On the Nonexistence of Completely Transitive Codes

Joaquim Borges and Josep Rifà, *Member, IEEE*

***Abstract*—Completely transitive codes were introduced by P. Solé as a special case of binary linear completely regular codes.**

The existence of such codes is closely related to the existence of certain permutation groups. The nonexistence of highly transitive permutation groups allows us to prove the nonexistence of completely transitive codes with error-correcting capability greater than 4.

***Index Terms*—Completely regular codes, completely transitive codes, permutation groups.**

I. Introduction

Let F^n be the n-dimensional vector space over GF(2). The *Hamming weight* $\mathrm{wt}\,(v)$ of a vector $v \in F^n$ is the number of its nonzero coordinates. The *Hamming distance* between two vectors $v,\ u \in F^n$ is $d(v,\ u) = \mathrm{wt}\,(v + u)$.

A *binary linear code* $\mathcal{C}$ of *length* n is a linear subspace of F^n. The elements of $\mathcal{C}$ are called *codewords*. We will denote by d the *minimum distance* between any two distinct codewords. We call $\mathcal{C}$ an e-*error-correcting* code if $e \leq (d-1)/2$. A code with only one codeword is said to be *trivial*. A code with only all-one codeword and all-zero codeword is called a *repetition code*. In this correspondence we will assume that all codes are binary, linear, and nontrivial.

Given any vector $v \in F^n$, its *distance to the code* $\mathcal{C}$ is

$$d(v,\ \mathcal{C}) \min_{x \in \mathcal{C}} \{d(v,\ x)\}$$

and the *covering radius* of the code $\mathcal{C}$ is

$$\rho = \max_{v \in F^n} \{d(v,\ \mathcal{C})\}.$$

Given two sets $X,\ Y \subset F^n$, we also define the sum $X + Y$ as the set of all vectors that can be expressed as the sum of a vector in X and a vector in Y. We write $X + x$ instead of $X + \{x\}$.

A binary linear code $\mathcal{C}$ of length n is called *completely regular* if $\forall v \in F^n$ and $\forall p = 0,\ \cdots,\ n$, the number of codewords at distance p apart from v depends only on p and $d(v,\ \mathcal{C})$.

An *automorphism* of $\mathcal{C}$ is a coordinate permutation fixing $\mathcal{C}$. The set of all automorphisms of $\mathcal{C}$ is the *full automorphism group* of $\mathcal{C}$ and is denoted by $\mathrm{Aut}\,(\mathcal{C})$. $\mathrm{Aut}\,(\mathcal{C})$ acts in the following way on the quotient set $F^n/\mathcal{C}$: $\forall \alpha \in \mathrm{Aut}\,(\mathcal{C}) \alpha(\mathcal{C} + x) = \mathcal{C} + \alpha(x)$, for all $x \in F^n$.

We call $\mathcal{C}$ a *completely transitive* code if $\mathrm{Aut}\,(\mathcal{C})$ acting on $F^n/\mathcal{C}$ has exactly $\rho + 1$ orbits. Since two cosets in the same orbit have identical weight distribution, we have that a completely transitive code is always completely regular. For a more detailed proof see [10].

Let $\mathcal{C}$ be a binary linear e-error-correcting code. It has been conjectured for a long time that if $\mathcal{C}$ is a completely regular code and $|\ \mathcal{C}\ | > 2$, then $e \leq 3$. In fact, this conjecture has been also stated for nonbinary and nonlinear codes. Moreover, in [8] it is conjectured that the only completely regular code $\mathcal{C}$ with $|\ \mathcal{C}\ | > 2$ and $d \geq 8$ is the well-known extended binary Golay code. In this correspondence we do not attempt to prove this conjecture but we study the subclass of completely transitive codes, which is strictly contained in the class of completely regular codes (see [10]). Our main result is Theorem 5 which states the nonexistence of completely transitive codes with more than two codewords and error-correcting capability greater than four.

Manuscript received May 5, 1999; revised August 4, 1999. This work was supported in part by Spanish Grant no. TEL97-0663.

The authors are with the Department d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra Spain.

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)00359-X.

II. Preliminaries on Permutation Groups

Let G be a finite permutation group acting on an n-set X. We say that G has *degree* n. G is called t-*transitive* $(0 < t \leq n)$ if for any pair of ordered t-tuples of distinct elements of X $(x_1,\ \cdots,\ x_t)$ and $(y_1,\ \cdots,\ y_t)$ there exists $\alpha \in G$ such that $\alpha(x_i) = y_i$ $(1 \leq i \leq n)$. G is *transitive* if it is 1-transitive. G is called t-*homogeneous* $(0 < t \leq n)$ if for any pair of unordered t-sets of distinct elements of X $\{x_1,\ \cdots,\ x_t\}$ and $\{y_1,\ \cdots,\ y_t\}$ there exists $\alpha \in G$ such that

$$\alpha(\{x_1,\ \cdots,\ x_t\}) = \{y_1,\ \cdots,\ y_t\}.$$

Of course, if G is t-transitive, it is also $(t-1)$-transitive and t-homogeneous. We also remark that if G is t-homogeneous it is $(n-t)$-homogeneous.

The relationship between transitivity and homogeneity is very strong as we can see by means of the following result of Livingstone and Wagner [7].

Theorem 1: If G is t-homogeneous, where $2 \leq t \leq n/2$, then G is $(t-1)$-transitive, and for $t \geq 5$ even t-transitive.

Proof: See [7] or [1 , Theorem 2.19 p. 251]. □

The following result shows the nonexistence of nontrivial highly transitive groups.

Theorem 2: Let G be a finite t-transitive group of degree n.

i) If $t > 5$, then G is the symmetric or the alternating group of degree n.

ii) If $t = 5$ and G is not the symmetric or the alternating group, then G is one of the Mathieu groups M_{12} or M_{24} (of degree 12 or 24, respectively).

Proof: The reader may see [2], [3, p. 591] or [6, pp. 623–625]. □

III. The Existence of Completely Transitive Codes

The following two results may be found in [10, Propositions 7.2 and 7.3].

Proposition 3: Let $\mathcal{C}$ be a binary linear code of length n and covering radius $\rho \leq n/2$. If $\mathrm{Aut}\,(\mathcal{C})$ is ρ-homogeneous, then $\mathcal{C}$ is completely transitive.

Proposition 4: If an e-error-correcting code $\mathcal{C}$ is a completely transitive code, then $Aut(\mathcal{C})$ is e-homogeneous on the coordinate positions.

The last proposition enables us to show that there is no completely transitive code with high error-correcting capability.

Theorem 5: If $\mathcal{C} \subset F^n$ is an e-error-correcting completely transitive nontrivial code, then $e \leq 4$ or $\mathcal{C}$ is a repetition code.

Proof: Assume that $\mathcal{C}$ is not trivial. $\mathrm{Aut}\,(\mathcal{C})$ must be e-homogeneous by Proposition 4. We have $|\mathcal{C}| > 1$, then $d \leq n$ and $e \leq n/2$. Thus if $e \geq 5$, $\mathcal{C}$ must also be e-transitive by Theorem 1.

i) If $e > 5$, then by Theorem 2, $\mathrm{Aut}\,(\mathcal{C})$ is the symmetric or the alternating group of degree n. Suppose that $\mathcal{C}$ has a codeword $x = (x_1,\ \cdots,\ x_n)$ which is neither the all-zero vector nor the all-one vector. Then, let $i,\ j$ and k be distinct indices such that $x_j \neq x_k$ $(i,\ j,\ k \in \{1,\ \cdots,\ n\})$. The permutation cycle $\pi = (i,\ j,\ k)$ is in the alternating and symmetric group, so

0018–9448/00$10.00 © 2000 IEEE

$d(x, \pi(x)) = 2$ and this is a contradiction with the assumption $e > 5$. We conclude that $\mathcal{C}$ is the repetition code of length n.

ii) Suppose that $e = 5$ and $\mathrm{Aut}(\mathcal{C})$ is not the symmetric or the alternating group of degree n. Then by Theorem 2, $\mathrm{Aut}(\mathcal{C})$ is either M_{12} or M_{24}. If $\mathrm{Aut}(\mathcal{C}) = M_{12}$, then $\mathcal{C}$ should be a nontrivial linear code of length 12 and minimum distance $d \geq 11$. Clearly, the only possibility is the repetition code. Assume that $\mathrm{Aut}(\mathcal{C}) = M_{24}$. Since $\mathcal{C}$ is a nontrivial completely regular code, then the minimum-weight codewords form an e-(n, d, λ) -design on the set of coordinates (see [12]), or $\mathcal{C}$ is a repetition code. In any e-(n, d, λ)-design with $e \geq 4$ and $n \geq d + 2$, the number of blocks is $b \geq n(n-1)/2$ (this bound is given in [9]). Hence, we have at least $24 \cdot 23/2 = 276$ codewords and $\mathcal{C}$ has dimension $k > 8$. But the sphere packing bound says that

$$2^k \leq \frac{2^{24}}{\sum_{i=0}^{5} \binom{24}{i}} \Longrightarrow 2^k \leq 302$$

hence $k < 9$, which contradicts the previous result. Thus $\mathcal{C}$ must be a repetition code. □

Applying Proposition 3, it is easy to see that perfect and extended perfect Hamming codes are completely transitive with $e = 1$. Also, the perfect and the extended perfect binary Golay codes are completely transitive with $e = 3$. These examples, and some other ones, are also mentioned in [10]. For the case $e = 2$, we can consider the truncated binary Golay code C (deleting any fixed coordinate form each codeword of the binary Golay code). Clearly, C has length 22, $e = 2$ and is invariant under the Mathieu group M_{22}, which is 3-transitive; therefore, C is a completely transitive code by Proposition 3. This last example comes from [4].

Hence, for $e = 1, 2$, or 3, there exist completely transitive codes. As we have mentioned above, for $e > 3$ it has been conjectured that there is no completely regular code containing more than two codewords, and hence there is no completely transitive code, with the exception of the trivial or the repetition codes. This has been proved for the case $e = \rho$ (*perfect* codes) by Tietäväinen in 1973 (see [11]), and also for the case $e + 1 = \rho$ (*uniformly packed* codes) by Van Tilborg in 1976 (see [5]). For $\rho > e + 1$ there is no proof of the conjecture.

We have shown the nonexistence of completely transitive codes for $e > 4$ with more than two codewords. However, the existence of such codes for $e = 4$ remains an open question .

Acknowledgment

The authors wish to thank P. Solé for his comments that were the starting point for the proof of the case $e = 5$ of Theorem 5. The authors also wish to thank M. Giudici and C. Praeger for helpful comments during the preparation of this correspondence and the anonymous referees who enlightened us about the example of the truncated Golay code.

References

[1] T. Beth, D. Junickel, and H. Lenz, *Design Theory*. Manheim, Germany: Wiessenschaftverlag, 1985.

[2] P. J. Cameron, "Finite permutation groups and finite simple groups," *Bull. London Math. Soc.*, vol. 13, pp. 1–22, 1981.

[3] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC Press, 1996.

[4] M. Giudici, "Completely transitive codes in Hamming graphs," Master thesis, Univ. Western Australia, 1998.

[5] J. M. Goethals and H. C. A. Van Tilborg, "Uniformly packed codes," *Philips Res.*, vol. 30, pp. 9–36, 1975.

[6] R. L. Graham, M. Grötschel, and L. Lovász, *Handbook of Combinatorics*. Amsterdam, The Netherlands: Elsevier Science B. V., 1995.

[7] D. Livingston and A. Wagner, "Transitivity of finite permutation groups on unordered sets," *Math. Z.*, vol. 90, pp. 393–403, 1965.

[8] A. Neumaier, "Completely regular codes," *Discr. Math.*, vol. 106/107, pp. 335–360, 1992.

[9] D. K. Ray-Chaudhuri and R. M. Wilson, "On t-designs," *Osaka J. Math.*, vol. 12, pp. 737–744, 1975.

[10] P. Solé, "Completely regular codes and completely transitive codes," *Discr. Math.*, vol. 81, pp. 193–201, 1990.

[11] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[12] H. C. A. Van Tilborg, "Uniformly packed codes," Ph.D. dissertation, Eindhoven Univ. Technol., Eindhoven, The Netherlands, 1976.

Elementary 2-Group Character Codes

Cunsheng Ding, *Member, IEEE*, David Kohel, *Member, IEEE*, and San Ling

***Abstract*—In this correspondence we describe a class of codes over GF (q), where q is a power of an odd prime. These codes are analogs of the binary Reed–Muller codes and share several features in common with them. We determine the minimum weight and properties of these codes. For a subclass of codes we find the weight distribution and prove that the minimum nonzero weight codewords give 1-designs.**

***Index Terms*—Group character codes, linear codes, Reed–Muller codes.**

I. Introduction

In this correspondence we describe a class of group character codes $C_q(r, n)$, defined over GF (q), with parameters $[2^n, s_n(r), 2^{n-r}]$, where q is a power of an odd prime and

$$s_n(k) = \sum_{i=0}^{k} \binom{n}{i}.$$

The codes $C_q(r, n)$ are defined in analogy with the binary Reed–Muller codes and have the same parameters [2]. Moreover, as for Reed–Muller codes, $C_q(r, n)$ is generated by minimum-weight codewords, and the dual of $C_q(r, n)$ is equivalent to $C_q(n-r-1, n)$, which is the analog of the equality $R(r, n)^{\perp} = R(n-r-1, n)$.

The purpose of this correspondence is to describe this class of codes, to determine the dimensions and minimum distances, to characterize

Manuscript received February 10, 1999; revised June 12, 1999. The work of C. Ding and S. Ling was supported in part under Grant RP 960668/M.

C. Ding is with the Department of Computer Science, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 (e-mail: dingcs@comp.nus.edu.sg).

D. Kohel was with the Department of Mathematics, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 . He is now with the School of Mathematics and Statistics, Carslaw Building, F07, University of Sydney, Sydney, NSW 2006, Australia (e-mail: kohel@maths.usvd.edu.au).

S. Ling is with the Department of Mathematics, National University of Singapore, Lower Kent Ridge Road, Singapore 119260 (e-mail: matlings@math.nus.edu.sg).

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)00075-4.

0018–9448/00$10.00 © 2000 IEEE