FROM IRREDUCIBLE REPRESENTATIONS TO LOCALLY DECODABLE CODES

KLIM EFREMENKO

Presented by: Marek Eliáš

Theorem (T1.1, informal)**.** *Let G be a finite group and let (ρ, V) be an irreducible representation of G with $g_1, \dots, g_q$ in G and $c_1, \dots, c_q \in \mathbb{F}$ such that* $\mathrm{rank}(\sum c_i \rho(g_i)) = 1$*. Then there exists a $(q, \delta, q\delta)$-locally decodable code $\mathcal{C}\colon V \to \mathbb{F}^G$.*

Definition (Group action)**.** A group G acts on a set X if there exists a mapping $T\colon G \times X \to X$ such that $T(g_2, T(g_1, x)) = T(g_2 g_1, x)$ and $T(1, x) = x$.

Definition (Permutation action)**.** Suppose G acts on the set X. A permutation action of G on Σ^X is defined by $(gf)(x) = f(g^{-1}x)$.

Definition (Representation of a Group)**.** A representation (ρ, V) of a group G in a vector space V is a group homomorphism $\rho\colon G \to GL(V)$, where $GL(V)$ denotes the group of invertible matrices on the vector space V.

Definition. Let V be a vector space over the field $\mathbb{F}$. A representation of a group G in V is an action of the group G on the set V which satisfies the following conditions:

- $v_1, v_2 \in V : g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2$
- $\lambda \in \mathbb{F} : g \cdot (\lambda v) = \lambda g \cdot v$
- $v \in V : 1 \cdot v = v$

Definition (Sub-Representation)**.** Let ρ be a representation of a group G in a vector space V. We say that $U \subset V$ is a sub-representation of ρ if U is a linear subspace of V and U is invariant under ρ, namely: for every $g \in G$ it holds that $\rho(g)U = U$.

Definition (Irreducible-Representation)**.** Let ρ be a representation of a group G in a vector space V. We say that ρ is an irreducible representation if it does not have any non trivial subrepresentations.

Lemma (L2.3)**.** *Let (ρ, V) be an irreducible representation of G. Let $v \in V$ be a non-zero vector. Then the set $\{\rho(g)v \mid v \in G\}$ spans V, and thus there exist $g_1, \dots, g_k \in G$ such that $\{\rho(g_i)v\}_{i=1}^k$ is a basis for V.*

Definition (Homomorphisms between Representations)**.** Let ρ_1 be a representation of the group G in a vector space V and ρ_2 be a representation of the group G in a vector space W. We say that a linear mapping $T\colon V \to W$ is a homomorphism from (ρ_1, V) to (ρ_2, W) iff $\forall g \in G : \rho_2(g) \circ T = T \circ \rho_1(g)$.

Definition (Support)**.** $supp(f) = \{x \in X \mid f(x) \neq 0\}$

Lemma (L2.5)**.** *Let U be a vector subspace of $\mathbb{F}^X$ of the full support and let $|\mathbb{F}| \geq t$. Then there exist a vector $u \in U$ such that $|\mathrm{supp}(u)| \geq (1 - \frac{1}{t})|X|$.*

Definition (Group Algebra)**.** The group algebra $\mathbb{F}[G]$ is the set of all functions from G to $\mathbb{F}$. Addition in this group algebra is given by $(f + g)(x) = f(x) + g(x)$ and multiplication is given by

$$(f * h)(x) = \sum_{g_1 \cdot g_2 = x} f(g_1) h(g_2)$$

We write $f \in \mathbb{F}[G]$ as a formal sum: $f = \sum_{i=1}^n f(g_i) g_i$ where the second appearance of g_i means an indicator function: $g_i(x) = 1$ if $x = g_i$ and $g_i(x) = 0$ else. We say that $f \in \mathbb{F}[G]$ is a q-sparse element if it has support of size at most q i.e., $f = \sum_{i=1}^q f(g_i) g_i$.

Let $\rho\colon G \to GL(V)$ be any representation of the group G. Then we can linearly extend ρ to the group algebra $\mathbb{F}[G]$ i.e., $\rho\colon \mathbb{F}[G] \to \mathrm{Mat}(V)$ ($\mathrm{Mat}(V)$ means all matrices on V) where $\rho(f)$ is defined as $\sum_{g\in G} f(g)\rho(g)$. Note that now $\rho(f)$ may be any matrix, not necessary invertible.

Definition (Dual Space)**.** Let V be a linear vector space over field $\mathbb{F}$. Then the dual space of V, denoted V^* is the set of all linear functionals from V to $\mathbb{F}$.

Definition (Dual Basis)**.** Let V be a vector space of dimension k. Let $u_1, \ldots, u_k$ be a basis of V and $v_1, \ldots, v_k$ be a basis of V^*. We say that these bases are dual if $v_i(u_j) = \delta_{ij}$, where δ_{ij} is Kronecker delta i.e., $\delta_{ij} = 1$ if $i = j$ and zero otherwise.

Proposition (T2.9)**.** *The representation (ρ, V) is irreducible if and only if $(\bar{\rho}, V^*)$ is irreducible.*

Definition (Locally Decodable Codes)**.** A code $\mathcal{C}\colon \mathbb{F}^k \to \mathbb{F}^n$ is said to be (q, δ, ε)-locally decodable if there exists a randomized decoding algorithm D^w with an oracle access to the received word w such that the following holds:

(1) For every message $m = (m_1, \ldots, m_k) \in \mathbb{F}^k$ and for every $w \in \mathbb{F}^n$ such that $\Delta(\mathcal{C}(m), w) \leq \delta n$, for every i it holds that $\Pr(D^w(i) = m_i) \geq 1-\varepsilon$, where probability is taken over internal randomness of D. This means that the decoding algorithm can recover the relevant symbol even if up to δ fraction of the codeword symbols are corrupted.
(2) The algorithm $D^w(i)$ makes at most q queries to w.

Definition. A code $\mathcal{C}\colon \mathbb{F}^k \to \mathbb{F}^n$ is said to have a c-smooth decoder if $D^{\mathcal{C}(m)}(i) = m_i$ for every $m \in \mathbb{F}^k$ and for every i. Each query of $D(i)$ is uniformly distributed over a domain of size cn.

Proposition (Fact 2.10)**.** *Any code with a c-smooth decoder which makes q queries is also $(q, \delta, \frac{q\delta}{c})$ locally decodable.*

Theorem (T3.1)**.** *Let G be a group acting on a set X. Let $(\tau, \mathbb{F}^X)$ be the permutational representation defined by this action. Let (ρ, V) be a representation of G. Let $\mathcal{C}\colon V \to \mathbb{F}^X$ be a G-homomorphism between representations (ρ, V) and $(\tau, \mathbb{F}^X)$. Assume that the following conditions hold:*

(1) *(a) There exists a q-sparse element $D \in \mathbb{F}[G]$, $D = \sum_{i=1}^{q} c_i g_i$ sucg that* $\mathrm{rank}(\rho(D)) = 1$.
(b) (ρ, V) is an irreducible representation.
(2) *Let $v \in Im(\rho(D))$ be a non-zero vector. Then* $\mathrm{supp}(\mathcal{C}(v)) \geq c|X|$.

Let $k = \dim V$. Then there exists a basis $b_1, \ldots, b_k$ for V such that

$$(m_1, \ldots, m_k) \mapsto \mathcal{C}\left(\sum_{i=1}^{k}(m_i b_i)\right)$$

is a $(q, \delta, \frac{q\delta}{c})$-Locally Decodable Code.

Lemma (L3.2)**.** *There exists a basis $\{b_1, \ldots, b_k\}$ for V and $h_1, \ldots, h_k \in G$ such that $b_i \in \ker(\rho(D * h_j))$ if and only if $i \neq j$.*

Lemma (L3.3)**.** *Let V be a vector space over a field $\mathbb{F}$. Then for every irreducible representation (ρ, V) and for every $v \in V, v \neq 0$ there exist a homomorphism $\mathcal{C}\colon V \to \mathbb{F}[G]$ of representations (ρ, V) and the regular representation in $\mathbb{F}[G]$ such that* $\mathrm{supp}(\mathcal{C}(v)) \geq |G|(1 - \frac{1}{|\mathbb{F}|})$.