Affine Invariant LCCs and LTCs

Sivakanth Gopi

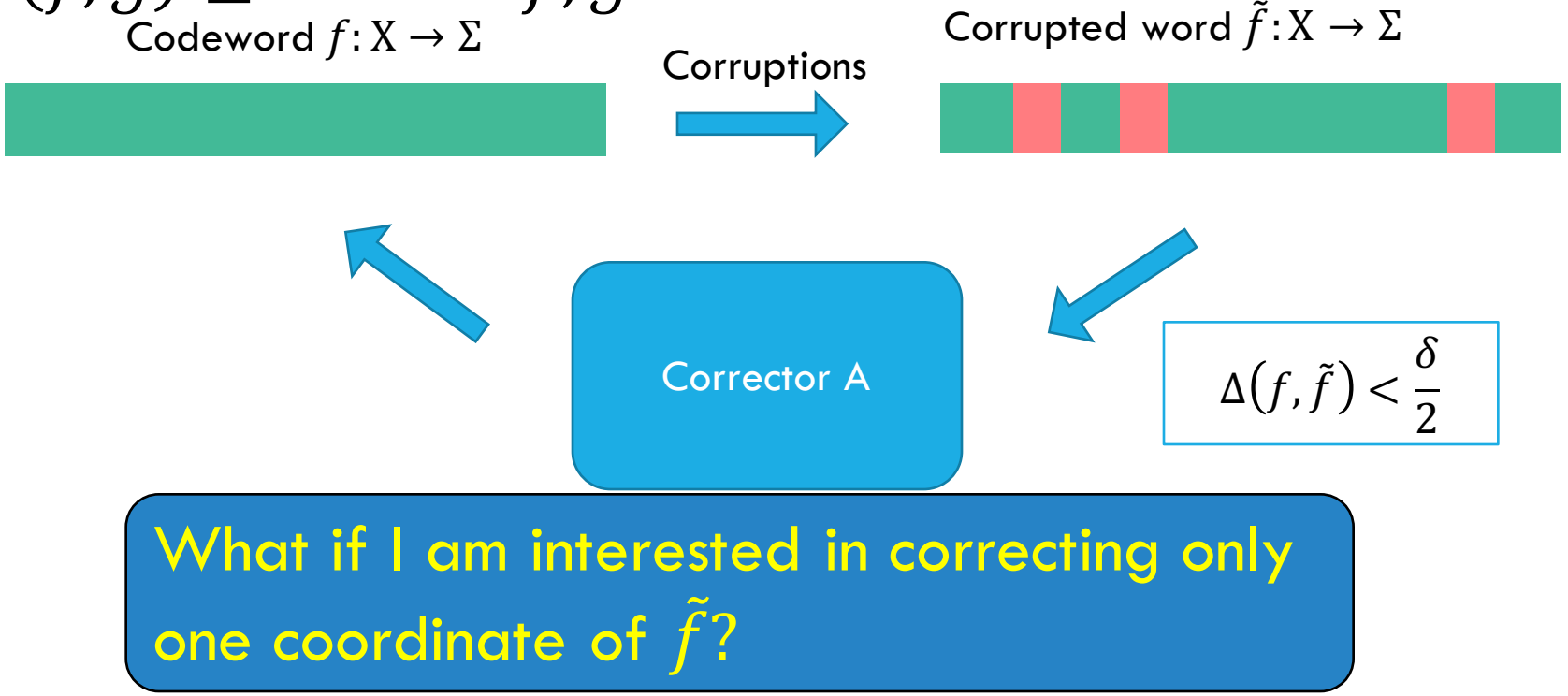
PRINCETON UNIVERSITY

Joint work with Arnab Bhattacharya

(Indian Institute of Science)

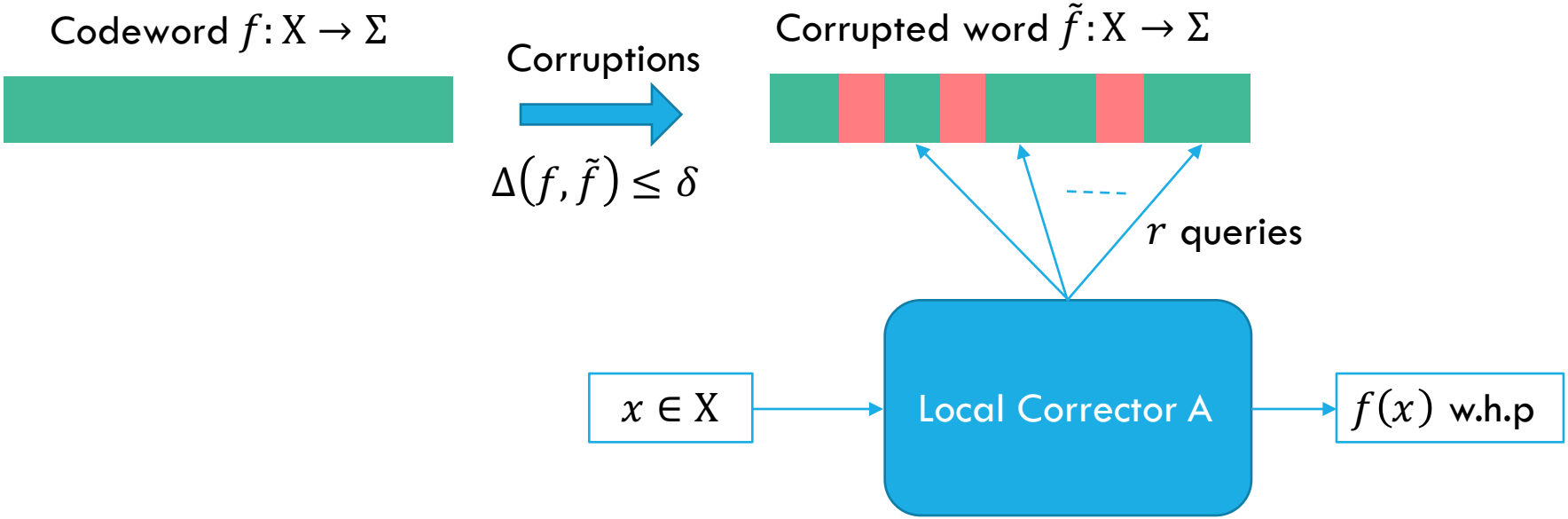
Error Correcting Code

- Σ : finite alphabet, X : set of coordinates of size N
- Σ^{X} : set of all functions from $\mathrm{X} \to \Sigma$
- Hamming distance, $\Delta(f,g) = \Pr_{x \in \mathrm{X}}[f(x) \neq g(x)]$
- $C \subset \Sigma^{\mathrm{X}}$: Error correcting code with minimum distance δ if $\Delta(f,g) \geq \delta$ for all $f, g \in C$



Locally Correctable Code (LCC)

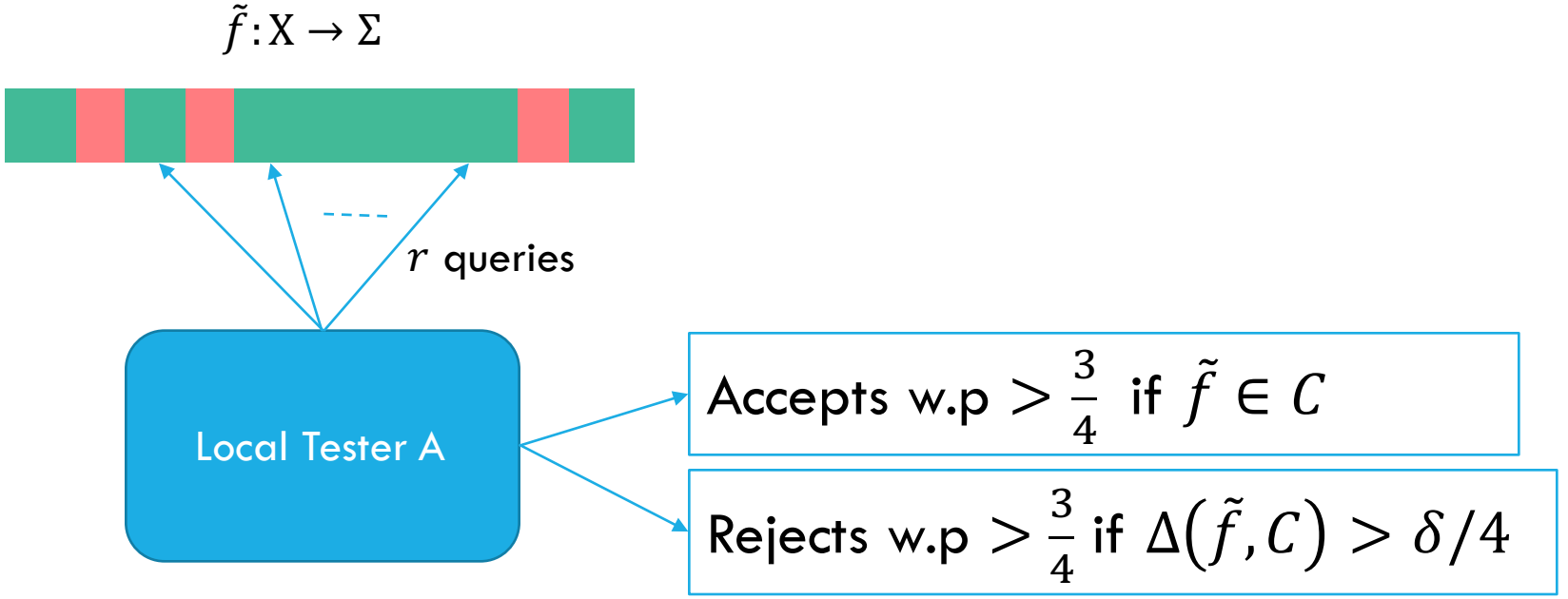
- Can correct any coordinate of a corrupted codeword by querying only r locations



How do we know if $\Delta(\tilde{f}, C) \leq \delta$, locally?

Locally Testable Code (LTC)

- Can test closeness to the code by querying only r locations



What's known?

- In this talk, constant query: $r = O(1)$, constant alphabet: $|\Sigma| = O(1)$,
- Let $|X| = N$, the length of messages we can encode is $\log |C|$

Bounds on $\log \lvert C \rvert$	Lower Bound	Upper Bound
2-query LCC	$\log N$ [Hadamard Code]	$O(\log N)$ [KdW04]
r-query LCC ($r \geq 3$)	$(\log N)^{r-1}$ [Reed Muller Codes]	$N^{1-1/\lceil r/2 \rceil}$ [KT00,KdW04,Woo07]
r-query LTC ($r \geq 2$)	$N/polylog(N)$ [BS05,Din07]	$O(N)$ [Trivial]

Local codes from invariance

- LCCs and LTCs need to satisfy many local constraints

$$\forall f \in C, \Gamma\big(f(x_1), \cdots, f(x_r)\big) = 1$$

- Let G be a group acting on X and so G also acts on functions $f: \mathrm{X} \to \Sigma$ as $\gamma(f)(x) = f \circ \gamma(x)$
- Let code $C \subset \Sigma^{\mathrm{X}}$ be invariant under this action i.e.

$$\forall f \in C, \gamma \in G: f \circ \gamma \in C$$

- Local constraint on $(x_1, \cdots, x_r) \Rightarrow$ Local constraint on $\big(\gamma(x_1), \cdots, \gamma(x_r)\big)$ for all $\gamma \in G$

$$\forall f \in C, \gamma \in G \;\; \Gamma\big(f(\gamma(x_1)), \cdots, f(\gamma(x_r))\big) = 1$$

Affine invariant codes

- Kaufman and Sudan in '07
- $\mathbb{F}$:any finite field. Let $\mathrm{X} = \mathbb{F}^n$ and let $G = \mathrm{Aff}(\mathrm{n}, \mathbb{F})$ be the group of invertible affine maps from $\mathbb{F}^n \to \mathbb{F}^n$
- A code $C \subset \Sigma^{\mathbb{F}^n}$ which is invariant under the action of $\mathrm{Aff}(n, \mathbb{F})$ is called *affine invariant* i.e.

$$\forall f \in C, \forall \ell \in \mathrm{Aff}(n, \mathbb{F}), f \circ \ell \in C$$

- Example
  - Reed-Muller code of degree d: set of polynomial functions of degree $\leq d$ from $\mathbb{F}^n \to \mathbb{F}$
  - If $f(x)$ is a degree $\leq d$ polynomial and $\ell(x) = Ax + b$, then $f(\ell(x))$ is also a degree $\leq d$ polynomial
  - Irreducible polynomials, products of two degree d polynomials...

Can we construct good LCCs or LTCs using affine invariance?

Main Results

Locally Correctable Codes

If $C \subset \Sigma^{\mathbb{F}^n}$ is an r-query affine invariant LCC then $\log |C| \leq O_{r,|\mathbb{F}|,|\Sigma|}(n^{r-1})$

(Note that $n = \log_{|\mathbb{F}|} N$, where N is length of the code)

- Achieved by Reed-Muller codes of degree $r-1$

Locally Testable Codes

If $C \subset \Sigma^{\mathbb{F}^n}$ is an r-query affine invariant LTC then $\log |C| \leq O_{r,|\mathbb{F}|,|\Sigma|}(n^{r-2})$

- Achieved by Lifted Codes of [GKS'13]
- [Ben-Sasson, Sudan '11] proved the same bounds when Σ is a subfield of $\mathbb{F}$ and C is a linear code over Σ

Higher Order Fourier Analysis

Gowers uniformity norms

- Define multiplicative derivative of $f: \mathbb{F}_p^n \to \mathbb{C}$ as

$$\Delta_h f(x) = f(x+h)\overline{f(x)}$$

- Gowers uniformity norm of order $d+1$ of $f: \mathbb{F}_p^n \to \mathbb{C}$

$$||f||_{U^{d+1}} = \mathbb{E}_{x,h_1,\cdots,h_{d+1}\in\mathbb{F}^n}\left[\Delta_{h_1}\cdots\Delta_{h_{d+1}} f(x)\right]^{1/2^k}$$

- If $f(x) = \omega^{g(x)}$ where ω: p^{th} root of unity and $g: \mathbb{F}_p^n \to \mathbb{F}_p$ is a degree d polynomial then

$$||f||_{U^{d+1}} = \mathbb{E}_{x,h_1,\cdots,h_{d+1}\in\mathbb{F}^n}\left[\omega^{D_{h_1}\cdots D_{h_{d+1}} g(x)}\right]^{1/2^k} = 1$$

- **Inverse Gowers theorem** [Tao, Ziegler '11]: $(p > d)$
  If $||f||_{U^{d+1}} = \Omega(1)$ then f is correlated with the phase of a degree d polynomial
- For $p \leq d$, we get non-classical polynomials

Von Neumann inequality

- If $||f||_{U^r} \ll 1$, then cannot find f at $\ell(x_0)$ from the values of g at $\ell(x_1), \cdots \ell(x_r)$ for a random $\ell \in_R \mathrm{Aff}(\mathbb{F}_p, n)$

$$\left|\mathbb{E}_\ell \left[f \circ \ell(x_0) \Gamma\left(g \circ \ell(x_1), \cdots, g \circ \ell(x_r)\right)\right]\right| \leq 2^r ||f||_{U^r}$$

- Proof: expand Γ in Fourier basis, make linear change of variables to get expressions like

g_i' doesn't depend on z_i

$$\mathbb{E}_{z_1,\cdots,z_r}[f(\sum z_i) g_1'(-z_1 + \sum z_i) \cdots g_r'(-z_r + \sum z_i)]$$

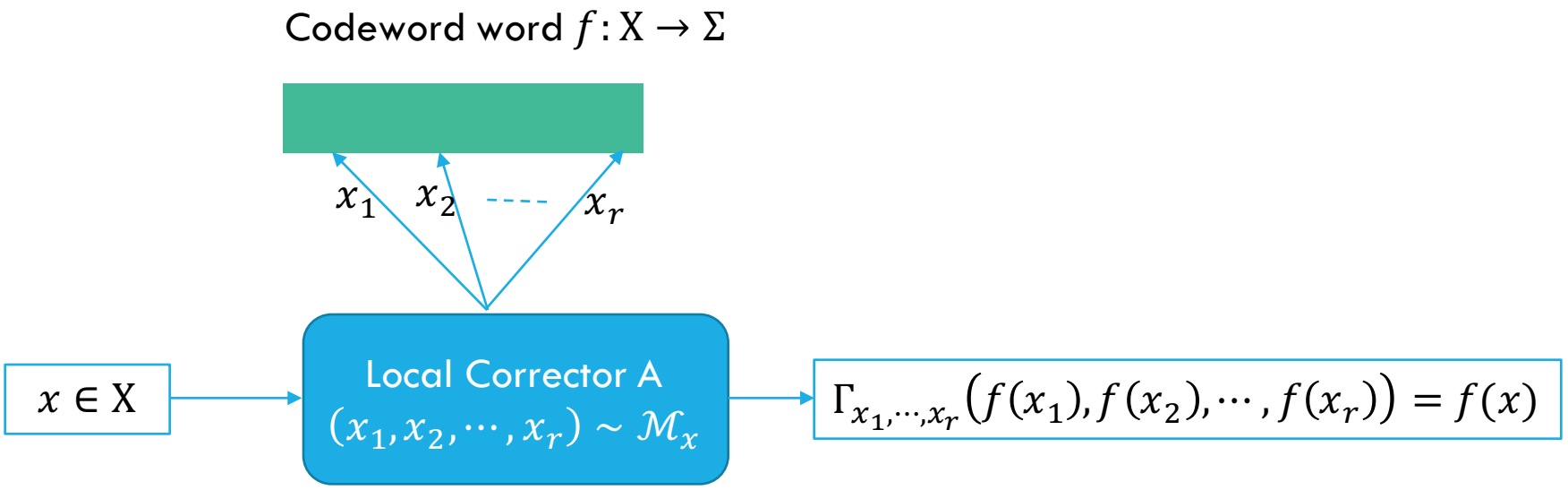
- and repeatedly apply Cauchy-Schwarz inequality

$$\left|\mathbb{E}_{z_1,\cdots,z_r}[f(\sum z_i) g_1'(-z_1 + \sum z_i) \cdots g_r'(-z_r + \sum z_i)]\right| \leq ||f||_{U^r}$$

Proof sketch for LCCs

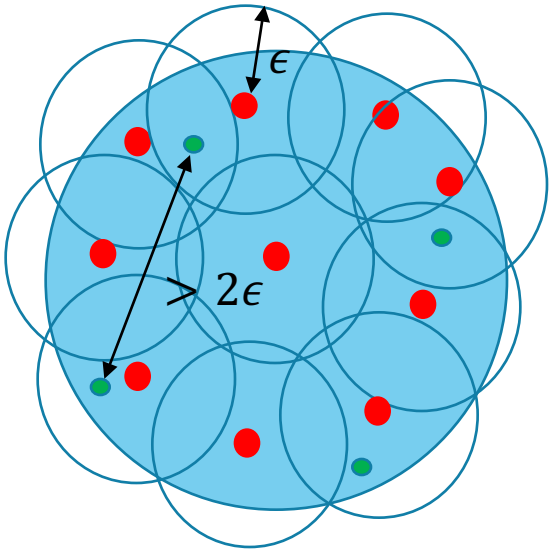
Some simplifications

- Assume $\Sigma = \{-1,1\}, \mathbb{F} = \mathbb{F}_p$ for some prime $p > r$
- Assume perfect recovery for codewords



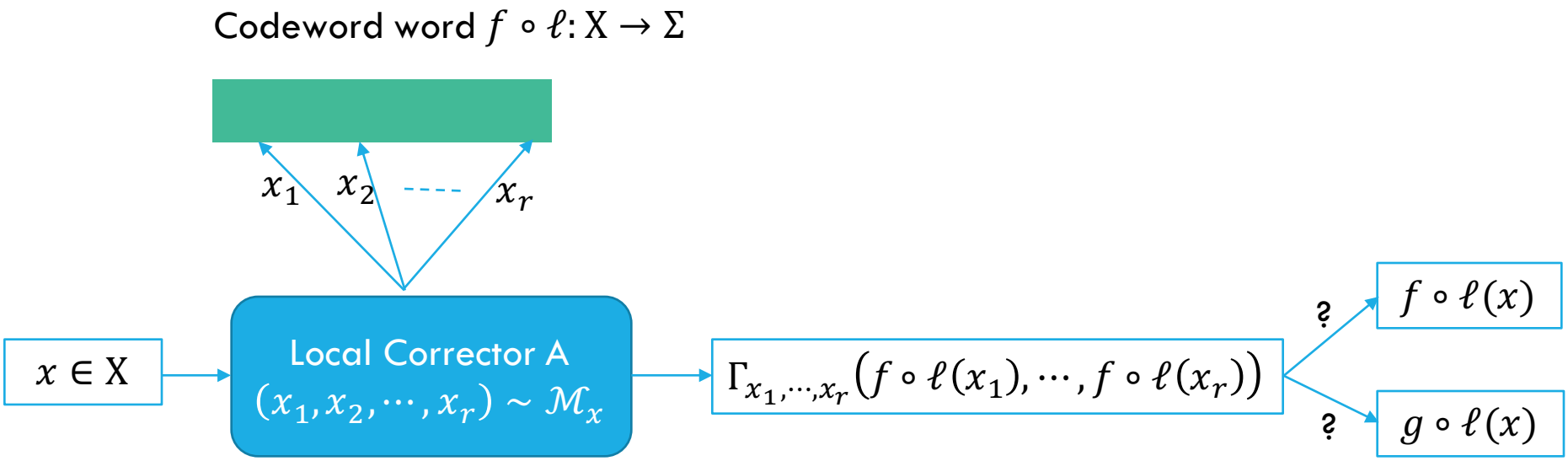
Proof Sketch

- **Step 1**: Show that any two distinct codewords $f, g \in C$ must be 2ϵ-far in U_r-norm i.e. $||f - g||_{U^r} > 2\epsilon$ (von Neumann inequality)
- **Step 2**: Construct a small ϵ-net $\mathcal{N}$ for the set of all functions in U_r-norm (Inverse Gowers theorem)
- $\mathcal{N} = \{\text{red points}\}, C = \{\text{green points}\}$, two green dots cannot fall in the same ball!
- $|C| \leq |\mathcal{N}|$



Proof of Step 1

- Intuitively, if $||f - g||_{U^r} < 2\epsilon$ then the local corrector cannot distinguish between $f \circ \ell, g \circ \ell$ for a random $\ell \in \mathrm{Aff}(n, \mathbb{F}_p)$
- But $f \circ \ell, g \circ \ell$ are valid codewords by invariance and the corrector should distinguish them – Contradiction!



Proof of Step 1

- $\Pr_x[\mathrm{A}^{f\circ\ell} \text{ outputs } f\circ\ell(x)] - \Pr_x[\mathrm{A}^{f\circ\ell} \text{outputs } g\circ\ell(x)]$
- $= 1 - \Pr_x[f\circ\ell(x) = g\circ\ell(x)]$
- $= \Delta(f,g) \geq dist(C)$

- $\frac{1}{2}\mathbb{E}_\ell\left[\Pr_x[\mathrm{A}^{f\circ\ell} \text{ outputs } f\circ\ell(x)] - \Pr_x[\mathrm{A}^{f\circ\ell} \text{outputs } g\circ\ell(x)]\right]$
- $\mathbb{E}_\ell\left[\mathbb{E}_x\mathbb{E}_{x_1,\cdots,x_r\sim\mathcal{M}_x}\left[\left(f\circ\ell(x) - g\circ\ell(x)\right)\Gamma_{x_1,\cdots,x_r}\left(f\circ\ell(x_1),\cdots,f\circ\ell(x_r)\right)\right]\right]$
- $\mathbb{E}_x\mathbb{E}_{x_1,\cdots,x_r\sim\mathcal{M}_x}\left[\mathbb{E}_\ell\left[\left(f\circ\ell(x) - g\circ\ell(x)\right)\Gamma_{x_1,\cdots,x_r}\left(f\circ\ell(x_1),\cdots,f\circ\ell(x_r)\right)\right]\right]$

$\leq 2^r\left||f-g|\right|_{U^r}$ (von Neumann inequality)

- Therefore $\left||f-g|\right|_{U^r} \geq 2\frac{dist(C)}{2^r} = 2\epsilon$

Proof of Step 2 (small ϵ-net)

- **Decomposition theorem** (Green, Tao, Ziegler'11) $\forall \epsilon, r\ \exists k(\epsilon, r)$ such that: any $h: \mathbb{F}_p^n \to [-1,1]$ can be ϵ-approximated by a function of k degree $r-1$ polynomials in U^r- norm

$$||h - \Gamma(p_1, \cdots, p_k)||_{U^r} < \epsilon$$

- A degree $r-1$ polynomial has n^{r-1} coefficients
- Gives an epsilon-net of size $|\mathcal{N}| = \exp\left(O_{p,r}(n^{r-1})\right)$
- Thus $|C| \leq |\mathcal{N}| = \exp\left(O_{p,r}(n^{r-1})\right)$

QED!

Open Questions

- We show "tight" bounds on the size of affine invariant constant query LCCs and LTCs
- Improve the dependence on $r, |\mathbb{F}|, |\Sigma|$
- Can we prove similar bounds for a more general class of codes? Codes invariant under some group action and some additional properties?
- Can we use sparse hypergraph regularity lemmas to understand the hypergraph structure of local codes?

ARIGATO GOZAIMASU!