On isomorphism problem for cyclic codes

Misha Muzychuk

Netanya Academic College,
Israel

Rogla, August, 2010

Linear codes

Let $\mathbb{F}_q, q = p^e$ be a finite field

Definition

An $[n, k]_q$-linear code is a k-dimensional subspace C of $\mathbb{F}_q^n$. The numbers n and k are called the length and dimension of a code.

A generating matrix G of C is any matrix the rows of which form a basis of C. Thus G is a full rank matrix.
Two full rank matrices of size $k \times n$ define the same $[n, k]_q$-code iff they are row equivalent.

Code equivalence

Two codes $C \leq \mathbb{F}_q^n$, $C' \leq \mathbb{F}_q^n$ are called (permutation) equivalent iff one of them may be obtained from another by permuting the coordinates. In other words, there exists an n-by-n permutation matrix P such that $CP = C'$.

The automorphism group of a code

Given a linear code $C \leq \mathbb{F}_q^n$, we define its automorphism group $\mathrm{Aut}(C)$ as the set of all $\pi \in S_n$ such that $CP_\pi = C$.

Code equivalence problem

Given two $[n, k]_q$ codes $C \leq \mathbb{F}_q^n, C' \leq \mathbb{F}_q^n$, find whether they are equivalent.

Matrix reformulation

Given two full-rank matrices $G, G' \in M_{k \times n}(\mathbb{F}_q)$. Does there exists a permutation matrix P such that GP and G' are row equivalent?
Do there exist $\pi \in S_n$ and $Q \in GL_k(\mathbb{F}_q)$ s.t. $QG' = GP_\pi$.

Code equivalence problem

Given two $[n, k]_q$ codes $C \leq \mathbb{F}_q^n$, $C' \leq \mathbb{F}_q^n$, find whether they are equivalent.

Matrix reformulation

Given two full-rank matrices $G, G' \in M_{k \times n}(\mathbb{F}_q)$. Does there exists a permutation matrix P such that GP and G' are row equivalent?
Do there exist $\pi \in S_n$ and $Q \in GL_k(\mathbb{F}_q)$ s.t. $QG' = GP_\pi$.

Open Problem

Does the exist an algorithm solving the code equivalence problem in time polynomial in q^k?

Automorphism group of a code

Given a linear $[n, k]_q$ code $C \leq \mathbb{F}_q^n$, find generators of its automorphism group $\mathrm{Aut}(C)$.

Matrix reformulation

Let $C \leq \mathbb{F}_q^n$ be an $[n, k]_q$ code and G its generating matrix. Then a permutation $\pi \in S_n$ is an automorphism of C iff there exists $Q(\pi) \in GL_k(\mathbb{F}_q)$ such that $GP_\pi = Q(\pi)G$.

Proposition

A mapping $\pi \mapsto Q(\pi)$ is a group homomorphism. It is monomorphism iff G has no repeated columns.

Cyclic and group codes

Cyclic codes

An $[n,k]_q$ codes $C \leq \mathbb{F}_q^n$ is called cyclic if it is invariant under cyclic shift $(c_0, ..., c_{n-1}) \mapsto (c_1, ..., c_{n-1}, c_0)$.

The vector space $\mathbb{F}_q^n$ may be identified with the group algebra $\mathbb{F}_q[H]$ of a cyclic group H generated by $h \in H$. In this case a cyclic code is an ideal of $\mathbb{F}_q[H]$. Since $\mathbb{F}_q[H] \cong \mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal algebra, every cyclic code has a form $g(h)\mathbb{F}_q[H]$ where $g(x)$ is a divisor of $x^n - 1$.

Group codes

Given a finite group H, any right ideal of the group algebra $\mathbb{F}_q[H]$ is called a group code over H. A group code is called semisimple if $gcd(q, |H|) = 1$.

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Examples

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Examples

1. Cayley graphs/digraphs/colored graphs;

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Examples

1. Cayley graphs/digraphs/colored graphs;
2. Cayley maps;

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Examples

1. Cayley graphs/digraphs/colored graphs;
2. Cayley maps;
3. Cayley designs = difference families;

Cayley combinatorial objects

Definition

For each group H we denote by $h_R \in \mathrm{Sym}(H)$ the right translation by h, that is $x^{h_R} = xh$.

Definition

A Cayley combinatorial object is a relational structure on H invariant under the group H_R where $H_R := \{h_R \mid h \in H\}$.

Examples

1. Cayley graphs/digraphs/colored graphs;
2. Cayley maps;
3. Cayley designs = difference families;
4. group codes;

Isomorphism problem for Cayley combinatorial objects

Problem

Given two Cayley combinatorial objects $C, C' \in \mathcal{C}$ over H. Find whether they are isomorphic.

Cayley equivalence

Two Cayley objects C and C' are Cayley equivalent/isomorphic, notation $C \cong_{Cay} C'$, if there exists $\pi \in \mathrm{Aut}(H)$ such that $C^{\pi} = C'$.

CI-groups

A group H is called a CI-group w.r.t. to a class $\mathcal{C}$ of Cayley objects over H if for any pair of $C, C' \in \mathcal{C}$ it holds that

$$C \cong C' \iff C \cong_{Cay} C'$$

Solving sets

Let $\mathcal{C}$ be a class of of Cayley objects over a group H

Definition

A set of permutations $S \subseteq \mathrm{Sym}(H)$ is called a solving sets for $\mathcal{C}$ iff for any pair $C, C' \in \mathcal{C}$ it holds that

$$C \cong C' \iff \exists_{\sigma \in S} C^{\sigma} = C'.$$

Being a CI-group w.r.t. $\mathcal{C}$ is equivalent to saying that $\mathrm{Aut}(H)$ is a solving set for $\mathcal{C}$.

Main Results

Theorem (CFSG-dependent)

Any solving set for colored circulant digraphs of order n is a solving set for semisimple cyclic codes of length n.

Corollary A

A cyclic group of square-free or twice square-free order n is a CI-group w.r.t. semisimple cyclic codes of length n.

Corollary B

There exists a solving set for semisimple cyclic codes of order n of size $O(n^3)$.

Group codes over p-groups.

Theorem

Any solving set for colored Cayley digraphs over a p-group H is also a solving set for semisimple group codes over H.

Corollary

An elementary abelian group H of order p^e, $e \leq 4$ is a CI-group with respect to semisimple group codes over H.

Main observation

Proposition

Let $C \leq \mathbb{F}_q^n$ be a linear code and $E \in M_n(F_q)$ be a projector onto C. Then each permutation matrix commuting with E is an automorphism of C. In particular, $C_{S_n}(E) \leq \mathrm{Aut}(C)$.

Proposition

For any matrix $E \in M_n(\mathbb{F}_q)$ the group $C_{S_n}(E)$ is 2-closed.

2-closed permutation groups

Recall that the orbits of the diagonal action of $G \leq S_n$ on the set of pairs $(i,j), 1 \leq i,j \leq n$ are called 2-orbits of G.

Definition

A 2-closure $G^{(2)}$ of G is the unique maximal subgroup of S_n that has the same 2-orbits as G.

Properties of 2-closure

1. $H \leq G \implies H^{(2)} \leq G^{(2)}$;
2. $G \leq G^{(2)}$;
3. $(G^{(2)})^{(2)} = G^{(2)}$

2-closed subgroups of the code automorphism group

Lemma

Let H be a subgroup of $\mathrm{Aut}(C)$, $C \leq \mathbb{F}_q^n$. If $\gcd(q, |H|) = 1$, then $H^{(2)} \leq \mathrm{Aut}(C)$. In particular, any Sylow r-subgroup of $\mathrm{Aut}(C)$ with $\gcd(r, q) = 1$ is 2-closed.

Proof.

Since $H \leq S_n$, the vector space $\mathbb{F}_q^n$ is an $\mathbb{F}_q[H]$-module. The code C is an $\mathbb{F}_q[H]$-submodule. The algebra $\mathbb{F}_q[H]$ is semisimple. By Maschke'e Theorem there exists a $\mathbb{F}_q[H]$-submodule of $\mathbb{F}_q^n$ complementary to C. Let E be a projector onto C with kernel D. Then E commutes with each permutation matrix $P_\pi, \pi \in H$. Thus $H \leq C_{S_n}(E) \leq \mathrm{Aut}(C)$ implying $H \leq H^{(2)} \leq C_{S_n}(E) \leq \mathrm{Aut}(C)$. □