = 2^n$$

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

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

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

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 $\Delta(e) = \frac{1}{2}$.

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

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

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 $\leq t$)

$$\mathbb{F}_q^{< t}[x] = \{ c_0 + c_1 x + \dots + c_t x^t \mid$$

$$c_0, \dots, c_t \in \mathbb{F}_q \}$$

Let $k \leq n \leq q$

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

(distinct)

Def (Reed - Solomon Code)

$$RS_p(k, n) = \{(p(\alpha_1), \dots, p(\alpha_n))\}$$

$$p \in \mathbb{F}_q^{< k-1}[x]$$

Extremely Important Fact

"Low degree polynomials have few roots"

Ex If $p \in F_q^{< t}[x]$, then

$$|\{x \in F_q \mid p(x) = 0\}| \leq t.$$

Ex $RS_{\Gamma}(k, n) \subseteq F_q^n$ is a

linear code

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

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

Ex Write a generating matrix for $RS_{\Gamma}(k, n)$

[Hint: Vandermonde]

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

Ex Given $p \in F_q^{k-1}[x]$,

how many evaluation points are needed to interpolate it?

A General Coder Upper Bound

Ex Any C with

$$\Delta(C) = \frac{d}{n} \quad \text{and}$$

$$r(C) = \frac{k}{n} \quad \text{ment}$$

Satisfy $k + d \leq n + 1$

(Singleton Bound)

Ex $RS_F(k, n)$ meets this bound

(optimality of RS coder)

Finite Field Properties

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

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

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

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

(Cyclic Property)

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

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 $n \rightarrow \infty$) is good 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)

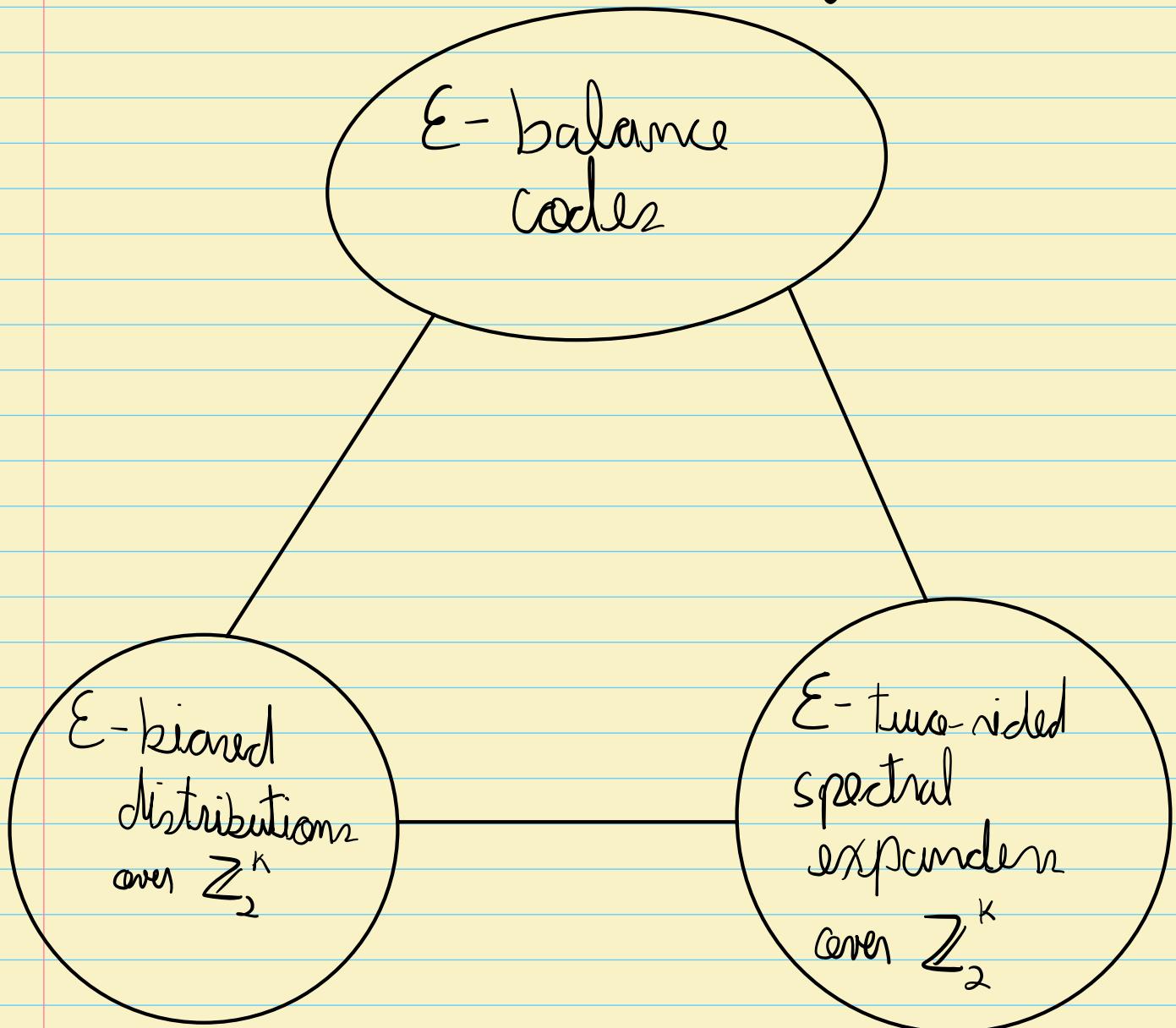
We say a linear binary code C is ϵ -balanced if $\forall 0 \neq x \in C$

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

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

Equivalence Triad of Pseudorandom Objects

Ex Formalize all the equivalences:



Entropy and Volume

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

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

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

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

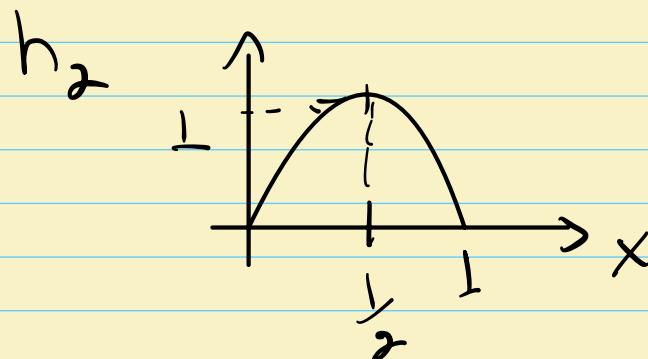
a function $f: [0,1] \rightarrow [0,1]$ s.t.

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

[Hint: look ahead if very stuck]

Ref (Binary Entropy) $h_2 : [0, 1] \rightarrow [0, 1]$

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



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

Ex Refine the α -ary entropy

by analogy with the binary case

Another Code Upper Bound

Ex If $\mathcal{C} \subseteq \Sigma^n$ with

$A(e) \geq d/n$, then

$$|e| \leq \cancel{g^n} |B(0, L^{\frac{d-1}{2}})|$$

(Hamming Bound)

$$d = \lambda \cdot n \quad \text{for } \lambda \in [0, 1 - \frac{1}{g}]$$

$$\text{Ex } r(e) \leq 1 - h_g(\lambda/2) + o_n(1)$$

(Asymptotic Hamming Bound)

A Code Lower Bound

Ex Show that $\exists e \subseteq \Sigma^n$ with

$$\Delta(e) \geq d/n \quad \text{n.t.}$$

$$r(e) \geq 1 - \frac{\log_2 (|B_f(0, d-1)|)}{n}$$

(Gilbert-Venhamov Bound)
or
GV Bound

Give two different proofs:

(1) Greedy Construction

(2) Random Construction

$$d = 2 \cdot n \quad \delta \in [0, 1 - \frac{1}{q})$$

$E_x \exists e \text{ with } A(e) \geq \delta \text{ s.t.}$

$$r(e) \geq 1 - h_q(\delta) - o_n(1)$$

(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 w.h.p.

OP van Gogh Prize

Construct explicit binary codes
achieving the GV bound ($\delta \in [0, \frac{1}{2}]$)
 $n \rightarrow \infty$

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 $\delta \in [0, \frac{1}{2}]$ and)
 $n \rightarrow \infty$

Tensor Coder

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 $r(C_A \otimes C_B) // r(C_A) \text{ and } r(C_B)$

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 ...