

Codes and groups

Rita Procesi

Dipartimento di Matematica

Università degli Studi di Roma "La Sapienza"

Piazzale Aldo Moro, 5

I-00185 Roma

Italy

Rosaria Rota

Dipartimento di Matematica

Università degli Studi di Roma Tre

Largo San Leonardo Murialdo, 1

I-00146 Roma

Italy

Abstract

In this paper codes with two control symbols, built over some classes of groups, are studied.

Keywords : Code, control symbol.

1. Introduction

In [1] some codes with control symbol are studied, in particular a code on the dihedral group D_5 is shown; this code can detect one error and one transposition of consecutive letters.

In this paper we study some code built over different classes of groups and having similar properties.

Journal of Information & Optimization Sciences

Vol. 27 (2006), No. 1, pp. 17–20

© Taru Publications

0252-2667/06 \$2.00 + 0.25

2. A code on D_{2k+1}

Our first result is about the construction of a code over a dihedral group.

Theorem. *Let G be the dihedral group D_{2k+1} , $S \subset G$ the subset of the elements of order two and:*

$$C = \{(\tau_1, \tau_2, \dots, \tau_{2n}) : \tau_i \in S, \forall i = 1, \dots, 2n, \tau_1 \circ \tau_2 \circ \dots \circ \tau_{2n} = id\};$$

then C is a code with one control symbol detecting one error and one transposition.

Proof. Since

$$G = D_{2k+1} = \langle \rho, \sigma \rangle = \{\rho^s \sigma^t : o(\rho) = 2k + 1, o(\sigma) = 2, \rho^s \sigma = \sigma \rho^{2k+1-s}\}$$

and $R = \langle \rho \rangle = \{\rho^s, s = 1, \dots, 2k + 1\}$ is a normal subgroup of G , of index two, the alphabet $S = G \setminus R$, over which C is defined, has the following properties:

1. $\forall \tau_1, \tau_2 \in S : \tau_1 \circ \tau_2 \in R$
2. $\forall \tau_1, \tau_2 \in S : \tau_1 \circ \tau_2 \neq \tau_2 \circ \tau_1$.

Generalizing [1], we can observe that this code detects one error; furthermore this code detects also a transposition.

In fact let us suppose that the word $(\tau_1, \tau_2, \dots, \tau_i, \tau_{i+1}, \dots, \tau_{2n})$ is wrongly transmitted as $(\tau_1, \tau_2, \dots, \tau_{i+1}, \tau_i, \dots, \tau_{2n})$; it is easy to check that such word does not belong to C and this because of Property 2.

Moreover this is a code with one control symbol, e.g. τ_{2n} .

3. A code over a group

We now consider the case of codes over groups with subgroups satisfying particular conditions.

Theorem. *Let G be a group, T_1, \dots, T_k k subgroups of G such that $T_i \cap T_j = \{u\}$, $\forall i \neq j$; then*

$$C = \{(a_1, a_2, \dots, a_{kn}) / a_h \in T_i - \{u\} \\ \iff h \equiv i \pmod k \wedge \prod_{t=0}^{n-1} a_{tk+i} = u, i = 1, \dots, k\},$$

is a code over the alphabet $\bigcup_{i=1}^k T_i \setminus \{u\}$, with k control symbols, one in each T_i

and reveals up to k errors of places i_1, i_2, \dots, i_k where $i_r \not\equiv i_s \pmod k$, $r \neq s$. Moreover this code detects some permutation of letters.

Proof. Without loss of generality we can prove the theorem for $k = 2$; in this case we have:

$$C = \{(a_1, a_2, \dots, a_{2n}) / a_{2h-1} \in T_1 - \{u\}, a_{2h} \in T_2 - \{u\}, h = 1, \dots, n \\ \wedge \prod_{h=1}^n a_{2h-1} = \prod_{h=1}^n a_{2h} = u\}.$$

This code has two control symbols, one in T_1 and one in T_2 and detects two errors if they occur one in an even place and the other in an odd one. Moreover this code detects a transposition as a consequence of the minimal intersection of T_1 and T_2 .

In the general case C will have k control symbols, one in each T_i moreover it will reveal up to k errors of places i_1, i_2, \dots, i_k where $i_r \not\equiv i_s \pmod k$, $r \neq s$.

Finally if the word $(a_1, a_2, \dots, a_i, \dots, a_{i+h}, \dots, a_{kn})$ is received as $(a_1, a_2, \dots, a_{\sigma(i)}, \dots, a_{\sigma(i+h)}, \dots, a_{kn})$, where $\sigma \in \mathcal{S}_h$, $h \leq k$, is a permutation over h elements, the code will detect this error.

Observation. In a group G , $|G| = p_1^{s_1} \cdot \dots \cdot p_t^{s_t}$, a family of subgroups T_i verifying the hypothesis of the previous theorem is the set of Sylow subgroups of G , S_1, \dots, S_t , where $|S_i| = p^{s_i}$.

4. A code with automorphisms

In [1] and [2] codes are considered of the following type:

$$C = \{(g_1, g_2, \dots, g_n) / g_i \in G, \pi_1(g_1) \cdot \dots \cdot \pi_n(g_n) = c\}$$

where G is a group, c a given element of G and π_1, \dots, π_n n permutations over the elements of the group G .

Theorem. If G is a group, $\sigma \in \text{Aut}(G)$ and $\sigma \neq \text{id}_G$ a non identical automorphism of G such that:

$$(*) \quad \sigma(h \cdot k) \neq k \cdot h \quad \forall h, k \in G, h \neq k^{-1},$$

then the code:

$$C = \{(g_1, g_2, \dots, g_n) / g_i \in G, \sigma^1(g_1) \cdot \dots \cdot \sigma^n(g_n) = c\}$$

detects one error and one transposition.

Proof. Following the results obtained in [1] the code C detects one error; as for the capability of detecting transpositions we can observe that, if

$$\begin{aligned} & \sigma(g_1) \cdot \sigma^2(g_2) \cdot \dots \cdot \sigma^i(g_i) \cdot \sigma^{i+1}(g_{i+1}) \cdot \dots \cdot \sigma^n(g_n) \\ &= \sigma(g_1) \cdot \sigma^2(g_2) \cdot \dots \cdot \sigma^i(g_{i+1}) \cdot \sigma^{i+1}(g_i) \cdot \dots \cdot \sigma^n(g_n) \end{aligned}$$

then it would result

$$\sigma(g_{i+1} \cdot g_i^{-1}) = g_i^{-1} \cdot g_{i+1}.$$

Thus C always reveals a transposition since the automorphism σ satisfies property (*).

Observation. For a commutative group, the previous condition becomes:

$$\sigma(g) \neq g \quad \forall g \neq u.$$

A family of commutative groups with automorphisms satisfying the previous condition exists being for example the class of cyclic groups of prime order.

References

- [1] L. Berardi and A. Beutelspacher, Fidarsi è bene controllare è meglio, *Archimede*, Vol. XLVII (1995), pp. 24–30.
- [2] R. H. Schultz, *Einführung in die Codierungstheorie*, Viewegs, 1991.

Received May, 2005