From Irreducible Representations to Locally Decodable Codes

Klim Efremenko

Tel-Aviv University

August 13, 2012

Error Correcting Codes

Motivation

- Encoding $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^n$, $n \geq k$.
- Even if $\mathcal{C}(x)$ is adversary corrupted in δn positions we still can recover x.
- We can achieve $n = O(k)$ and linear time encoding and decoding.

If we want only one bit x_i we still need to decode the hole message

Error Correcting Codes

Motivation

- Encoding $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^n$, $n \geq k$.
- Even if $\mathcal{C}(x)$ is adversary corrupted in δn positions we still can recover x.
- We can achieve $n = O(k)$ and linear time encoding and decoding.

If we want only one bit x_i we still need to decode the hole message

Definition of LDC

Definition: Locally Decodable Codes

$C(x_1, x_2, \dots, x_k) = (w_1, w_2, \dots, w_n)$
is LDC if every x_i can be recovered from q entries of $C(\vec{x})$,
even if $C(x)$ is corrupted (in up-to δn coordinates)
with high probability (w.p $1 - \varepsilon$).
There exists a probabilistic decoding algorithm d_i s.t.
$d_i(w_1, w_2, \dots, w_n) = x_i$
d_i reads only q symbols of $\vec{w}$

Applicationsof LDCs

Applications of LDCs

- Probabilistically checkable proofs.
- Worst case – average case reductions
- Pseudo-random generators
- Hardness amplification
- Private information retrieval schemes
- Banach Spaces

Constructions of LDC

Constructions of LDC

- Reed-Muller Codes: Codes based on evaluation of multivariate polynomials.
- Matching Vectors Codes: Codes based on matching vector families.

This Work

We present a framework for the construction of LDCs from the representation theory which captures both of the above constructions.

Constructions of LDC

Constructions of LDC

- Reed-Muller Codes: Codes based on evaluation of multivariate polynomials.
- Matching Vectors Codes: Codes based on matching vector families.

This Work

We present a framework for the construction of LDCs from the representation theory which captures both of the above constructions.

Upper and Lower Bounds(LDC)

# queries	Lower Bounds	Upper Bounds
1	Do not exist	
2	2^k	2^k
> 2	$k^{1+\varepsilon(q)}$	$\approx \exp(\exp O(\sqrt[\log q]{\log k}))$ MVC
polylog(k)	-	Poly(k), RM
k^ε	-	$1+\delta(\varepsilon)k$, RM

[KT00, KdW03, Woo07,Yek08, E09, IS08, MFL+10, KSY11 ...]

Definition: Representations

Definition (Representation of a Group)

Let G be a group. A representation (ρ, V) of G is a group homomorphism $\rho : G \to GL(V)$,
$\rho(g_1 \cdot g_2) = \rho(g_1) \cdot \rho(g_2), \forall g_1, g_2 \in G$.

Definition (Sub-Representation)

Let $\rho : G \to GL(V)$ be a representation of G. Subspace $W \subset V$ is a sub-representation if $\rho(g)W = W$ for every $g \in G$.

Definition (Irreducible-Representation)

A representation (ρ, V) is irreducible if it does not have non-trivial sub-representations.

Examples of Representations

Example

1. Trivial representation: $\rho(g) = 1$ for every g
2. Permutational representation: G acts on X then $(\mathbb{F}^X, \rho)$ where $\tau(g)$ permutes coordinates. $\tau(g)v[x] = v[g^{-1}x]$. Let $v = (1, 1, \ldots, 1) \in \mathbb{F}^X$. Then v spans one dim. sub-reps of $\mathbb{F}^X$. Let
$$V = \{v \in \mathbb{F}^X : \sum_{x \in X} v[x] = 0\}.$$
Then V is sub-representation of $\mathbb{F}^X$.
3. Regular representation: permutational representation when $X = G$.

Main Theorem

Theorem (Main Theorem)

(ρ, V) irrep. of G Let $g_1, g_2, \ldots g_q \in G, c_1, \ldots c_q \in \mathbb{F}$ s. t.
$\sum c_i \rho(g_i)$ is a rank one matrix
then there exists $(q, \delta, q\delta)$ LDC

$$\mathcal{C} : V \to \mathbb{F}[G].$$

Example of LDC

Example

Let $G = S_n$,

1. $(\rho, \mathbb{F}^n)$ perm. reps. Let $V = \{v \in \mathbb{F}^n : \sum_{i=1}^n v[i] = 0\}$ is an irreducible sub-reps. Let $g_1 = id, g_2 = (1,2)$ then

$$(\rho(g_1) - \rho(g_2))v = (v[1] - v[2])(1, -1, 0, \ldots, 0).$$

   Thus $\rho(g_1) - \rho(g_2)$ rank one matrix.

2. This gives [n-1,n!] LDC with 2-queries.

Conclutions and Future Work

- Give a conditions for representations to have sparse rank one element.
- Prove any non-trivial lower bounds for this model.
- Extend this model for modular representation theory.