ICTS HDX and Codes

Coding

Lecturer: Swastik Kopparty

Abhinav

Error-correcting Codes

28/04

Lec-1

Σ finite set, "alphabet"
$\{0,1\}$

Σ^n all asymptotics in $n \to \infty$

Hamming metric $\Delta(x,y) = \#$ coordinates where x, y differ

Def: ECC
A subset of Σ^n

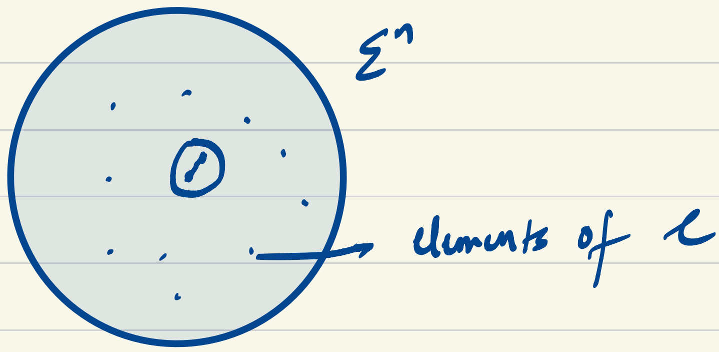
Let $\mathcal{C}$ be an ECC.

Key things about $\mathcal{C}$.
1) $|\mathcal{C}|$
2) How far apart the elements of $\mathcal{C}$ are

Def: Min. dist of $\mathcal{C}$

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

Observation: If $\mathcal{C}$ has min. dist d,
$x \in \mathcal{C}$
$y \in \Sigma^n$ s.t $\Delta(x,y) < \frac{d}{2}$, then
x is uniquely determined by y.



Key Question:

How big can $\mathcal{C}$ be if we want the min. dist of $\mathcal{C}$ to be d?

Packing balls of radius $\frac{d}{2}$ in Σ^n.

Good setting:

$d = \delta n$
or
$\delta = O(1)$

Volume Packing Bound (Hamming Bound)

If $\mathcal{C}$ has min. dist d, then

$$|\mathcal{C}| \le \frac{|\Sigma|^n}{|\mathrm{Vol}(B_n(d/2))|}$$

$\Sigma = \{0,1\}$; $\quad |\mathcal{C}| \le \dfrac{2^n}{\binom{n}{0} + \dots + \binom{n}{\lfloor \frac{d-1}{2} \rfloor}}$

$$|\mathcal{C}| \le \begin{cases} O\left(\dfrac{2^n}{n^{\lfloor \frac{d-1}{2} \rfloor}}\right) & d = O(1) \\ 2^{(1 - H(\frac{\delta}{2}))n + o(n)} & d = \delta \cdot n \end{cases}$$

Elias-Bassalygo bound
(related to list-decoding)
LP-bound

$\left(\delta \in (0, \tfrac{1}{2}) : \binom{n}{\delta n} \approx 2^{(h_\delta + o(1))n} \right)$

eg $d = 3$, ECC that can correct 1 error

$$|\mathcal{C}| \leq \frac{2^n}{n+1}$$

__Greedy Existence result__

$\exists\ \mathcal{C} \subseteq \Sigma^n$ with min. dist d with

$$|\mathcal{C}| \geq \frac{|\Sigma|^n}{\mathrm{Vol}(B(d-1))}$$

$d = 3$, $\Sigma = \{0, 1\}$

$\exists\ \mathcal{C}$ with $|\mathcal{C}| \geq \Theta\left(\frac{2^n}{n^2}\right)$

__Hamming Codes__ : $\exists\ \mathcal{C}$ with $|\mathcal{C}| \geq \Theta\left(\frac{2^n}{n}\right)$

BCH Codes : amazing codes for $\Sigma = \{0, 1\}$, $d = O(1)$

__Algorithmic Questions__:

- Give an efficient construction of an ECC with $|\mathcal{C}|$ big.
- Find $\mathcal{C}$ and an algorithm that runs in time $\mathrm{poly}(n, \log|\Sigma|)$ that maps $\{1, 2, \ldots, |\mathcal{C}|\} \to \mathcal{C}$ bijectively.

Linear Codes

If $\Sigma = (\mathbb{F}_q)^s$, then

$$\Sigma^n \cong \mathbb{F}_q^{ns}$$

and $\mathcal{C} \subseteq \Sigma^n$ is an $\mathbb{F}_q$-linear subspace.

Linear codes are automatically efficiently encodable "given" the code.

- **Decoding**: Given $y \in \Sigma^n$ with the promise that $\Delta(x, y) < \frac{d}{2}$ for some $x \in \mathcal{C}$.

  Find x efficiently. $(\text{poly}(n, \log|\Sigma|))$

Let $\mathcal{C}$ be a linear code. $\Sigma = \mathbb{F}_q^s$
$\mathcal{C} \subseteq (\mathbb{F}_q)^s$

Let $k = \dim(\mathcal{C})$
$= \#$ of $\mathbb{F}_q$-information symbols in $\mathcal{C}$

$R =$ Rate of $\mathcal{C} = k/_{sn}$ (s is usually 1)

Encoding Map
Linear Bijection $E: \mathbb{F}_q^k \to \mathcal{C}$

Local Testing | Checking membership

Local Decoding | Given $y \in \Sigma^n$, is $y \in \mathcal{C}$?

Easy for linear codes

The Best Code

Reed-Solomon Codes

$\Sigma = \mathbb{F}_q$

$n = q$

List $\mathbb{F}_q : \{\alpha_1, \ldots, \alpha_n\}$

$\mathcal{C} = \{(P(\alpha_1), P(\alpha_2), \ldots, P(\alpha_n))\}$
where $P(x) \in \mathbb{F}_q[x]$ is a poly of deg $\leq k$.

$|\mathcal{C}| = q^{k+1}$

$|\mathcal{C}|$ is linear, $\dim(\mathcal{C}) = k+1$

$|\mathcal{C}|$ has min. dist. $\geq n-k$
(Deg k polys can have at most k points of agreement)

If we view Σ as changing with n,
this gives us codes with rate $\frac{k}{n}$, rel. min. dist. $1-\frac{k}{n}$

Rate $R = k/n$, Rel. min dist $\delta = 1-\frac{k}{n} = 1-R$

Codes with $R+\delta = 1$
(optimal R vs δ tradeoff) $\boxed{\text{Singleton Bound}}$

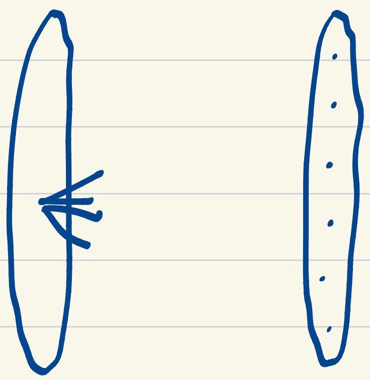
Lec-3

29/04

Expander Codes [Sipser - Spielman 95]

Given $\{0,1\}$-alphabet codes with $R = \Omega(1)$, $\delta = \Omega(1)$

L n R m



degree c degree c'

G is a (δ, γ) expander if $\in (0,1)$
$\forall\ S \subseteq L$, $|S| \leq \delta n$,
$|\Gamma(S)| \geq c(1-\gamma)|S|$.

$$c \cdot n = c' m$$

Fact: $\forall$ constants c, c' $\exists$ (δ, γ)-expanders of size $\left(n, \frac{c}{c'} n\right)$ for $\delta < \frac{1}{\gamma^2} \frac{1}{c'}$.

Code coming from G.

$$\mathcal{C} = \{ f : L \to \{0,1\} \text{ s.t } \forall\, v \in R \ \bigoplus_{u \sim v} f(u) = 0 \}$$

$\mathcal{C}$ is a linear code over $\mathbb{F}_2$.

$$\dim(\mathcal{C}) \geq n - m = n\left(1 - \frac{c}{c'}\right)$$

$$\text{Rate} : \frac{\dim(\mathcal{C})}{n} = 1 - \frac{c}{c'} = \Omega(1)$$

Distance:

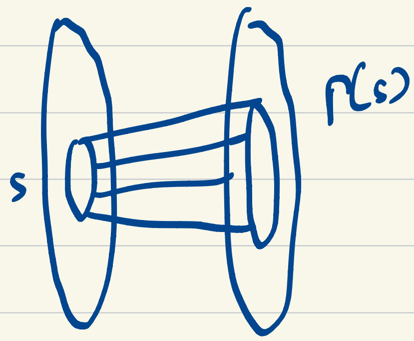
Claim: Any non-zero $f \in \mathcal{C}$ has $\geq \delta n$ 1s.

Then $\mathcal{C}$ has rel. dist δ.

Suppose $f: L \to \mathbb{F}_2$ is non-zero on S. $(|S| \leq \delta n)$

We want to show that $\exists\, v \in R$ s.t v has an odd # nbrs in S.

Claim: If $\gamma < \frac{1}{2}$, $\exists\, v \in R$ s.t v has 1 nbr in S.



If every vertex in $\Gamma(S)$ has ≥ 2 nbrs in S

Then, $c|S| \geq 2|\Gamma(S)|$

$\Rightarrow |\Gamma(S)| \leq \frac{c}{2}|S|$ violates expansion property.

unique nbrs in S. $\geq (1-2\gamma) \cdot c \cdot |S|$

$\Rightarrow$ $\mathcal{C}$ has min. dist. $\geq \delta n$.

Explicit Construction of such extreme expanders

[CRVW]

[Golowich][CTR] HDX-based construction

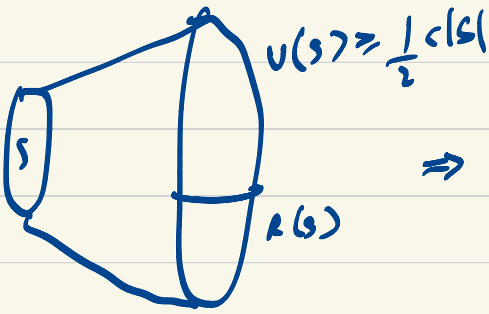
Decoding:

Each constraint is either happy or not.

We look for a vertex $u \in L$ s.t it has more unhappy nbrs than happy nbrs, flip it.

Thm: If our given received word has dist $< \frac{\delta n}{2}$ from ℓ and $\gamma < \frac{1}{4}$, then this algorithm finds the nearby codeword.

We know that there are at least $(1-2\gamma)c|S|$ unique nbrs of S.



$\Rightarrow \exists\, u \in S$ which has at least has $\frac{1}{2}c$ unique nbrs.

unhappy constraints starts at $\leq c \cdot \Delta(\text{received}, \text{true})$ and strictly reduces.

Need this property:

$\Delta(\text{current}, \text{true})$ always is $\leq \delta n$, in order to always have a vertex to flip.

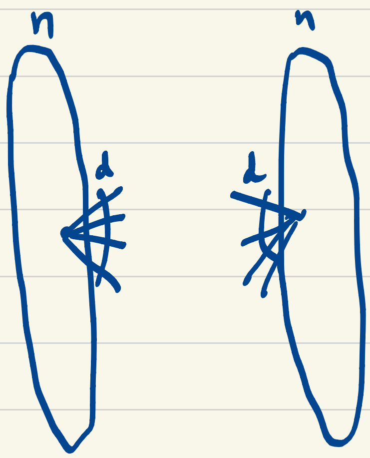
So, at every stage of algo, # unhappy constraints $\leq c \cdot \frac{\delta n}{2}$

Consider S at the step where $|S| = \delta n$

Then, # unhappy constraints $\geq c(1-2\gamma)\delta n > \frac{c\delta n}{2}$

Tanner Codes [80s]

[Linear-time decoder by Sipser Spielman 95]



d-regular

λ-absolute eigenvalue expander

$\lambda_1 = d$, $\in [\lambda, -\lambda]$, $\lambda_{2n} = -d$

We can get such graphs with $\lambda = O(\sqrt{d})$

Have a linear code $C_0 \subseteq \mathbb{F}_2^d$ with rel. dist. δ_0 and $\dim(C_0) = d(1-\alpha_0)$

Define $C \subseteq \mathbb{F}_2^{nd}$

$$C = \{ f : E \to \mathbb{F}_2 \text{ s.t } f|_{\substack{\text{edges}\\ \text{out of}\\ v}} \in C_0 \ \forall v \in V \}$$

$$\dim(C) \geq nd - 2n(\alpha_0 d) = nd(1 - 2\alpha_0)$$

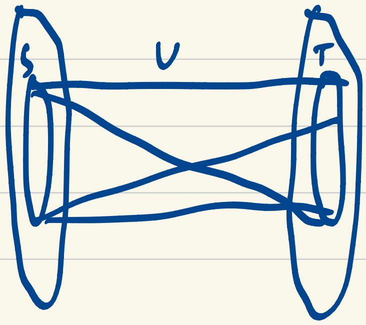
Choose $\alpha_0 < \frac{1}{2}$, the C has rate $\Omega(1)$

Lemma: C has min. dist. $\geq \delta_0\left(\delta_0 - \frac{\lambda}{d}\right)nd \approx \delta_0^2 nd$ for d big enough $\lambda = O(\sqrt{d})$

Proof: Let f be a non-zero codeword

Let $U \subseteq E$ be the support of f.

Want to show $|U| \geq$ big



$S \subseteq L$ $\quad$ $U \subseteq$ edges between S and T
$T \subseteq R$

U has at least $\delta_0 d$ edges incident on each vertex of S (and also T).

$\delta_0 d|S| \leq |U| \leq e(S,T) \leq \frac{|S|.|T|.d}{n} + d\sqrt{|S|.|T|}$
$\delta_0 d\sqrt{|S||T|}$

$m = \sqrt{|S||T|}$

$\delta_0 d m \leq \frac{m^2 d}{n} + dm$

$m \geq \frac{\delta_0 d - \lambda}{d/n} = n \cdot \left(\delta_0 - \frac{\lambda}{d}\right)$

$U \geq \delta_0 d\, m \geq \delta_0 \left(\delta_0 - \frac{\lambda}{d}\right) nd$

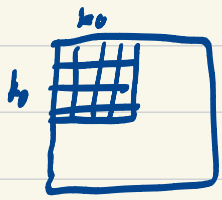
Tensor Codes

C_0 is a linear code $\subseteq \mathbb{F}_2^n$

Tensor code $C_0 \otimes C_0$

$$= \{ f : [n]^2 \to \mathbb{F}_2 \text{ s.t. } \forall i \in [n] \ f(i, \cdot) \in C_0, \ \forall j \in [n] \ f(\cdot, j) \in C_0 \}$$

$\dim(C_0 \otimes C_0) = \dim(C_0)^2$



$$\text{Rate}(C_0 \otimes C_0) = \frac{\dim(C_0 \otimes C_0)}{n^2} = (\text{Rate}(C_0))^2$$

$\text{dist}(C_0 \otimes C_0) \geq \text{dist}(C_0)^2$

Decoding algorithm for Tanner Codes

Keep doing the following

L - For each left vertex v, correct $f|_{\text{edges of } v}$ to a codeword in C_0 if it is within $\frac{\delta_0 d}{2}$ of C_0.

R - Same for right

Start with a received word with distance $\le (1-\epsilon)\frac{\delta_0}{4}(\delta_0 - \frac{\lambda}{d})dn$ from a codeword. [Zémor]

Claim: This algorithm finds the nearby codeword in $O(\log n)$ rounds.

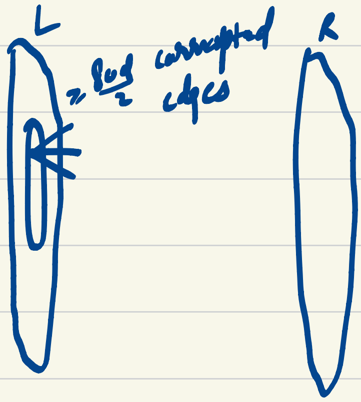
Obs: After step L, there are only happy and devastated vertices on the left.

Let S be the set of devastated vertices $\overset{\in L \text{ (before R)}}{}$ after step L.

$$|S| \le \frac{(1-\epsilon)\frac{\delta_0}{4}(\delta_0 - \frac{\lambda}{d})nd}{\frac{\delta_0 d}{2}}$$

$$\le \frac{(1-\epsilon)\left(\delta_0 - \frac{\lambda}{d}\right)n}{2}$$

Let T be the set of devastated vertices $\overset{\in R}{}$ after step L (and then also R)



Consider U, the set of edges incident on S which were not corrected by step L.

There are $\frac{\delta_0 d}{2}$ edges per vertex of S.

$$|U| \approx \frac{\delta_0 d}{2}|S|$$

$$|T|\frac{\delta_0 d}{2} \le e(S,T) \le \frac{|S|\cdot|T|\cdot d}{n} + \lambda\sqrt{|S|\cdot|T|}$$

$$\le \frac{|S|\cdot|T|\cdot d}{n} + \lambda\left(\frac{|S|+|T|}{2}\right)$$

$$\frac{|T|\delta_0 d}{2} \le \left(\frac{(1-\epsilon)\left(\delta_0 - \frac{\lambda}{d}\right)d}{2} + \frac{\lambda}{2}\right)|T| + \frac{\lambda|S|}{2}$$

$$d|T|\left(\frac{\delta_0}{2} - \frac{(1-\epsilon)\left(\delta_0 - \frac{\lambda}{d}\right)}{2} - \frac{\lambda}{2d}\right) \le \frac{\lambda}{2}|S|$$

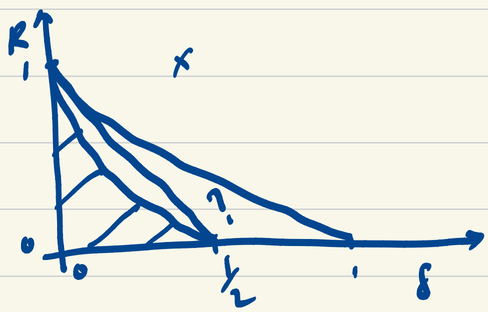
$$|T| \le \frac{\lambda/2d}{\frac{\delta_0}{2} - (1-\epsilon)\left(\frac{\delta_0}{2} - \frac{\lambda}{2d}\right) - \frac{\lambda}{2d}}|S| = \frac{\lambda/2d}{\epsilon\frac{\delta_0}{2} - \frac{\epsilon\lambda}{2d}}|S|$$

$$= \frac{\lambda/2d}{\frac{\epsilon}{2}\left(\delta_0 - \frac{\lambda}{d}\right)}|S|$$

Lec-7

$\{0,1\}$ - alphabet

R vs δ



Focus on $\delta = \frac{1}{2} - \epsilon$

Volume Packing
$R \leq 1 - H\left(\frac{\delta}{2}\right)$

Greedy/Random Existence
(Gilbert-Varshamov Bound)

Can have $R \geq 1 - H(\delta)$

Plotkin: for $\delta \geq \frac{1}{2}$, $R = 0$

For $\delta = \frac{1}{2} - \epsilon$

Take a random linear code of $\dim_{\wedge}^{k=} Rn \leq \mathbb{F}_2^n$

Set R so that the code has dist δ.

Pick $v_1, \ldots, v_k \in \mathbb{F}_2^n$ uniformly

Consider span $0, v_1, v_2, \ldots, v_1 + v_2 + v_3, \ldots$

$$\Pr\left[\exists S \neq \phi, S \subseteq [k] : \sum_{i \in S} v_i \in B(0, \delta)\right] \leq \frac{2^k \cdot |B(0,\delta)|}{2^n}$$

$$\frac{|B(0,\delta)|}{2^n} \leq e^{-\Omega(\epsilon^2 n)}$$

Can take $k = \Omega(\epsilon^2 n)$
$R \geq \Omega(\epsilon^2)$ is possible

LP bound [Joe] $R \le O\left(\epsilon^2 \log\left(\frac{1}{\epsilon}\right)\right)$

[Alon]

$\mathcal{C}$ of dist $\delta = \frac{1}{2} - \epsilon$

- assume $\mathcal{C}$ is ϵ-biased Call non-zero codewords have # 1s $\in \left[\left(\frac{1}{2}-\epsilon\right)n, \left(\frac{1}{2}+\epsilon\right)n\right]$

- assume $\mathcal{C}$ is linear

Let $G = \begin{bmatrix} \text{---} & v_1 & \text{---} \\ \text{---} & v_2 & \text{---} \\ & \vdots & \\ \text{---} & v_k & \text{---} \end{bmatrix}$ be s.t. $v_1, v_2, \dots, v_k$ is a basis for $\mathcal{C}$.

$= \begin{bmatrix} | & | & & | \\ u_1 & u_2 & \cdots & u_n \\ | & | & & | \end{bmatrix}$. Then $u_i \in \mathbb{F}_2^k$.

By ϵ-bias, $\forall x \in \mathbb{F}_2^k \setminus \{0\}$

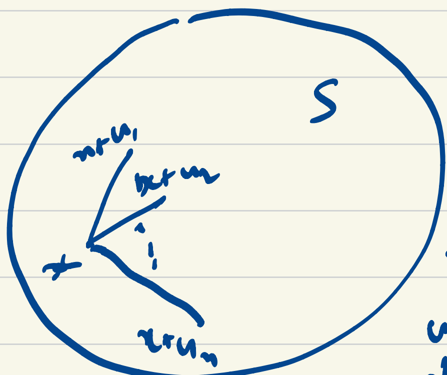
$$\Pr_{i \in [n]}\left[\langle x, u_i \rangle = 1\right] \in \left(\frac{1}{2}-\epsilon, \frac{1}{2}+\epsilon\right)$$

<u>Cayley Graph</u>

$Cay(\mathbb{F}_2^k, S)$ $S = \{u_1, \dots, u_n\}$

Vertex set = $\mathbb{F}_2^k$

Join x to $x+u_i$ for each i.



n-regular
undirected
2^k vertices

Take $f: \mathbb{F}_2^k \to \mathbb{C}$

Let A be the adj. matrix of G

$$(Af)_x = \sum_{i=1}^{n} f(x+u_i)$$

For $a \in \mathbb{F}_2^k$,

define $\varphi_a : \mathbb{F}_2^k \to \mathbb{R}$

by $\varphi_a(x) = (-1)^{\langle a, x \rangle}$

$$\begin{aligned}(A\varphi_a)(x) &= \sum_{i=1}^{n} \varphi_a(x+u_i) \\ &= \sum_{i=1}^{n} (-1)^{\langle x+u_i, a\rangle} \\ &= \sum_{i=1}^{n} (-1)^{\langle x, a\rangle} \cdot (-1)^{\langle u_i, a\rangle} \\ &= \varphi_a(x)\left(\sum_{i=1}^{n} (-1)^{\langle u_i, a\rangle}\right)\end{aligned}$$

Eigenvalues of φ_a is

$$\sum_i (-1)^{\langle a, u_i\rangle} \in (-\epsilon n, +\epsilon n)$$

Process:

Pick $X_0 \in \mathbb{F}_2^k$ uniformly at random.

Take a random walk on G.

$X_0, X_1, \ldots, X_{2t}$

$$\Pr[X_0 = X_{2t}] = \frac{1}{2^k} \operatorname{Tr}(\mathcal{J}^{2t})$$

$$\leq \frac{1}{2^k}\left(1 + (2^k - 1)\epsilon^{2t}\right)$$

$$\leq \frac{1}{2^k} + \epsilon^{2t}$$

$$\Pr[X_0 = X_{2t}] = \Pr[\text{the two walks } X_0, \ldots, X_t \text{ and } X_{t+1} \ldots X_{2t} \text{ satisfy } X_0 = X_{2t}]$$

$$= \Pr[\text{two independent walks starting at } X_0 \text{ end at the same vertex}]$$

$$\geq \mathop{\mathbb{E}}_{X_0}\left[\frac{1}{\#\text{ vertices reachable from } X_0 \text{ in } t \text{ steps}}\right]$$

$$\geq \frac{1}{|B_n(0,t)|} \approx \frac{1}{\binom{n}{t}}$$

$$\frac{1}{\binom{n}{t}} \leq \frac{1}{2^k} + \epsilon^{2t}$$

$$\Rightarrow \left(\frac{t}{en}\right)^t \leq \frac{1}{2^k} + \epsilon^{2t}$$

Set t s.t.

$$\frac{1}{2^k} = \epsilon^{2t} \qquad \left(t = \frac{k}{\log\left(\frac{1}{\epsilon}\right)}\right)$$

$$\Rightarrow \left(\frac{t}{en}\right)^t \leq 2\epsilon^{2t}$$

$$\Rightarrow \quad n \geq \Omega\left(t \cdot \frac{1}{\epsilon^2}\right) = \Omega\left(\frac{k}{\epsilon^2 \log(1/\epsilon)}\right)$$

Explicit Constructions of Codes at $\delta = 1/2 - \epsilon$

Optimal $R \approx \tilde{O}(\epsilon^2)$

Best known R for an explicit code till 2018 was $R = O(\epsilon^3)$

[Ta-Shma 18] Explicit code $R = \Omega(\epsilon^{2+o(1)})$

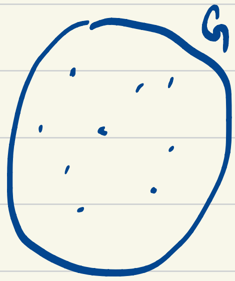
[Madhu et. al] Decodable in poly(n) now $n^{1+o(1)}$ time.

[Rozenman - Wigderson]

A transformation that takes an ϵ-biased code and makes it an $O(\epsilon^2)$-biased code.

Code $\mathcal{C}$ - ϵ-biased, linear

Impose a graph G on $[n]$



expander, d-regular
n vertices

$$\hat{\mathcal{C}} = \{(x_i + x_j)_{(i,j)\in E} : (x_1, x_2, \dots, x_n) \in \mathcal{C}\}$$

$$\subseteq \mathbb{F}_2^{nd}$$

If G is an expander, then $\hat{\mathcal{C}}$ is $(\epsilon^2 + \frac{\lambda}{d})$-biased.
(Exercise)

Start with a code C_0 of rate $r = 0.1$
loss $\epsilon_0 = 0.1$

Produce new codes
C_{i+1} from C_i with $\epsilon_{i+1} = (\epsilon_i)^2 + \frac{d_i}{d_i} = O(\epsilon_i^2)$

$$R_{i+1} = \frac{R_i}{d_i} = R_i \epsilon_i^4$$

Set $d_i = \left(\frac{1}{\epsilon_i}\right)^4$, $d_i = \left(\frac{1}{\epsilon_i}\right)^2$

Do this till $\epsilon_t = \epsilon$

$$R_t = R_1 \epsilon_1^4 \epsilon_2^4 \dots \epsilon_t^4$$
$$\approx O(\epsilon_t^4) = O(\epsilon^4)$$

Lecture on Gap Codes

05/05

Gap Codes

Reed-Muller Codes

$\mathbb{F}_q$ $\quad m = O(1)$

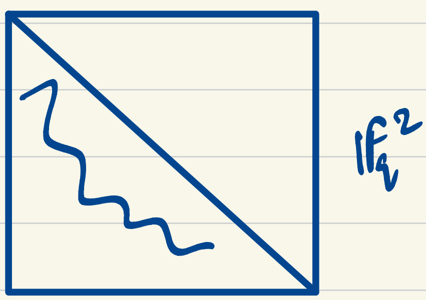
$\mathbb{F}_q^m$ Evaluate polynomials of degree $d = 0.9q$.

Rel. dist 0.1

$$\text{Rate } R = \frac{\dim(\text{space of polys of deg} \le d)}{q^m} = \frac{\binom{d+m}{m}}{q^m}$$

$$\approx \frac{1}{m!}(0.9)^m$$

Q: Find $S \subseteq \mathbb{F}_q^m$ so that R can approach 1 while still having rel. dist $= \Omega(1)$?



CAP Codes

$m=2$ $\quad R \le \frac{1}{2}$

Fact: polys preserve $\Omega(1)$ dist. even on this set

One can take d, m arbitrary

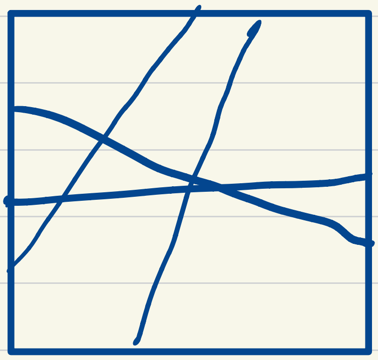
Open to find $S \subseteq \mathbb{F}_q^m$ with $|S| = O\left(\binom{d+m}{m}\right)$ s.t. rel. dist $= \Omega(1)$

Known: $|S| = \binom{d+m}{m}^{O(1)}$

m=2 GAP codes

$$S = \{ (a+b, ab) : \underset{a \neq b}{a, b} \in \mathbb{F}_q \}$$

Fact: Polys of deg $0.9q$ have vanish on $\leq 0.1^2$ fraction of S.



$\mathbb{F}_q^2$

Lines $L_1, L_2, \ldots, L_q$ in general position

$$S = \{ L_i \cap L_j : \{i,j\} \subseteq [q] \}$$

Gap codes in general

$\mathbb{F}_q^m$. $H_1, \ldots, H_t$ hyperplanes in general position.

$$S = \{ \bigcap_{j \in J} H_j : |J| = m, J \subseteq [t] \}$$

$$|S| = \binom{t}{m}$$

Claim: NZ Polys of degree d does not vanish on at least $\binom{t-d}{m}$ points of S.

$$R = \frac{\binom{d+m}{m}}{\binom{t}{m}}$$

If $d = \ell \cdot t$

$$R = \ell^m$$

$$\delta = (1-\ell)^m$$

$$\delta = \frac{\binom{t-d}{m}}{\binom{t}{m}}$$

$$R^{1/m} + \delta^{1/m} = 1$$

If S is an interpolating set for polys of deg $t-m$, then any non-zero polynomial of deg d does is non-zero at $\geq \binom{t-d}{m}$ pts of S.

codim m	$H_{i_1} \cap H_{i_2} \ldots \cap H_{i_m}$
$\vdots$	$\vdots$
codim 2	$H_i \cap H_j$
codim 1	$H_1, \ldots, H_t$

Local Characterization

For GAP Codes,

$f : S \to \mathbb{F}_q$ is a codeword (eval table of a deg. d poly) iff $\forall L \in (m-1)$-wise intersections of H_i

$f|_L$ is consistent with a univariate poly of deg d.

some $\delta > 0$

<u>Thm:</u> GAP codes can achieve any $R < 1$, and local testability with n^{ϵ} queries for any $\epsilon > 0$.
(n - blocklength)