Completely regular codes and completely transitive codes

P. Sole

INRIA

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP105
78153 Le Chesnay Cedex
France
Tél. (1) 39 63 55 11

Rapports de Recherche

N° 727

COMPLETELY REGULAR CODES AND COMPLETELY TRANSITIVE CODES

Patrick SOLE

OCTOBRE 1987

Completely Regular Codes and Completely Transitive Codes

Patrick SOLE

INRIA, Domaine de Voluceau 78 153 Le Chesnay , France. (*)

ABSTRACT

A binary code C is said to be completely regular if the weight distribution of any translate x+C only depends on the distance of x to C.

Such codes are related to designs and distance regular graphs. Their covering radius is equal to their external distance. All perfect and uniformly packed codes are known to be completely regular.

We construct new examples of a different kind, including the non linear extended Preparata and Goethals codes. Three constructions are given: direct sum , extension, and action of the automorphism group of the code.

We introduce the class of completely transitive codes which seems to be strictly contained in the class of completely regular codes. A sufficient condition for complete transitivity is given.

Codes complètement réguliers et Codes complètement transitifs

RESUME

Un code binaire C est dit complèment régulier si la distribution des poids de tout translaté x+C dépend seulement de la distance de x à C.

De tels codes sont reliés aux designs et aux graphes distances réguliers. Leur rayon de recouvrement est égal à leur distance externe. On sait que tous les codes parfaits et uniformément empilés sont complètement réguliers.

Nous construisons de nombreux exemples d'un genre différent, comprenant les codes non linéaires de Goethals et de Preparata. On donne trois constructions : par somme directe, extension, et action du groupe d'automorphisme du code.

Nous introduisons la classe des codes complètement transitifs qui semble être strictement incluse dans la classe des codes complètement réguliers. On donne une condition suffisante pour qu'un code soit complètement régulier.

(*) ce travail a été effectué lorsque l'auteur était stagiaire de recherche à l'INRIA Rocquencourt.

1 Introduction

Completely regular codes in Hamming metric, were introduced by Delsarte [10], and by the author in the Lee metric [17].

In particular they are distance invariant [10], and in some cases [10],[11] give rise to designs. In the linear case, the set of the cosets can be endowed with a P-polynomial association scheme structure, whose dual is a scheme on the words of the dual code [10], called the distance scheme [3]. In the unrestricted case one only obtains a s' partition design [7].

Known examples were perfect and uniformly packed codes [10], and dual codes of some three weight codes [3].

We construct new examples of a different kind. Direct sums of single error correcting perfect codes give rise to completely regular codes with s'-e arbitrarily large. In many cases adjonction of a parity check symbol yields new examples, even in the non linear case. We introduce the new class of completely transitive codes which is contained in the class of completely regular codes and allows no to recover many classical examples by simple symmetry arguments. A sufficent condition for complete transitivity in terms of homogeneity of the automorphism group of the code is given. A partial converse is given with applications to a class of codes introduced in [6].

The existence of completely regular codes that would not be completely transitive is considered.

2.Some fundamental parameters of a code :

We denote by d(x,y) the Hamming distance between words x,y of F_2^n.

We denote by C an unrestricted binary code of length n, and minimal distance δ, error correcting capacity e (e=[δ–1/2]) and covering radius r :

$$r = \max_{x \notin C} d(x,C)$$

We call outer distribution matrix of C, the matrix B, of size 2^n by n+1 with entries :

$$B_{x,i} = \{c \in C / d(x,c)=i\}$$

which means that the row B_x is the weight distribution of the translate C+x.

The number of distinct rows of B is noted b+1. We denote by 1+s the number of nonzero terms in the distance distribution of C, $\{a_i(C)/i:0,1,...,n\}$, and 1+s' the number of non zero terms in the dual distance distribution $\{a'_i(C)/i:0,1,...,n\}$ of C, obtained from the former by Mac Williams transform. s' is called the external distance of C, and is equal to the number of nonzero weights of C if C is linear.

The automorphism group Aut(C) of C in the largest group of nxn permutation matrices which fixes C.

Aut(C) is said to be t-transitive (resp. t-homogeneous) if it sends any t-uple (resp any t-set) on any t-uple (resp. t-set). We denote by GL(m,q) the group of m.m invertible matrices over the finite field with q elements F_q.

3.Relations between the parameters :

We admit the technical [9] :

lemma 3.1 : rank B = s'+1

It seems that the next easy result has not been previously stated.

Theorem 3.1 : $b \geq s'$

Proof : Obvious since the number of distinct rows of B upper bounds the rank of B. Q.E.D.

Now we give a new proof of a celebrated result [9].

Theorem 3.2 : (Delsarte) $r \leq s'$

Proof : By definition of r, it exists x_r such that $d(x_r,C) = r$. Then, using the fact that the Hamming distance is graphic [2] we see that it exists x_{r-1} such that both $d(x_{r-1},C)=r-1$ and $d(x_{r-1},x_r)=1$ hold.

Using repeatedly the same argument shows the existence of r+1 x_i such that $d(x_i,C)=i$ for i=0,1,...,r.

Then the first nonzero term in B_{xi} is $B_{xi,r}$. This shows that the rows (B_{xi}) are linearly independent. Consequently $1+r \leq$ rank (B). Q.E.D.

Remark 3.1 : The two preceding inequalities imply $r \leq b$ which is clear from the definitions.

Remark 3.2 : Using $e \leq r$ yields the MacWilliams, inequality : $s' \geq e$. [9] [10]. Then, if s'=e r=e and the code is perfect.

Remark 3.3 : We shall admit the following characterizations e is perfect if and only if s'=e [9].
C is uniformly packed if and only if s'=e+1. [11].

4.Completely regular codes :

A code C is said to be λ -regular [11] if B_x only depends on d(x,c) for $d(x,c) \leq \lambda$ and completely regular if r-regular [10]. Clearly, C is completely regular if and only if r=b.

Theorem 4.1 : if C is completely regular then r=s'.

Proof : C is completely regular if and only if r=b. Since we have the inequalities of theorems 3.2 and 3.1: $r \leq s' \leq b$ the result follows. Q.E.D.

Remark 4.1 : The converse is false. Delsarte gives the example of the [48,24,12] extended quadratic residue code which has r=8 and b=14. [9].

The following sufficient condition implies that all perfect and uniformly packed codes are completely regular in view of remark 3.3. The aim of sections 5 and 6 is to construct completely regular codes of a different kind.

Theorem 4.3 : If $\delta \geq 2s'-1$, then C is completely regular.[10]

We shall neeed the following result [10] in section 6:

Theorem 4.2 : Then all rous B(x) of B corresponding to a fixed value of d(x,C) are identical if $d(x,C) \leq \delta - s'$ or $d(x,C) = s'$.

5.Direct sum construction:

Let C be a single error correcting perfect code [n,M,3], not necessarily linear, but containing the all zero word.

We recall that the direct sum $C_1 + C_2$ of two codes of length n is the code of length 2n defined by :

$$C_1 + C_2 = \{(c_1/c_2)/c_1 \in C_1 \text{ and } c_2 \in C_2\}$$

Now we can consider the code $C^{(p)}$ recursively defined by :

$$C^{(2)} = C + C$$
$$C^{(p+1)} = C^{(p)} + C$$

Clearly $C^{(p)}$ is a code of parameters $[np, M^p, 3]$

Theorem 5.1 : The covering radius of $C^{(p)}$ is p.

Proof : Write an arbitrary x in $F_2{}^{pn}$ as $(x_1 / x_2 / \ldots / x_p)$ then $d(x,C^{(p)}) = \sum_{i=1}^{p} d(x_i,C) \leq p$

since the covering radius of C is one. This bound is attained by taking each x_i at distance one of C. Q.E.D.

Now from the preceding construction we see that the weight distribution of $x+C^{(p)}$ only depends on the weight distribution of the translates x_i+C, which only depend on $d(x_i,C)$. Consequently $b(C^{(p)})=p$, and $C^{(p)}$ is completely regular with $s'=p$.

For $p=2$ we obtain an uniformly packed code, which seems to be new.

For $p\geq 3$ $C^{(p)}$ is such that $s'=p-1+e\geq e+2$ and $C^{(p)}$ is neither perfect nor uniformly packed.

VI.Extension construction :

Let C be a completely regular code of length n and C_e obtained from C by adding a parity check symbol :

$$C = \{(c/ \sum_{i=1}^{n} c_i) / c\in C\}$$

Moreover, we assume that, by deleting any coordinate of C_e we obtain C.

Proposition 6 : If $s'(C_e) \leq s'(C) + 1$ then C_e is completely regular.

Proof : By construction $r(C_e) = r(C)$ or $r(C_e) = r(C)+1$. For any x_e in F_2^{n+1} such that $d(x_e, C_e) \leq r(C)$ it exists an x in F^n_2 such that $x_e + C_e$ is obtained from x+C by adding a suitable parity check symbol and such that $d(x_e, C_e)=d(x,C)$.

Since C is completely regular, the weight distribution of x+C only depends on d(x,C).

The weight of a codeword of $x_e + C_e$ only depends on the parity of the weight of its projection in x+C. (This would not hold in F^n_q, $q\geq 3$).

If $r(C_e) = r(C)$ we are done.

If not, then $r(C_e) \leq s'(C_e) = s'(C)+1 = r(C)+1$ implies that $r(C_e) = s'(C_e)$. We can apply theorem 4-2 to show that all $x_e + C_e$ with $d(x_e, C_e)=r(C_e)$ share the same weight distribution. Q.E.D.

Corollary 6.1 : If C is linear completely regular the weights of its orthogonal dual C^o are even and symmetrical with respect to (1+n)/2, and it Aut (C_e) is 1-transitive then C is completely regular.

Proof : Since $Aut(C_e)$ is 1-transitive, by deleting one coordinate we always obtain the same code C.

The condition on the weights of C^o implies that :

$$s'(C_e) = s'(C)+1$$

since we have :

$$(C_e)^o = (C^o)_e + \mathbf{1}$$

Where **1** is the all-one vector and where D+**1** denotes the code obtained from the linear code D by adding the row **1** to its generator matrix. Q.E.D.

Example 6.1 : Let C be a double error correcting BCH code with parameters $[2^m-1, 2^m-1-2m,5]$ m odd, m≥3. It is known that C^o has exactly three nonzero weights namely $2^{m-1}+2^{(m-1)/2}$, $2^{m-1}-2^{(m-1)/2}$ and 2^{m-1} [16] and that C is uniformly packed. Moreover C_e is left invariant by the affine group. C_e is completely regular with parameters: s'=4 and e=2.

Example 6.2 : Let C be the dual of a three weight cyclic code of lenght $n=2^m-1$ studied by Calderbanks and Goethals [3], [4]. C is completely regular as is explicitly stated in [4 section 2]. Since C_e is left invariant by the affine group [4], and that the three weights of C^o, namely $2^{m-1}-2^{m-1-r}$, 2^{m-1}, $2^{m-1}+2^{m-1-r}$ (in the notation of [4]) are symmetrical with respect to $n+1/2 = 2^{m-1}$, we can apply corollary 6.1 to obtain a completely regular code with r=s'=4,and e=1.

In corollary 6.1, we can drop the hypothesis in view of theorem 30 of [16, chapter 14] :

Lemma 6.1 : If C has even dual distances and that, by deleting any coordinate of C_e we still get C then we have :

$$a'_i(C) = a'_i(C) + a'_{n-i}(C)$$

Consequently, we can state :

Corollary 6.2 Let C be an unrestricted binary code whose dual distances are even and symmetrical with respect to (1+n)/2. Assume that $Aut(C_e)$ is 1-transitive. If C is completely regular, so is C_e.

Proof : Using lemma 6.1 we readily obtain $s'(C_e)=s'(C)+1$. The checking of the other conditions goes as in Corollary 6.1. Q.E.D.

Example 6.3 : We let $C_e = \bar{P}(m)$, extended Preparata code of length 2^m, m even, and m≥4.. From the presentation of [1], we see that $Aut(C_e)$ is 1-transitive, and that C_e is obtained from C, the shortened Preparata code of length 2^m-1 by adding a parity check digit.

Moreover, it is known [16] that C is uniformly packed and even nearly perfect, hence completely regular, and that its dual distances are :

$2^{m-1}-2^{(m-2)/2}, 2^{m-1}, 2^{m-1}+2^{(m-2)/2}$.

We conclude that C is completely regular, non linear and non uniformly packed since $s'(C_e)=4=e(C_e)+2$.

This result was independently obtained by B. Courteau and A. Monpetit [8].

Example 6.4: Let C_e be the (12,24,6) Hadamard code, and C the punctured (11,24,5) [18]. It is known, that C is uniformly packed with dual distances 4,6,8.[7] . Aut(C_e) is isomorphic to the Matthieu group M_{12}, and is 2-transitive [14]. C_e is completely regular with s'=4 and e=2.

7.Completely transitive codes :

Let C be a linear binary code. Then Aut(C) acts in a natural way on the cosets of C :$\forall\ \phi \in$ Aut(C),$\phi(x+C) = \phi(x)+C$. we denote by a+1 the number of orbits of Aut(C) on F^n_2/C. We say that C is completely transitive if r=a. Then we have the easy :

Proposition 7.1 : If C is completely transitive then C is completely regular.

Proof : As already noticed in Remark 3.1 $r \leq b$
Two cosets in the some orbit have the same weight distribution. This yields : $b \leq a$. Consequently, if r=a then r=b.

Q.E.D.

Corollary 7.1 : If C is completely transitive, then a = s'.

Proof : By theorem 4.1, and proposition 7.1 we have r=s'. By definition of complete transitivity we have r=a. Q.E.D.

A sufficient conditon for complete transitivity is

Proposition 7.3 : Let C be a linear binary code of covering radius $r \leq n/2$. If Aut (C) is r-homogeneous then C is completely transitive.

Proof : If Aut (C) is r-homogeneous with $r \leq n/2$, then it is also i-homogeneous ($i \leq r$). This is a deep result of Livingstone and Wagner [15].

The fact that Aut (C) is i-homogeneous implies that all coset leaders of weight i are equivalent, and, consequently, so are the associated cosets. This shows that $a \leq r$. But $r \leq a$ aiways holds. We conclude that r=a. Q.E.D.

Exemple : The perfect Hamming codes [$2^{m-1}, 2^m-1, 3$] are cyclic with r=1. The uniformly packed extended Hamming codes [$2^m, 2^m-m, 4$] are left invariant by the affine group [16] with r=2

Example : The Golay codes [23,12,7] (perfect) and [24,12,8] (uniformly packed) are left invariant by the Matthieu groups M_{23} and M_{24} respectively 3 and 4 times transitive, and have covering radius 3 and 4.

Proposition 7.3 admits a partial converse :

Proposition 7.4 : If C is completely transitive then Aut(C) is e-homogeneous.

Proof : It is well known that cosets of weight i, $i \leq e$, admit a unique coset leader. If two such cosets are equivalent, so are their leaders. Q.E.D.

This is the best possible result as the next example shows

Example : Let C be the [9,5,3] binary code dual of the Kronecker product of two [3,2,2] parity check codes [13]. Then C in uniformly packed since r=s'=2 and e=1. Words of C are best thought of as matrices, and Aut(C) is generated by row and column permutations, and symmetry with respect to the main diagonal. This group is 1-transitive but not two-homogeneous, since two entries of a 3 by 3 matrix cannot be transformed by action of Aut(C) into two entries on the same horizontal line. Fortunately the latter configurations belong to cosets of weight one. The former generate all cosets of weight two, and are equivalent under permutations or rows and columns.

This is an example where C is completely transitive but where Aut (C) is not r-homogeneous.

Now a natural question [5] is :

Question 7.1 : Are there completely regular linear codes that are not completely transitive ?

If we assume that the full automorphism group of the code C of example 6.2 is GL(m,2) as for the shortened the Reed Muller codes [16], then we can give a negative answer by use of

Lemma 7.1 : For any binary linear code C, the number of orbits of Aut(C) on the words of C is a.

Proof : see [17] and also theorem 6.3 of [2]. Q.E.D.

For this, we show that for this particular code C we cannot have a=s', contradicting corollary 7.1. For in C there are two sorts of words of weight 2^{m-1} : words in shortened RM(m,1) [16], and words corresponding to symplectic forms of rank ≥ 1 [12], which cannot be equivalent under GL(m,2), since linear transforms preserve the rank. So, $a \geq s'+1$.

Remark 7.1 : We can use the argument of proposition 7.4 together withlemma 7.1 to show that some codes are not e-error correcting with e>1.

If we consider the code C, such that C^0 is a tri-weight code of length 168 dimension 9 constructed by Camion [6], we see that it is at most single error correcting. For there are three nontrivial orbits on the words of C^0, hence three orbits onthe cosets of C under GL(3,2) acting on itself by left and right multiplication.

Clearly this action is not 2-transitive since the action of a one point stabiliser is simply conjugation in the group GL (3,2), which yields three orbits, one for each possible rank of the matrices of GL(3,2).

Remark 7.2 : If we could prove that r(C)=3 then the code of remark 7.1 would be completely transitive. More generally, if the code C^o constructed in [6 ,section 1] had m^2 non zero weights, and if C had covering radius m^2, then C would be completely transitive hence completely regular with $s' \geq e+2$ for $m \geq 3$.

References :

[1] R.D BAKER, JH VAN LINT, RM WILSON "On the Preparata and Goethals codes" IEEE IT 29 p.342-348 (1983)
[2] E. BANNAI and T. ITO "Algebraic combinatorics I Benjamin Cummings 1984.
[3]A;.R CALDERBANKS and JM GOETHALS"On a pair of dual subschemes of H(n,q)" Europ J. of Comb. (1985) 6, pp 133-147.
[4] A.R. CALDERBANKS and J.M. GOETHALS "Three weight codes and association schemes "Philips J. Res. 39 (1984) p. 143-152.
[5] P.CAMION,private communication.
[6] P.CAMION Codes with given automorphism groups
[7] P.CAMION,B.COURTEAU, P.DELSARTE "On r-partition designs in Hamming spaces"INRIA research report 626, February 1987
[8] B. COURTEAU and A. MONPETIT "On dual distances of completely regular codes "submitted to Discrete Math.
[9] P. DELSARTE "Four fundamental parameters of a code, and their combinatorial significance. Info and Control 23 (1973) p. 407-438.
[10]P. DELSARTE "An algebraic approach to the association shcemes of coding theory" Philips Research Reports Supplements 10 (1973).
[11]J.M. GOETHALS and H.C.A. VAN TILBORG "Uniformly packed codes" Philips Research 30 (1975), 9-36.
[12] J .M GOETHALS "Nonlinear codes defined by quadratic forms over GF(2)" Info &
Control,31 p43-74 (1976)
[13]R.L. GRAHAM and N.J.A SLOANE "On the covering radius of codes "IEEE IT 31 (1985) p.385-401
[14]W. KANTOR "Automorphisms groups of Hadamard matrices" J. Comb Theory, 6 (1969) p. 279-281.
[15] D. LIVINGSTONE, A. WAGNER "Transitivity of finite permutation groups on unordered sets" Math Z.90 (1965) p. 393-403.
[16]F.J. MAC WILLIAMS and N.J.A SLOANE "The theory of error correcting codes" North Holland.
[17] W.W. PETERSON and E.J. WELDON "Error correcting codes" MIT Press (1972).
[18] P. SOLE "On parameters of codes for the Lee and modular distance" submitted to IEEE Info Theory
[19]J.H. VAN LINT "Introduction to coding theory" 1982 Springer Verlag.

Imprimé en France

par

l'Institut National de Recherche en Informatique et en Automatique