Comm. Korean Math. Soc. **11** (1996), No. 3, pp. 575–584

CODE AUTOMORPHISM GROUP ALGORITHMS AND APPLICATIONS

HAN HYUK CHO*, HYE SUN SHIN AND TAE KYUNG YEO

ABSTRACT. We investigate how the code automorphism groups can be used to study such combinatorial objects as codes, finite projective planes and Hadamard matrices. For this purpose, we write down a computer program for computing code automorphisms in PASCAL language. Then we study the combinatorial properties using those code automorphism group algorithms and the relationship between combinatorial objects and codes.

1. Introduction

There are many kinds of automorphism groups in mathematics. Amo ng them such automorphism groups as code automorphisms, disign automorphisms and graph automorphisms are important to combinatorics. These automorphism groups play a key role in determining the corresponding structure, and provide a playground to study elementary algebra and geometry (group actions, projective transformations, etc.). In particular, code automorphism group is useful in determining the structure of codes, computing weight distributions, classfying codes, and devising decoding algorithms, and many kinds of code automorphism group algorithms were developed [4-6]. In this paper, we will investigate how the code automorphism group can be used to study some combinatorial structures. For this purpose, we compute the automorphism group of a given code using the computer programs written in PASCAL language [12]. Using these computational results, we can derive the structure of some combinatorial objects.

Received December 30, 1995. Revised April 20, 1996.

1991 AMS Subject Classification: 05, 15, 94.

Key words and phrases: code, code automorphism group, finite projective plane, Hadamard matrix.

*Partially supported by the Korea Research Foundation.

2. Codes and code automorphism groups

Let F be a finite field $GF(q)$. Any subset C of F^n is called an q-ary code, and each element in C is a codeword of C. If C is a subspace of F^n, then C is called a linear code [9]. In this section, we introduce basic definitions related to code automorphism group algorithms, and introduce some computations to find the weight distributions of a code using its automorphism group.

DEFINITION 2.1. Let C be a binary code of length n. The binary code of length $n+1$ obtained from C by adding parity check bit is called the extended code of C. The permutations of coordinate places which send C into itself form the *code automorphism group* of C denoted by $Aut(C)$ (codewords go into possibly different codewords). Two binary codes C_1 and C_2 are equivalent if there is a permutation of coordinate places which sends C_1 onto C_2. If $C \in GF(q)^n$ is a nonbinary code, $Aut(C)$ consists of all $n \times n$ monomial matrices A over $GF(q)$ such that $vA \in C$ for all $v \in C$.

Note that if two binary codes C_1 and C_2 are equivalent, then $Aut(C_1)$ and $Aut(C_2)$ are isomorphic. But the converse may not always hold. Let C be a binary code and H be a subgroup of $Aut(C)$. For a codeword $v \in C$, the number of 1's in the coordinate places of v is the weight of v. Usually A_i denotes the total number of codewords in C of weight i and is denoted by $wt(v)$, and $A_i(H)$ the number of codewords which are fixed by some element of H. Now, we will investigate a method of using the automorphism group to find out the weight distribution of a given code C. The following theorem is a known one, but we give a proof to explain the computations.

THEOREM 2.2. *Let C be a binary code and H be a subgroup of $Aut(C)$. Then, $A_i \equiv A_i(H) \pmod{|H|}$, where $|H|$ denotes the cardinality of H.*

PROOF. The codewords of weight i can be divided into two classes, those fixed by some element of H, and the rest. If $v \in C$ is not fixed by any element of H, then the $|H|$ codewords gv for $g \in H$ must all be distinct. Thus $A_i - A_i(H)$ is a multiple of $|H|$.

DEFINITION 2.3. Let C be a binary code of length n and G is a subgroup of $Aut(C)$. Then G acts on the coordinate places $\Omega = \{1, 2, \cdots, n\}$. A subset $\{c_1, \cdots, c_k\}$ of Ω is called a coordinate base for G provided that the identity element fixes all the coordinate places c_i's (i.e. stabilizer $G_{c_1,\cdots,c_k}$ = identity). A strong generators for G on Ω relative to the ordered coordinate base $\{c_1, \cdots, c_t\}$ is a generating set S for G such that $G_{c_1,\cdots,c_j}$ is generated by $S \cap G_{c_1,\cdots,c_j}$ for $j = 1, \cdots, k$.

Let $G^j = G_{c_1,\cdots,c_j}$, $G^0 = G$ and $\Delta_j = [G^{j-1} : G^j]$ for $j = 1, \cdots, k$. Note that $|Aut(C)| = \prod_{j=1}^{k} \Delta_j$ when $G = Aut(C)$.

COMPUTATION 2.4. Consider the (7,4,3) Hamming code C. The $Aut(C)$ determind by the computer algorithms is given as follows;

(1) Input : $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

(2) Output : 1) Coordinate base ; $1, 2, 3, 4$.

2) Strong generators ;

$$s_1 = (45)(67), \quad s_2 = (46)(57), \quad s_3 = (23)(67)$$
$$s_4 = (24)(35), \quad s_5 = (12)(56).$$

It follows that $Aut(C_1) =< s_1, s_2, s_3, s_4, s_5 >$ and $|Aut(C_1)| = 2^3 \times 3 \times 7 = 168$. For a prime p dividing $|Aut(C)|$, let H be a maximal subgroup of $Aut(C)$ whose order is a power of p (i.e. H is a Sylow p-subgroup of $Aut(C)$). If $g \in H$ fixes $v \in C$, the stabilizer H_v of v forms a subgroup of H. Thus $|H_v| \mid |H|$. On the other hand, the number of permutation which fixes the codeword with weight i is $i!(n-i)!$. Hence if $A_i(H) \neq 0$, then $|H_v| \mid i!(n-i)!$. Therefore, if $|H_v| \nmid i!(n-i)!$, then $A_i(H) = 0$. thus $A_i \equiv 0 \pmod{|H|}$.

Note that the minimum weight of C is 3 ($A_3 \neq 0$). Thus the number of permutation which fixes the codeword of weight 3 is $3!(7-3)!$. Let H be a Sylow 7-subgroup of $Aut(C)$. Then $|H| = 7 \nmid 3!4!$. Thus $A_3 \equiv 0 \pmod 7$. Since C is self-orthogonal, A_4 is nonzero. By the same method, $A_4 \equiv 0 \pmod 7$. Since the total number of codeword is $2^4 = 16$, the weight distribution of Hamming code is $A_3 = A_4 = 7$, $A_0 = A_7 = 1$. By

the same method the weight distribution of (8,4,4) extended Hamming code can be found as follows; $A_0 = A_1 = 1$, $A_4 = 14$.

COMPUTATION 2.5. Consider (24,12,8) Golay code C. The $Aut(C)$ determind by the computer algorithm is given as follows;

(1) Input : (24, 12, 8) Golay code [7, page 65]

(2) Output :

1) Coordinate base ; $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$.

2) Strong generators ; $s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8$.

It follows from the output that $Aut(C) = < s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8 >$, and $Aut(C) = 3 \times 16 \times 20 \times 21 \times 22 \times 23 \times 24 = 2^{10} \times 3^3 \times 5 \times 7 \times 11 \times 23$. In fact, it is known that the automorphism group of Golay code is equal to the much larger *Mathieu group* M_{24} and is a 5-fold transitive group. Since Golay code is self-dual and doubly even, A_i is nonzero for $i = 0, 8, 12, 16, 24$. Let H be a Sylow 23-subgroup of C. Note that the number of permutation which fixes the codeword with weight 8 is 8!16!, and $23 \nmid 8!16!$. Thus $A_8 = A_{16} \equiv 0 \pmod{23}$. By the same way, $A_{12} \equiv 0 \pmod{23}$ since $23 \nmid 12!12!$. Therefore, the weight distribution of Golay code is $A_0 = A_{24} = 1$, $A_8 = A_{16} = 23m$, $A_{12} = 23n$ $(m, n \in \mathbb{Z})$. In fact, it is known that $A_8 = A_{16} = 759 = 23 \times 33$, $A_{12} = 2576 = 23 \times 112$. For (23,12,7) Golay code that is a punctured code of (24,12,8) code, there exist A_i for $i = 0, 7, 8, 11, 12, 15, 16, 23$. By the same method, $\forall i$ $(i \neq 0, 23)$, $A_i \equiv 0 \pmod{23}$. Finally, we give a complete description of s_i's as follows;

$$s_1 = (7\,14\,11)(8\,16\,19)(9\,13\,20)(10\,15\,12)(17\,21\,23)(18\,22\,24),$$

$$s_2 = (6\,7)(8\,12)(9\,15)(10\,23)(11\,14)(13\,21)(16\,20)(17\,19)(22\,24),$$

$$s_3 = (6\,8)(7\,12)(9\,10)(11\,13)(14\,21)(15\,23)(16\,19)(17\,20)(22\,24),$$

$$s_4 = (5\,6)(8\,19)(9\,18)(10\,12)(11\,14)(13\,24)(17\,23)(20\,22),$$

$$s_5 = (4\,5)(7\,9)(10\,12)(11\,13)(14\,20)(16\,19)(17\,21)(22\,24),$$

$$s_6 = (3\,4)(7\,10)(8\,16)(9\,20)(11\,15)(12\,14)(17\,21)(18\,24),$$

$$s_7 = (2\,3)(8\,19)(9\,13)(10\,23)(11\,14)(12\,17)(15\,21)(18\,24),$$

$$s_8 = (1\,2)(8\,23)(10\,12)(11\,14)(13\,20)(16\,21)(17\,19)(22\,24).$$

Note that if we can find a subgroup H of $Aut(C)$ satisfying $A_i \equiv 0 \pmod{|H|}$, the weight distribution of C can be determined exactly by

Chinese Remainder theorem. In general, Theorem 2.2 is often proper enough to determine A_i exactly when $|Aut(C)|$ is large. Computation 2.4, 2.5 are the cases when there exists a subgroup with large prime order. Then how can Theorem 2.2 be used if there is no such a subgroup?

3. Projective planes and Hadamard matrices

In this section, we introduce incidence matrices of finite projective planes and Hadamard matrices. Then we investigate the codes generated by the incidence matrices and Hadamard matrices.

DEFINITION 3.1. A t-(v, k, λ) design consists of a set of v points and a set of b blocks satisfying the following;

(1) Each block has k points.
(2) Every t points lie on exactly λ blocks.

A $b \times v$ (0,1)-matrix $A = [a_{ij}]$ satisfying $a_{ij} = 1$ iff the j-th point is in the i-th block is called an incidence matrix of the design. A 2-$(v, m+1, 1)$ design with $v = b$, denoted by $PG(2, m)$, is called a *projective plane of order m*. In design, an automorphism is a permutation of its points which preserves the block set.

For all m equal to the power of a prime number, finite projective planes of order m can be constructed [3]. No planes have as yet been constructed for any other orders, but they are known to be impossible for infinitely many values of m. In 1989, it was shown that there is no projective plane of order 10 using sophisticated computer calculations. For a p-ary code in $GF(p)$, it is worth investigating the variation of the dimension and automorphism group of C according to changing of p. In fact, the some relations between design and p-rank are known [11]. It is also known that an incidence matrix of $PG(2, m)$ generates a self-orthogonal code.

THEOREM 3.2. *Let A be an incidence matrix of $PG(2, m)$ and C be a binary code of length n generated by the rows of A. If m is even, then $Aut(C) \cong Aut(PG(2, m))$. If m is odd, then $|Aut(C)| = n!$.*

PROOF. Note that $n = m^2 + m + 1$ and A is an $n \times n$ matrix. First, let m be even. We claim that every codeword having minimum weight in C is a line vector in $PG(2, m)$. Let $v \in C$ be a nonzero codeword having

the minimum weight d. Note that every line contains odd number of points and has a 1 as overall parity check. Thus if d is odd then v and each line vector have a positive common position. If d is even then v and every line vector having 1 in a fixed positive position of v have another positive common position. Therefore if d is even, then we have $d > m+1$. Also if d is odd, then we have $(m+1) \cdot d \geq m^2+m+1$ (i.e. $d \geq m+1$). Therefore the minimum weight is $m+1$. Now let $v \in C$ be a nonzero codeword with $wt(v) = m+1$. Then there is a line vector l of $PG(2,m)$ which has at least three common positive positions with v. If there is a positive position of l not on v, every other line vector having 1 at that position has a common positive position with v since v and every line vector have at least one common positive position. This would yield $wt(v) \geq m+3$. This is a contradiction. Therefore every vector of minimum weight in C is a line vector in $PG(2,m)$. Therefore every projective automorphism is a code automorphism and vice versa when m is even.

Next, let m be odd. If we take the sum of the rows of A which have a 1 in a fixed column position, the result is a vector with a 0 in that position and 1's elsewhere. Thus C is the code generated by the rows of the following $n \times n$ matrix

$$B = \begin{pmatrix} 0 & 1 & \cdots & \cdots & \cdots & 1 \\ 1 & 0 & 1 & & 1 & 1 \\ 1 & 1 & 0 & 1 & & 1 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & 1 & & \ddots & \ddots & 1 \\ 1 & \cdots & \cdots & \cdots & 1 & 0 \end{pmatrix}.$$

Here the sum of all the rows of B is 0 because m is odd. But the sum of all the rows of B except the last row gives a nonzero vector. Thus $rank\, B = dim\, C = m^2+m$. Now, consider the minimum weight d of C. Suppose C is a (n,k,d) code with $d \geq 3$, where $k = m^2+m$. Then

$$\left[\binom{n}{0} + \binom{n}{1}\right] \cdot 2^k \leq 2^n,$$

i.e.

$$(m^2+m+2) \cdot 2^{m^2+m} \leq 2^{m^2+m+1},$$

A contradiction since $m \geq 1$. Thus the minimum weight of C is 2. Therefore if m is odd, the vectors of C generate the subspace of $GF(2)^n$ consisting of all words of even weight. Hence, we conclude $|Aut(C)| = n!$.

COMPUTATION 3.3. Let D_1 be an incidence matrix of $PG(2,2)$. Note that $PG(2,2)$ contains 7 points and 7 lines, and the code C generated by D_1 has $h(x) = 1 + x + x^3$ as generator polynomial. Using the computer algorithm, we compute $Aut(C)$ as follows.

(1) Input : $\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

(2) Output :

1) Coordinate base ; 1, 2, 3, 4.

2) Strong generators ;

$$s_1 = (35)(67), \quad s_2 = (36)(57),$$
$$s_3 = (23)(47), \quad s_4 = (12)(57).$$

It follows from the output that $Aut(C) =< s_1, s_2, s_3, s_4 >$ and $|Aut(C)| = 4 \times 6 \times 7 = 168$.

COMPUTATION 3.4. Let D_2 be an incidence matrix of $PG(2,3)$ (we omit the description of D_2). Note that $PG(2,3)$ contains $13 (= 3^2 + 3 + 1)$ points and 13 lines. It follows that the code C generated by D_2 has $h(x) = x + x^2 + \ldots + x^{12}$ as generator polynomial, and consists of all codewords of even weight of length 13, and $|Aut(C)| = 13!$ by Theorem 3.2. We can verify our conjecture by the program, and the result is $Aut(C) =< s_1, s_2, \cdots, s_{12} >$ and $|Aut(C)| = 13!$. In $PG(2,m)$, if we choose a stabilizer of a given line, it is equivalent to an another stabilizer of a different line because an automorphism sends a line to an another line. So, stabilizers of all lines must be intersect with the Affine group which always invariants the infinite line, i.e. $H \cap A\Gamma L(2,m) = \emptyset$ implies $A_i(H) = 0$.

DEFINITION 3.5. A *Hadamard matrix* H of order n is an $n \times n$ matrix of $+1$'s and -1's such that $HH^T = H^TH = nI$. Hadamard matrix is a normalized Hadamard matrix in the sense that all entries in the first row and column are $+1$. Two Hadamard matrices are called equivalent if one can be obtained from other by permuting rows and columns and multiplying rows and columns by -1.

For an $n \times n$ Hadamard matrix, n is necessarily 1, 2, or a multiple of 4. And it is conjectured that Hadamard matrices exist whenever the order is a multiple of 4. But the conjecture has not yet been proved. We see there is only one equivalence class of Hadamard matrices of orders 1, 2, and 4, and there is only one class of order 8 and one class of order 12. But there are five classes of order 16, and 3 of order 20 [7]. Let H be a $4m \times 4m$ Hadamard matrix, and $N(H)$ be the matrix obtained from H by deleting the first row and column. Now, let A_H and $A_{N(H)}$ be the matrices obtained from H and $N(H)$ respectively by replacing -1 with 0. Let C_H and $C_{N(H)}$ be the binary codes generated by the rows of A_H and $A_{N(H)}$ respectively.

THEOREM 3.6. *Let H be a $4m \times 4m$ normalized Hadamard matrix, and m be an even integer. Then C_H is the extened code of $C_{N(H)}$.*

PROOF. Let E be the extened code of $C_{N(H)}$. Note that $A_{N(H)}$ is an incidence matrix of a $2-(4m-1, 2m-1, m-1)$ design with $v = b = 4m-1$. Note that the number of 1's in each row of $A_{N(H)}$ is also $m-1$ since $A_{N(H)}$ is an incidence matrix and $v = b$. Also the sum of all rows of $A_{N(H)}$ is an all one vector since $m-1$ is an odd integer. Thus all one vector of length $4m$ is in E, and the length $4m$ vector (1, each row of $A_{N(H)}$) is also in E. Note that those vectors generate E (i.e. the rows of A_H generates E), and each row of A_H is an element of E. Therefore C_H is the extened code of $C_{N(H)}$.

By Theorem 3.6, we can introduce the (7,4,3) Hamming code and its extended code using 8×8 Hadamard matrix as follows. Note that inequivalent Hadamard matrices can generate equivalent codes. The codes generated by 59 inequivalent 24×24 Hadamard matrices were investigated and there appear to be only nine inequivalent codes (two with minimum weight 9 and seven with minimum weight 6) [6].

COMPUTATION 3.7. Starting with $S_1 = (1)$, this gives S_2, S_4, $S_8, \ldots$, as follows;

$$S_{2n} = \begin{pmatrix} S_n & S_n \\ S_n & -S_n \end{pmatrix}.$$

For each n, S_{2n} is a normalized Hadamard matrix of order $2n$. For a prime number p with $p \equiv 3 \pmod 4$, consider a $p \times p$ matrix $Q = (q_{ij})$ whose rows and columns are labeled $0, 1, \cdots, p-1$, and $q_{ij} = \chi(j-i)$. Let

$$P = P_{p+1} = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q - I \end{pmatrix}.$$

Then $PP^T = P^TP = (p+1)I_{p+1}$ holds, and $P(= P_{p+1})$ is a normalized Hadamard matrix of order $p+1$. Note that S_8 and P_8 are equivalent.

Now let $A_{N(S)}$, $A_{N(P)}$ be the matrices obtained by deleting the first row and column of $S = S_8$ and $P = P_8$ respectively, and replacing -1 by 0 throughout. Also let $C_{N(S)}$, $C_{N(P)}$ be the codes generated by the rows of $A_{N(S)}$, $A_{N(P)}$, respectively. Then $C_{N(S)}$ is exactly equal to the (7,4,3) Hamming code and C_S is its extended code. Also $C_{N(P)}$ is exactly equal to the codes having $h(x) = 1 + x + x^3$ as generator polynomial.

References

1. M. Aschbacher, *On collineation Graphs of Symmetric Block Designs*, J. Combinatorial Theory **11** (1971), 272–281.
2. J. H. Conway, V. Pless, *On the Enumeration of Self-Dual Codes*, J. Combinatorial Theory **28A** (1980), 26–53.
3. T. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge-London-New York, 1986.
4. N. Ito, J. S. Leon, and Judith Q. Longyear, *Classification of 3-(24,12,5) Designs and 24-Demensional Hadamard Matrices*, J. Combinatorial Theory **31A** (1981), 66–93.
5. J. S. Leon, *An Algorithm for Computing the Automorphism Group of a Hadamar d Matrix*, J. Combinatorial Theory **27A** (1979), 289–306.
6. J. S. Leon, V. Pless, and N. J. A. Sloane, *On Ternary Self-dual Codes of Length 24*, IEEE Trans. Inform. Theory **IT-27** (1981), 176-180.
7. F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science publishing Company Inc., Now York, 1977.
8. V. Pless, N. J. A. Sloane, *On the Classification and Enumeration of Self-Dual Codes*, J. Combinatorial Theory **18A** (1975), 313–335.
9. V. Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley and Sons, Inc., New York, 1982.

10. V. D. Tonchev, *Hadamard Matrices of Order 28 with Automorphisms of Order 13*, J. Combinatorial Theory **35A** (1983), 43–57.
11. ———, *Combinatorial Configurations Design, Codes, Graphs*, Longman Scientific & Technical, Essex, 1988.
12. T. K. Yeo, *Algorithms for Code Automorphism Group Computing, Master Thesis, Seoul National University*, 1991.

Department of Mathematics Education
Seoul National University
Seoul 151-742, Korea