The Role of Symmetry in LDCs and the Representations Theory

Klim Efremenko

Ben Gurion University

February 13, 2020

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 Talk

We study the role of symmetry in the construction of LDCs. We will look on the LDCs from the perspective of representation theory.

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 Talk

We study the role of symmetry in the construction of LDCs. We will look on the LDCs from the perspective of representation theory.

Definition of Self Correctable Codes

Definition: Locally Decodable Codes

$C(x_1, x_2, \ldots, x_n) = (c_1, c_2, \ldots, c_N)$
is (q, δ, ε)-LDC if 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 $1 - \varepsilon$)

Definition: Self Correctable Codes

$C(x_1, x_2, \ldots, x_n) = (c_1, c_2, \ldots, c_N)$
is (q, δ, ε)-LDC if c_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 $1 - \varepsilon$)

Example

Hadamard Code, Reed-Muller Code.

Definition of Self Correctable Codes

Definition: Locally Decodable Codes

$C(x_1, x_2, \ldots, x_n) = (c_1, c_2, \ldots, c_N)$
is (q, δ, ε)-LDC if 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 $1 - \varepsilon$)

Definition: Self Correctable Codes

$C(x_1, x_2, \ldots, x_n) = (c_1, c_2, \ldots, c_N)$
is (q, δ, ε)-LDC if c_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 $1 - \varepsilon$)

Example

Hadamard Code, Reed-Muller Code.

G-Invariant Codes

Definition: Two transitive group

Let G be a group acting on the set X. A group G called two transitive if for every $x_1 \neq x_2 \in X$ and $y_1 \neq y_2 \in X$ there exist $g \in G$ s.t. $g \cdot x_1 = y_1, g \cdot x_2 = y_2$.

Example

1. S_n group of all permutations acts on $[n]$.
2. Affine group $G = \{x \mapsto ax + b : a, b \in \mathbb{F}_q\}$ acts on $\mathbb{F}_q$.
3. $GL_n(\mathbb{F}_q)$ acts on $\mathbb{F}_q^n \backslash \{\vec{0}\}$

Two Transitive Groups

If G acts on X it is also acts on vector space $\mathbb{F}^X$ by permuting coordinates. $(g \cdot v)[x] = v[g \cdot x]$

Definition: G–Invariant Codes

Let G be a group acting on the set X. A code $\mathcal{C} \subset \mathbb{F}^X$ is a G-invariant if $c \in \mathcal{C}$ then $g \cdot c \in \mathcal{C}$.

Example

1. Hadamard code invarient under GL_n.
2. Reed-Solomon code invariant under affine group.
3. Reed-Muller Code invariant under GL_n.

Two Transitive Codes Self Correctable

Theorem

Let G two transitive group acting on X and $\mathcal{C} \subset \mathbb{F}^X$ is a G-invariant code. Then if $\mathcal{C}^\perp$ has a codeword of sparsity $q+1$ then $\mathcal{C}$ is self correctable.

Decoder

Exist $a_i \in \mathbb{F}_q, b_i \in X$ such that for any $c \in \mathcal{C}$ holds $\sum_{i=0}^{q} a_i c(b_i) = 0$. $(a_0 = 1)$
Consider a set $H_i = \{g \in G : g \cdot b_0 = i\}$. $H \neq \emptyset$. Pick $h \in H_i$ random. Return $-\sum_{i=1}^{q} a_i w(h \cdot b_i)$

Smooth LDC

Smooth LDC

A code is smooth LDC with q queries iff

- d_i makes q queries
- Smoothness: Each one query is uniformly distributed.
- Completeness: $d_i(C(x_1, x_2, \ldots, x_n)) = x_i$

Theorem

smooth-LDC is $(q, \delta, q\delta)$-LDC

Smooth LCC

Smooth LCC

A code is smooth LCC with q queries iff

- d_i makes q queries
- Smoothness: Each one query is uniformly distributed.
- Completeness: $d_i(c_1, \ldots c_N) = c_i$.

Theorem

smooth-LCC is $(q, \delta, q\delta)$-LCC

Two Transitive Codes Self Correctable

Theorem

Let G two transitive group acting on X and $\mathcal{C} \subset \mathbb{F}^X$ is a G-invariant code. Then if $\mathcal{C}^\perp$ has a codeword of sparsity $q+1$ then $\mathcal{C}$ is self correctable.

Proof.

Smoothness: G two transitive. For every b $j \neq i$ exist $h \in H_i$ s.t. $h \cdot b = j$.

Completeness: For every $c \in \mathcal{C}$ holds $\sum_{i=0}^{q} a_i c(b_i) = 0$. $\mathcal{C}$ is G invariant therefore holds also for $g \cdot c$. $\sum_{i=0}^{q} a_i c(g \cdot b_i) = 0$.

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 $X = G$.

Group Algebra

Definition (Group Algebra)

$\mathbb{F}[G]$ is group algebra of formal sums:

$$\sum_{g \in G} c_g g.$$

Multiplication defined naturally.

Notation:

We can extend any representation $\rho : G \mapsto GL(V)$ to $\rho : \mathbb{F}[G] \to Mat(V)$.
Note for $a, b \in \mathbb{F}[G]$ it holds: $\rho(ab) = \rho(a)\rho(b)$.

Definition: Irreducible Representations

Lemma

A representation (ρ, V) *is irreducible iff* $\forall v \neq 0$ *the set* $\{\rho(g)v : g \in G\}$ *spans the space* V*.*

Proof.

Let $W \subsetneq V$ sub-representation $\Rightarrow \rho(g)w \in W$ for $w \in W$.
Let $W = span\{\rho(g)v : g \in G\} \subsetneq V$ then W is a sub-representation of V □

Main Theorem

Theorem (Main Theorem)

(ρ, V) irrep. of G and $D = \sum_{i=1}^{q} c_i g_i \in \mathbb{F}[G]$ s.t. $\rho(D)$ of rank one. Then there exists $(q, \delta, q\delta)$ LDC

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

Proof Outline.

1. We show if we have $\mathcal{C}$ which admits some conditions then it is LDC.
2. We can also construct such $\mathcal{C}$.

Homomorphisms of Representations

Definition

A linear mapping $T : V \to W$ is an homomorphism from (ρ_1, V) to (ρ_2, W) iff $\forall g \in G \; \rho_2(g) \circ T = T \circ \rho_1(g)$.

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ \rho_1(g) \downarrow & & \downarrow \rho_2(g) \\ V & \xrightarrow{T} & W \end{array}$$

Example

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.
2. Let X be all subsets of n of size k.
3. Let $\mathcal{C} : \mathbb{F}^n \to \mathbb{F}^X$ defined by $\mathcal{C}(x_1, x_2, \ldots, x_n) = g$,where

$$g(S) = \sum_{j \in S} x_j.$$

Then $\mathcal{C}$ is an homomorphism of the permutational representations.

Theorem 1

Theorem

Assume that we have:

1. (ρ, V) *irrep. of* G *and* $D = \sum_{i=1}^{q} c_i g_i \in \mathbb{F}[G]$ *s.t.* $\rho(D)$ *of rank one.*
2. *Homomorphism of reps* $\mathcal{C} : V \to \mathbb{F}^X$.
3. *Let* $v \in Im(\rho(D))$ *it holds that* $supp(\mathcal{C}(v)) \geq c|X|$.

Then there exists a basis $b_1, \ldots, b_k$ *for* V *such that*

$$(m_1, m_2, \ldots, m_k) \mapsto \mathcal{C}(\sum_{i=1}^{k}(m_i b_i))$$

is a $(q, \delta, \frac{q\delta}{c})$*-LDC.*

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

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

2. Let X be all subsets of n of size $n/2$.
3. $\mathcal{C}(x_1, x_2, \ldots, x_n) = g$,where

$$g(S) = \sum_{j \in S} x_j.$$

Support of $\mathcal{C}(1, -1, 0, \ldots, 0) = \frac{|X|}{2}$.

Proof of Theorem 1.

Lemma (Construction of basis)

Exists a basis $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $\rho(D \cdot h_j)b_i = \delta_{ij} v$.

Encoding and Decoding Algorithm

Encoding Algorithm

$(m_1, m_2, \ldots, m_k) \mapsto \mathcal{C}(\sum_{i=1}^{k}(m_i b_i))$

Decoding Algorithm

Input: $w \in \mathbb{F}^X$, index i.

1. Pick $r \in X$ at random from the support of $\mathcal{C}(v)$.
2. For $j = 1, \ldots, q$ query w at location: $(g_j h_i)^{-1} \cdot r \in X$.
3. Calculate $n_i \triangleq \sum_{j=1}^{q} c_j w[(g_j h_i)^{-1} \cdot r] = \tau(D \cdot h_i) w[r]$.
4. Return $m_i = \mathcal{C}(v)[r]^{-1} n_i$.

Proof of Theorem

Proof.

Smoothness: Trivial

Completness:

1. Observe that $n_i = (\tau(Dh_i)w)[r]$.
2. If $w = \mathcal{C}(\sum(m_i b_i))$ then $n_i = m_i v[r]$.
   $\mathcal{C}$ is homomorphism thus:

$$n_i = \tau(Dh_i)\mathcal{C}(\sum_j m_j b_j)[r] = \mathcal{C}(\rho(Dh_i)\sum_j m_j b_j)[r].$$

Use lemma $n_i = \mathcal{C}(m_i \rho(Dh_i) b_i)[r] = m_i v[r]$.

Proof of Theorem

Proof.

Smoothness: Trivial

Completness:

1. Observe that $n_i = (\tau(Dh_i)w)[r]$.
2. If $w = \mathcal{C}(\sum(m_i b_i))$ then $n_i = m_i v[r]$.
   $\mathcal{C}$ is homomorphism thus:

$$n_i = \tau(Dh_i)\mathcal{C}(\sum_j m_j b_j)[r] = \mathcal{C}(\rho(Dh_i)\sum_j m_j b_j)[r].$$

Use lemma $n_i = \mathcal{C}(m_i \rho(Dh_i) b_i)[r] = m_i v[r]$.

Dual Vector Space

Definition

V vector space, *dual* V^* linear functionals from V to $\mathbb{F}$.
$b_1 \dots b_k$ basis of V *dual basis* of V^* is: $\ell_1 \dots \ell_k$, s.t. $\ell_i(v_j) = \delta_{ij}$.
(ρ, V) reps of G *dual representation* $(\bar{\rho}, V^*)$ define by:
$(\bar{\rho}(g)\ell)(v) = \ell(\rho(g^{-1})v)$

Lemma

For every basis exist dual basis
(ρ, V) *irreducible* $\Leftrightarrow$ $(\bar{\rho}, V^*)$ *irreducible.*

Proof of Lemma

Lemma

Exists a basis $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $\rho(D \cdot h_j)b_i = \delta_{ij}v$.

Proof.

- define u by: $\rho(D)x = u(x)v$ for $u \in V^*$.
- (ρ, V) irreducible V^* irreducible
- $\{\rho(h)u\}_{h\in G}$ span $V^* \Rightarrow \exists\ h_1, \ldots h_k$ s.t. $\bar{\rho}(h_i^{-1})u$ basis of V^*
- $b_1, \ldots b_k$ dual basis of $\bar{\rho}(h_i^{-1})u$
- $\rho(D \cdot h_j)(x) = \rho(D)(\rho(h_i)x) = u(\rho(h_i)x)v = \bar{\rho}(h_i^{-1})u(x)v$

Proof of Lemma

Lemma

Exists a basis $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $\rho(D \cdot h_j)b_i = \delta_{ij}v$.

Proof.

- define u by: $\rho(D)x = u(x)v$ for $u \in V^*$.
- (ρ, V) irreducible V^* irreducible
- $\{\rho(h)u\}_{h\in G}$ span $V^* \Rightarrow \exists\ h_1, \ldots h_k$ s.t. $\bar{\rho}(h_i^{-1})u$ basis of V^*
- $b_1, \ldots b_k$ dual basis of $\bar{\rho}(h_i^{-1})u$
- $\rho(D \cdot h_j)(x) = \rho(D)(\rho(h_i)x) = u(\rho(h_i)x)v = \bar{\rho}(h_i^{-1})u(x)v$

Proof of Lemma

Lemma

Exists a basis $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $\rho(D \cdot h_j)b_i = \delta_{ij}v$.

Proof.

- define u by: $\rho(D)x = u(x)v$ for $u \in V^*$.
- (ρ, V) irreducible V^* irreducible
- $\{\rho(h)u\}_{h\in G}$ span $V^* \Rightarrow \exists\ h_1, \ldots h_k$ s.t. $\bar{\rho}(h_i^{-1})u$ basis of V^*
- $b_1, \ldots b_k$ dual basis of $\bar{\rho}(h_i^{-1})u$
- $\rho(D \cdot h_j)(x) = \rho(D)(\rho(h_i)x) = u(\rho(h_i)x)v = \bar{\rho}(h_i^{-1})u(x)v$

Proof of Lemma

Lemma

Exists a basis $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $\rho(D \cdot h_j)b_i = \delta_{ij}v$.

Proof.

- define u by: $\rho(D)x = u(x)v$ for $u \in V^*$.
- (ρ, V) irreducible V^* irreducible
- $\{\rho(h)u\}_{h\in G}$ span $V^* \Rightarrow \exists\ h_1, \ldots h_k$ s.t. $\bar{\rho}(h_i^{-1})u$ basis of V^*
- $b_1, \ldots b_k$ dual basis of $\bar{\rho}(h_i^{-1})u$
- $\rho(D \cdot h_j)(x) = \rho(D)(\rho(h_i)x) = u(\rho(h_i)x)v = \bar{\rho}(h_i^{-1})u(x)v$

Embeding to Permutational Representation

Lemma

$\forall(\rho, V)$ *irep. and* $v \in V$ *exist G-homomorphism* $C : V \to \mathbb{F}^G$ *s.t.* $supp(C(v)) \geq \frac{G}{2}$.

Proof.

For $u \in V^*$ define:

$$C_u(x) = \sum_{g \in G} (u(\rho(g^{-1})x))g. \tag{1}$$

C_u is a G-homomorphism.
$\{C_u(v) : u \in V^*\}$ linear vector space with full support.
For some u $C_u(v)$ has large support. □

Embeding to Permutational Representation

Lemma

$\forall(\rho, V)$ *irep. and* $v \in V$ *exist G-homomorphism* $C : V \to \mathbb{F}^G$ *s.t.* $supp(C(v)) \geq \frac{G}{2}$.

Proof.

For $u \in V^*$ define:

$$C_u(x) = \sum_{g \in G} (u(\rho(g^{-1})x))g. \tag{1}$$

C_u is a G-homomorphism.

$\{C_u(v) : u \in V^*\}$ linear vector space with full support.

For some u $C_u(v)$ has large support. □

Embeding to Permutational Representation

Lemma

$\forall(\rho, V)$ *irep. and* $v \in V$ *exist G-homomorphism* $C : V \to \mathbb{F}^G$ *s.t.* $supp(C(v)) \geq \frac{G}{2}$.

Proof.

For $u \in V^*$ define:

$$C_u(x) = \sum_{g \in G} (u(\rho(g^{-1})x))g. \tag{1}$$

C_u is a G-homomorphism.
$\{C_u(v) : u \in V^*\}$ linear vector space with full support.
For some u $C_u(v)$ has large support. □

Matching Vector Codes

Goal

Describe matching vector codes(MVC) in framework of irreducible representations.

Matching Vectors

Definition (Dual group)

Let A be an abelian group. Then dual group A^* is the set of the group homomorphisms $v : A \to Z_m$, where m is the order of A.

Definition (Matching Vectors)

Let $S \subset \mathbb{Z}_m - \{0\}$, the families $\mathcal{U} = \{u_i\}_{i=1}^k \subset A, \mathcal{V} = \{v_i\}_{i=1}^k \subset A^*$ are *S-Matching Vectors(MV)* if

1. $v_j(u_i) \in S$ for every $i \neq j$.
2. $v_i(u_i) = 0$ for every $i \in [k]$.

Matching Vector Codes

Definition (Matching Vector Codes)

Let $\gamma \in \mathbb{F}^*, \gamma^m = 1$. Let $\{u_i\}_{i=1}^k, \{v_i\}_{i=1}^k$ be S-matching vectors. $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^A$ given by

$$(m_1, m_2, \ldots m_k) \mapsto \sum_{i=1}^{k} m_i \gamma^{v_i}$$

Semidirect Produt

Definition

A group H acts on a *group* A if it acts on it as a set and

$$h \cdot (a_1 + a_2) = h \cdot a_1 + h \cdot a_2.$$

Definition (Semidirect product)

Let H acts on a group A. A semi-direct product group $G = A \rtimes H < Sym(A)$ is a group generated by permutations: $x \mapsto x + a$ and $x \mapsto h \cdot x$.

Note

$\mathbb{F}^A$ is a permutational representation of $G = A \rtimes H$.

Symetric Matching Vectors

Definition

Let H acts on A. We say that MV $\{u_i\}_{i=1}^k, \{v_i\}_{i=1}^k$ symmetric if for every i, j exists $h \in H$ s.t. $h \cdot u_i = u_j$.

Observation

All good constructions of MV are symmetric.

Symetric Matching Vectors

Definition

Let H acts on A. We say that MV $\{u_i\}_{i=1}^k, \{v_i\}_{i=1}^k$ symmetric if for every i, j exists $h \in H$ s.t. $h \cdot u_i = u_j$.

Observation

All good constructions of MV are symmetric.

Theorem

Let H acts on A and $\{u_i\}_{i=1}^k, \{v_i\}_{i=1}^k$ be a symmetric MV. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^A$ be a MVC. Then there exists an irreducible representation $\rho : G \mapsto GL(\mathbb{F}^k)$ s.t. $\mathcal{C}$ is a G-homomorphism.

If there exist S-decoding polynomial of sparsity q then there exist $D = \sum_{i=1}^q c_i g_i$ with $\rho(D)$ of rank one.

Theorem

Let H acts on A and $\{u_i\}_{i=1}^k, \{v_i\}_{i=1}^k$ be a symmetric MV. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^A$ be a MVC. Then there exists an irreducible representation $\rho : G \mapsto GL(\mathbb{F}^k)$ s.t. $\mathcal{C}$ is a G-homomorphism. If there exist S-decoding polynomial of sparsity q then there exist $D = \sum_{i=1}^q c_i g_i$ with $\rho(D)$ of rank one.

Conclusions

Conclusions

1. We show the connection between representation theory and LDCs.
2. We show that MVC are special case of irreducible representations.
3. It is possible to extend this framework for modular representations.

Open Problems

1. Construct ”large” representations with sparse element in group algebra of rank one.
2. Does $\mathbb{F}^A$ is the best possible permutational representation for embedding?

Conclusions

Conclusions

1. We show the connection between representation theory and LDCs.
2. We show that MVC are special case of irreducible representations.
3. It is possible to extend this framework for modular representations.

Open Problems

1. Construct ”large” representations with sparse element in group algebra of rank one.
2. Does $\mathbb{F}^A$ is the best possible permutational representation for embedding?

Conclusions

Conclusions

1. We show the connection between representation theory and LDCs.
2. We show that MVC are special case of irreducible representations.
3. It is possible to extend this framework for modular representations.

Open Problems

1. Construct ”large” representations with sparse element in group algebra of rank one.
2. Does $\mathbb{F}^A$ is the best possible permutational representation for embedding?

Thanks

Thank you!!!