The Equivalence Problem for Cyclic Combinatorial Objects

K. Guenda

Dept. of Electrical and Computer Engineering

University of Victoria

CanaDAM, June. 11, 2013

- $T = (12 \ldots n)$ is the complete cycle of length n
  $T : i \longmapsto i + 1 \mod n$
- The automorphism group of $\mathcal{C}$ is

$$Aut(\mathcal{C}) = \{\sigma \in S_n; \sigma(\mathcal{C}) = \mathcal{C}\}$$

- $AG(n) = \{\tau_{a,b},\ a \neq 0, (a, n) = 1, b \in Z_n\}$

$$\begin{aligned} \tau_{a,b} : Z_n &\longrightarrow Z_n \\ i &\longmapsto (ai + b) \mod n \end{aligned} \tag{1}$$

  Multiplier $\tau_{a,0} = \mu_a$

- A class of cyclic objects on n elements is a class of combinatorial objects on these elements.
- Isomorphisms of objects in this class are permutations of S_n, and the automorphism group of each object in the class contains T.

Examples

- Circulant graphs
- Circulant digraphs
- Cyclic designs
- Cyclic codes

Problems

- Find $\sigma \in S_n$ such that $\sigma(\mathcal{C}) = \mathcal{C}'$
- Find $Aut(\mathcal{C}) = \{\sigma \in S_n; \sigma(\mathcal{C}) = \mathcal{C}\}$

Motivation

- Cryptosystems (McEliece,....)
- Permutation decoding (PD set)
- Weight distribution of codes
- Optical character recognition
- Image processing

Previous Work

- Knapp, Schmid. 1978
- Dobson and Witte. 2002-2005
- Bienert, Klopsch. 2010
- Li and Praeger 2012
- Sendrier, Skersys. 1996-1999
- Babai, Codenotti and Groshow. 2011
- Lambossy, Alspach, Parson, Palfy, Morris, Brand, Huffman, Job and Pless. 1937-2006

Classification of $Aut(\mathcal{C})$

- $Aut(\mathcal{C})$ is an imprimitive group; or

- $Aut(\mathcal{C}) = S_n$ or $Alt(n)$.
- $N = C_p \leq Aut(\mathcal{C}) \leq AG(p)$.
- $Aut(\mathcal{C}) = PSL(2, 11)$; .
- $Aut(\mathcal{C}) = M_{11}$ or $Aut(\mathcal{C}) = M_{23}$, .
- $N = PSL(d, r^{d^b})$ and $PGL(d, r^{d^b}) \leq Aut(\mathcal{C}) \leq P\Gamma L(d, r^{d^b})$ where $d \in \mathbb{N}$, $d \geq 3$ and r is a prime number such that $(d, r-1) = 1$, and $p = (r^{d^{b+1}} - 1)/(r^{d^b} - 1)$, or

Cyclic Codes over $\mathbb{F}_q$

- $Aut(\mathcal{C}) = S_n$; or
- $C_p \leq Aut(\mathcal{C}) \leq AG(p)$, $n = p$; or
- $Aut(\mathcal{C}) = PSL(2, 11)$ and q is a power of 3; or
- $Aut(\mathcal{C}) = M_{23}$ and q is a power of 2; or
- $Aut(\mathcal{C}) = P\Gamma L(d, r^{d^b})$ where $d \in \mathbb{N}$, $d \geq 3$ and $n = (r^{d^{b+1}} - 1)/(r^{d^b} - 1)$, $q = r^a$; or

- $Aut(\mathcal{C})$ is an imprimitive group

Cyclic Codes of Length p^m over $\mathbb{F}_p$

- If $m = 1$, then

$$Aut(\mathcal{C}) = AG(p),$$

- If $p \geq 5$, then $Aut(\mathcal{C})$ is an imprimitive group
  - It also contains a transitive p-Sylow subgroup of order p^s with

$$m < s \leq p^{m-1} + p^{m-2} + \ldots + 1$$

Cyclic Codes of Length p^m over $\mathbb{F}_{r^\alpha}$

Let z be the largest integer such that $p^z | (r^{\alpha t} - 1)$

If $z = 1$, $p \nmid \alpha$ and $p \nmid (d, r^a - 1)$, then

- $Aut(\mathcal{C})$ is an imprimitive group which contains a transitive Sylow p-subgroup of order p^s, with

$$2m - 1 \leq s \leq p^{m-1} + p^{m-2} + \ldots + 1$$

Multiplier Equivalency

Alspach, Parson. 1979, Palfy. 1987

Let $\mathcal{C}$ and $\mathcal{C}'$ be two cyclic combinatorial objects on n elements

- If $(n, \phi(n)) = 1$, or
- $n = 4$, or
- $n = p \cdot r$, $p > r$ and $|P| = p$, then

$\mathcal{C}$ and $\mathcal{C}'$ can be equivalent only by a multiplier

Equivalency when $n = p^m$

- $P \leq Aut(\mathcal{C}); T \in P$
- $H(P) = \{\sigma \in S_n | \sigma^{-1} T \sigma \in P\}$
- $\mathcal{C}' = \sigma(\mathcal{C}) \iff \sigma \in H(P)$

Brand's Sets

$\mathcal{A} = \{f : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_{p^m}[x]_n, f(x) = \sum_{i=0}^{n} a_i x^i\}$

- $Q^n = \{f \in \mathcal{A}|, (p, a_1) = 1, p^{m-1}$ divides a_i for $i = 2, 3, \ldots, n\}$
- $Q_1^n = \{f \in Q^n | f(x) = \sum_{i=0}^{n} a_i x^i,$ with $a_1 \equiv 1 \bmod p^{m-1}\}$

$m = 2$: Cylic Objects and Cyclic Codes, Job, Huffman and Pless

- $H(Q_1^n) = Q^{n+1}$
- Q_1^{p-1} is the p-Sylow subgroup of S_{p^2}
- $\langle T \rangle \leq Q_1^1 \leq \ldots \leq Q_1^{p-1}$ is the unique maximal chain of p-groups of S_{p^2}, such that T is minimal

$m > 2$

- Q_1^1 is the unique subgroup of S_{p^m} of order p^{m+1} which contains T.
- If P is a p group of S_{p^m} with $Q_1^n \lneq P \leq Q^{n+1}$, then $P = Q_1^{n+1}$

- If a p-subgroup P of S_{p^m} contains T and is of order $\leq p^{p+m-1}$, then P is in the chain

$$\langle T \rangle \leq Q_1^1 \leq \ldots \leq Q_1^{p-1}$$

Let $G \leq S_{p^m}$ and P be a p-Sylow subgroup of G of order p^s such that $T \in P$. Then the following holds:

- If $s = m, P =< T >$
- If $m < s \leq p + m - 1$, then we have $P = Q_1^{s-m}$

If $|P| = p^s$ and $s \leq p + m - 1$.
Then $\mathcal{C}$ and $\mathcal{C}'$ can be equivalent only under the permutation of the following subgroups of S_{p^m}:

- $AG(p^m)$ if $s = m$; or
- Q^{s-m+1} if $s > m$

Serious Problem !!!

How to find s ??

Nice Permutations !!

- $f_i(x) = x + p^{m-1}(x + x^2 + \ldots + x^i) \in Q_1^i$
  for $1 \leq i \leq p-2$

Let $G \leq S_{p^m}$ with a p-Sylow subgroup P.

If $f_i \notin G$ then $P =< T >$

Let I be the largest value of i such that $f_i \in G$.

- If $I \leq p-2$, then $P = Q_1^I$.

Algorithm A

Then the equivalence of $\mathcal{C}$ and $\mathcal{C}'$ can be determined as follows.

Step 1: Find the order of the Sylow subgroup of $Aut(\mathcal{C})$ as follows. Find the largest I such that $f_I \in Aut(\mathcal{C})$. If I does not exist then $s = m$.

If $I = p - 1$, then declare a failure.

If $\emptyset \neq I < p-1$, then $s = I + m$ and do Step 2.

Step 2: Find $f \in Q^{I+1}$ such that $\mathcal{C}' = f\mathcal{C}$.

Question ???

Is the complexity of the Algorithm Polynomial?

Answer

If you can specify it you can Analyze it

To find the required I in Algorithm A, a binary search can be used which requires checking at most $\lceil \log_2(p-1) \rceil + 1$ of the f_i. Furthermore, the cardinality of Q^{I+1} is $(p-1)p^{2m+I-2}$.