COMPLETELY REGULAR CODES AND COMPLETELY TRANSITIVE CODES

Patrick SOLÉ*
School of Computer and Information Science, 313 Link Hall, Syracuse University, Syracuse, NY 13244-1240, USA

Received 6 August 1987
Revised 22 February 1988

A binary code C is said to be completely regular if the weight distribution of any translate \( x + C \) depends only 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 nonlinear 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.

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 obtains only an \( s' \)-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 adjunction of a parity check symbol yields new examples, even in the nonlinear case. We introduce the new class of completely transitive codes which is contained in the class of completely regular codes and allows us to recover many classical examples by simple symmetry arguments. A sufficient 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].

* Supported by a grant from INRIA, France.

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 $F^n$.

We denote by $C$ an unrestricted binary code of length $n$, and minimal distance $\delta$, error correcting capacity $e(e = \lceil \delta - 1/2 \rceil)$ and covering radius $r$:

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

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

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

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 $C$, $\{a_i(C)/i:0, 1, \ldots, n\}$ of $C$, and $1 + s'$ the number of nonzero terms in the dual distance distribution $\{a'_i(C)/i:0, 1, \ldots, n\}$ of $C$, obtained from the former by MacWilliams' transform. The parameter $s'$ 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 $\text{Aut}(C)$ of $C$ is the largest group of $n \times n$ permutation matrices which fixes $C$.

$\text{Aut}(C)$ is said to be $t$-transitive (resp. $t$-homogeneous) if it sends any $t$-tuple (resp. any $t$-set) on any tuple (resp. $t$-set). We denote by $\text{GL}(m, q)$ the group of $m \times m$ invertible matrices over the finite field with $q$ elements $F_q$, and by $R(r, m)$ the $r$th order Reed Muller code of length $2^n$.

3. Relations between the parameters

We admit the technical [9]:

**Lemma 3.1.** $\text{rank } B = s' + 1$.

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 $B$. $\square$

Now we give a new proof of a celebrated result [9].
Theorem 3.2 (Delsarte). \( r \leq s' \).

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

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

Then the first nonzero term in \( B_{s'} \) is \( B_{s'} \). This shows that the rows \( (B_{s'}) \) are linearly independent. Consequently, \( 1 + r = \text{rank}(B) \). \( \Box \)

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 \( s' = e \) we have \( r = e \) and the code is perfect.

Remark 3.3. We shall admit the following characterizations: \( C \) 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 \( \lambda \)-regular [11] if \( B_s \) depends only 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 Theorem 3.2 and 3.1, \( r \leq s' \leq b \), the result follows. \( \Box \)

Remark 4.1. The converse is false. Delsarte gives the example of the [48, 24, 12] extended quadratic residue code which has \( r = s' = 8 \) 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 4.2. If \( \delta \geq 2s' - 1 \), then \( C \) is completely regular [10].

We shall need the following result [10] in Section 6:

Theorem 4.3. All rows \( B(x) \) of \( B \) corresponding to a fixed value of \( d(x, C) \) are identical if \( d(x, C) = \delta - s' \) 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 \( F_2^n \) as \( (x_1/x_2 \cdots /x_p) \) then

\[
d(x, C^{(p)}) = \sum_{i=1}^{p} (x_i, C) \leq p
\]

since the covering radius of \( C \) is one. This bound is attained by taking each \( x_i \) at distance one of \( C \). \( \Box \)

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

For \( p = 2 \) we obtain a 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.

6. Extension construction

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

\[
C = \left\{ \left( c / \sum_{i=1}^{n} c_i \right) : c \in C \right\}.
\]

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

Proposition 6.1. 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 \( d(x_e, C_e) \leq r(C) \) there exists an \( x \) in \( F_2^n \) such that \( x + C_e \) is obtained from \( x + C \) by adding a suitable parity check symbol and such that \( d(x, C_e) = d(x, C) \).

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

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

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

If not, then \( r(C_e) < s'(C_e) = s'(C) + 1 = r(C) + 1 \) 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. \( \square \)

**Corollary 6.1.** If \( C \) is linearly completely regular the weights of its orthogonal dual \( C^\perp \) are even and symmetrical with respect to \( (1 + n)/2 \), and if \( \text{Aut}(C_e) \) is 1-transitive, then \( C \) is completely regular.

**Proof.** Since \( \text{Aut}(C_e) \) is 1-transitive, by deleting one coordinate we always obtain the same code \( C \).

The condition on the weights of \( C^\perp \) implies that:

\[ s(C_e) = s'(C) + 1, \]

since we have:

\[ (C_e)^\perp = (C^\perp)_e + 1, \]

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. \( \square \)

**Example 6.1.** Let \( C \) be a double error correcting BCH code with parameters \([2^m - 1, 2^m - 1 - 2m, 5] \) \( m \) odd, \( m \geq 3 \). It is known that \( C^\perp \) 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 length \( n = 2^m - 1 \) studied by Calderbank 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 the three weights of \( C^\perp \), namely \( 2^{m-1} - 2^{m-1-1}, 2^{m-1}, 2^{m-1} + 2^{m-1-1} \) (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 linearity hypothesis in view of Theorem 30 of [16, Chapter 14]:

**Lemma 6.1.** If \( C \) has even dual distances and by deleting any coordinate of \( C_e \), we
still get $C$, then we have:

$$a'_i(C) = a'_i(C) + a'_{i-1}(C).$$

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 $\text{Aut}(C_e)$ 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. □

**Example 6.3.** We let $C_e = P(m)$, extended Preparata code of length $2^m$, $m$ even, and $m \geq 4$. From the presentation of [1] we see that $\text{Aut}(C_e)$ 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:

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

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

This result was independently obtained by Courteau and 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]. $\text{Aut}(C_e)$ is isomorphic to the Mathieu 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 $\text{Aut}(C)$ acts in a natural way on the cosets of $C$:

$$\forall \phi \in \text{Aut}(C), \quad \phi(x + C) = \phi(x) + C.$$  

We denote by $a + 1$ the number of orbits of $\text{Aut}(C)$ on $F_2^n / C$. 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, $r = b$. Two cosets in the same orbit have the same weight distribution. This yields $b < a$. Consequently, if $r - a$, then $r = b$. □
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 \( r = a \). \( \square \)

A sufficient condition for complete transitivity is:

Proposition 7.2. Let C be a linear binary code of covering radius \( r \leq n/2 \). If \( \text{Aut}(C) \) is \( r \)-homogeneous then C is completely transitive.

Proof. If \( \text{Aut}(C) \) 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 \( \text{Aut}(C) \) 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 \( r \leq a \) always holds. We conclude that \( r = a \). \( \square \)

Example. The perfect Hamming codes are cyclic with \( r = 1 \). The uniformly packed extended Hamming codes are left invariant by the affine group [16] with \( r = 2 \).

Example. The G\o{}l\o{}y codes \([23, 12, 7]\) (perfect) and \([24, 12, 8]\) (uniformly packed) are left invariant by the Mathieu groups \( M_{23} \) and \( M_{24} \), respectively 3 and 4 times transitive, and have covering radius 3 and 4.

Proposition 7.2 admits a partial converse:

Proposition 7.3. If C is completely transitive, then \( \text{Aut}(C) \) 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. \( \square \)

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 is uniformly packed since \( r = s' = 2 \) and \( e = 1 \). Words of C are best thought of as matrices, and \( \text{Aut}(C) \) is generated by row and column permutations, and symmetry with respect to the main diagonal. This group is 1-transitive but not 2-homogeneous, since two entries of a 3 by 3 matrix not on the same line cannot be transformed by action of \( \text{Aut}(C) \) 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 \( \text{Aut}(C) \) 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 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].

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$(1, m)$ [16], and words corresponding to symplectic forms of rank $\geq 1$ [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 with Lemma 7.1 to show that some codes are not $e$-error correcting with $e > 1$.

If we consider the code $C$, such that $C^+$ is a tri-weight code of length $168$, dimension 9, constructed by Camion [6], we see that it is, at most, single error correcting. There are three nontrivial orbits on the words of $C^+$, hence three orbits on the 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 stabilizer 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 $C^+$ constructed in [6, Section 1] had $m^2$ nonzero weights, and if $C$ had covering radius $m^2$, then $C$ would be completely transitive, hence completely regular with $s' \geq e + 2$ for $m \geq 3$.

**Acknowledgement**

We thank the referee for helpful comments and Ms. Elaine Weinman for careful TeXing.
References