On completely regular and completely transitive codes derived from Hamming codes

J. Borges, J. Rifà and V. A. Zinoviev

March 7, 2019

JOAQUIM BORGES
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona

JOSEP RIFÀ
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona

VICTOR ZINOVIEV
A.A. Kharkevich Institute for Problems of Information Transmission
Russian Academy of Sciences

Abstract

Given a parity-check matrix $H_m$ of a $q$-ary Hamming code, we consider a partition of the columns into two subsets. Then, we consider the two codes that have these submatrices as parity-check matrices. We say that anyone of these two codes is the supplementary code of the other one.

We obtain that if one of these codes is a Hamming code, then the supplementary code is completely regular and completely transitive.
If one of the codes is completely regular with covering radius 2, then the supplementary code is also completely regular with covering radius at most 2. Moreover, in this case, either both codes are completely transitive, or both are not.

With this technique, we obtain infinite families of completely regular and completely transitive codes which are quasi-perfect uniformly packed.

1 Introduction

Let \( \mathbb{F}_q \) be the finite field of order \( q \). The weight of a vector \( \mathbf{v} \in \mathbb{F}_q^n \), denoted by \( \text{wt}(\mathbf{v}) \), is the number of nonzero coordinates of \( \mathbf{v} \). The vector of weight 0, or zero vector, is denoted by \( \mathbf{0} \). The distance between two vectors \( \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n \), denoted by \( d(\mathbf{v}, \mathbf{w}) \), is the number of coordinates in which they differ. A subset \( C \subseteq \mathbb{F}_q^n \) is called a \( q \)-ary code of length \( n \). Denote by \( d \) the minimum distance among codewords in \( C \). The packing radius of \( C \) is \( e = \lfloor (d - 1)/2 \rfloor \) and \( C \) is said to be an \( e \)-error-correcting code. Given any vector \( \mathbf{v} \in \mathbb{F}_q^n \), its distance to the code \( C \) is \( d(\mathbf{v}, C) = \min_{\mathbf{x} \in C} \{d(\mathbf{v}, \mathbf{x})\} \) and the covering radius of the code \( C \) is \( \rho = \max_{\mathbf{v} \in \mathbb{F}_q^n} \{d(\mathbf{v}, C)\} \). Note that \( e \leq \rho \). If \( e = \rho \), then \( C \) is a perfect code. If \( e = \rho - 1 \), then \( C \) is called a quasi-perfect code. If \( C \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \), then \( C \) is linear and referred to as an \([n, k, d; \rho]_q\)-code. If \( C \) is linear of length \( n \) and dimension \( k \), then a generator matrix \( G \) for \( C \) is any \( k \times n \) matrix with \( k \) linearly independent codewords as rows. A parity-check matrix for \( C \) is an \((n - k) \times n \) matrix \( H \) such that \( C \) is the null space of \( H \), i.e. \( H\mathbf{x}^T = \mathbf{0}^T \) if and only if \( \mathbf{x} \in C \). The dual code \( C^\perp \) is the orthogonal subspace to \( C \). Hence, \( H \) generates \( C^\perp \) and \( G \) is a parity-check matrix for \( C^\perp \).

A linear single-error-correcting (\( e = 1 \)) perfect code is called a Hamming
code. Such a code has parameters

\[ n = (q^m - 1)/(q - 1), k = n - m, d = 3; \rho = 1 \] (m > 1)

and is denoted by \( H_m \). A parity-check matrix for \( H_m \), denoted by \( H_m \), contains a maximal set of \( n = (q^m - 1)/(q - 1) \) pairwise linearly independent column vectors of length \( m \) \([13]\). The dual code \( H_m^\perp \) generated by \( H_m \) is called simple and it is a constant-weight code, that is, all nonzero codewords have the same weight \( q^m - 1 \).

We denote by \( D = C + x \) a coset of \( C \), where + means the componentwise addition in \( \mathbb{F}_q \).

For a given \( q \)-ary code \( C \) of length \( n \) and covering radius \( \rho \), define

\[ C(i) = \{ x \in \mathbb{F}_q^n : d(x, C) = i \}, \quad i = 0, 1, \ldots, \rho. \]

The sets \( C(0), C(1), \ldots, C(\rho) \) are called the subconstituents of \( C \).

Say that two vectors \( x \) and \( y \) are neighbors if \( d(x, y) = 1 \). Given two vectors \( x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n \), we say that \( y \) covers \( x \) if \( y_i = x_i \), for all \( i \) such that \( x_i \neq 0 \).

**Definition 1.1** ([13]). A \( q \)-ary code \( C \) of length \( n \) and covering radius \( \rho \) is completely regular, if for all \( l \geq 0 \) every vector \( x \in C(l) \) has the same number \( c_l \) of neighbors in \( C(l - 1) \) and the same number \( b_l \) of neighbors in \( C(l + 1) \). Define \( a_l = (q - 1)n - b_l - c_l \) and set \( c_0 = b_\rho = 0 \). The parameters \( a_l, b_l \) and \( c_l \) (\( 0 \leq l \leq \rho \)) are called intersection numbers and the sequence \( IA = \{b_0, \ldots, b_{\rho - 1}; c_1, \ldots, c_\rho\} \) is called the intersection array of \( C \).

Let \( M \) be a monomial matrix, i.e. a matrix with exactly one nonzero entry in each row and column. Such a matrix can be written as \( M = DP \), where \( D \) is a monomial diagonal matrix and \( P \) is permutation matrix. If \( q \) is prime, then the automorphism group of \( C \), \( \operatorname{Aut}(C) \), consists of all monomial
n × n matrices M over \( \mathbb{F}_q \) such that \( xM \in C \) for all \( x \in C \). If \( q \) is a power of a prime number, then the monomial automorphism group of \( C \) is denoted by \( \text{MAut}(C) \), however, \( \text{Aut}(C) \) also contains any field automorphism of \( \mathbb{F}_q \) which preserves \( C \).

**Lemma 1.2.** If \( DP \) is the corresponding matrix to an automorphism \( \alpha \) of a code (where \( D \) is a monomial diagonal matrix and \( P \) is a permutation matrix), then \( D^{-1}P \) corresponds to an automorphism \( \alpha' \) of the dual code.

**Proof.** See [10, Thm. 1.7.9, p. 27]. \( \square \)

**Remark 1.** As a consequence of Lemma 1.2, \( \alpha \) and \( \alpha' \) are both transitive on the set of one-weight vectors, or both are not. Note also that if, for a code \( C \), \( \text{MAut}(C) \) is transitive, then so is \( \text{Aut}(C) \) since \( \text{MAut}(C) \subseteq \text{Aut}(C) \).

It is well known, e.g. see [13], that the monomial automorphism group of a Hamming code \( H_m \) is isomorphic to the general linear group \( \text{GL}(m, q) \), which acts transitively on the set of one-weight vectors. In the binary case, the action of \( \text{GL}(m, 2) \) on the set of coordinate positions is even doubly transitive.

The group \( \text{Aut}(C) \) acts on the set of cosets of \( C \) in the following way: for all \( \pi \in \text{Aut}(C) \) and for every vector \( \mathbf{v} \in \mathbb{F}_q^n \) we have \( \pi(\mathbf{v} + C) = \pi(\mathbf{v}) + C \).

**Definition 1.3 ([8, 17]).** Let \( C \) be a linear code over \( \mathbb{F}_q \) with covering radius \( \rho \). Then \( C \) is completely transitive if \( \text{Aut}(C) \) has \( \rho + 1 \) orbits when acts on the cosets of \( C \).

Since two cosets in the same orbit have the same weight distribution, it is clear that any completely transitive code is completely regular.

Completely regular and completely transitive codes are classical subjects in algebraic coding theory, which are closely connected with graph theory,
combinatorial designs and algebraic combinatorics. Existence, construction and enumeration of all such codes are open hard problems (see \([2, 3, 5, 11, 14, 18]\) and references there).

It is well known that new completely regular codes can be obtained by the direct sum of perfect codes or, more general, by the direct sum of completely regular codes with covering radius 1 \([1, 17]\).

In the current paper, starting from Hamming codes and choosing appropriate columns of their parity-check matrix, we obtain parity-check matrices for completely regular codes. More precisely, given the parity-check matrix \(H_m\) of a \(q\)-ary Hamming code, we consider a partition of the columns of \(H_m\) into two subsets. We consider these two subsets of columns as parity-check matrices of two codes, \(A\) and \(B\). We say that \(B\) is the supplementary code of \(A\) (and \(A\) is the supplementary code of \(B\)). If \(A\) or \(B\) is a Hamming code, then the supplementary code is also completely regular and completely transitive. We point out that, in this case, the dual code of the supplementary code belongs to the family SU1 in \([6]\). If \(A\) or \(B\) is a completely regular code with covering radius 2, then the supplementary code is completely regular with covering radius at most 2. Moreover, in this situation both codes are completely transitive or are not, simultaneously.

In this way, we construct infinite families of \(q\)-ary completely regular and completely transitive codes. It is worth mentioning that for fixed \(q\), we obtain a growing number of completely regular codes as the length of the starting Hamming code increases.

In the next section, we recall several known results on completely regular codes, which we shall use later. The main results and constructions are presented in Section 3.
2 Preliminary results

In this section we see several results we will need in the next sections.

Lemma 2.1 ([14]). Let $C$ be a completely regular code with covering radius $\rho$ and intersection array $\{b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_{\rho}\}$. If $C(i)$ and $C(i+1)$, $0 \leq i < \rho$, are two subconstituents of $C$, then

$$b_i|C(i)| = c_{i+1}|C(i+1)|.$$  

Let $C \subset \mathbb{F}_q^n$ be a code. For any vector $x \in \mathbb{F}_q^n$ and for all $j = 0, \ldots, n$, define $B_{x,j}$ as the number of codewords at distance $j$ from $x$:

$$B_{x,j} = |\{z \in C \mid d(x, z) = j\}|.$$  

Definition 2.2 ([9]). A quasi-perfect $e$-error-correcting $q$-ary code $C$ is called uniformly packed if there exist natural numbers $\lambda$ and $\mu$ such that for any vector $x$:

$$B_{x,e+1} = \begin{cases} \lambda & \text{if } d(x, C) = e, \\ \mu & \text{if } d(x, C) = e + 1. \end{cases}$$  

Van Tilborg [19] (see also [12, 16]) showed that no nontrivial codes of this kind exist for $e > 3$.

Proposition 1 ([9], see also [16]). A uniformly packed code is completely regular.

For a code $C$, we denote by $s + 1$ the number of nonzero terms in the dual distance distribution of $C$, obtained by the MacWilliams transform. The parameter $s$ was called external distance by Delsarte [7], and is equal to the number of nonzero weights of $C^\perp$ if $C$ is linear. The following properties show the importance of this parameter.
Theorem 2.3. If $C$ is any code with packing radius $e$, covering radius $\rho$, and external distance $s$, then

(i) \[ \rho \leq s. \]

(ii) \[ C \text{ is perfect } (e = \rho) \text{ if and only if } e = s. \]

(iii) \[ C \text{ is quasi-perfect uniformly packed if and only if } s = e + 1. \]

(iv) \[ \text{If } C \text{ is completely regular, then } \rho = s. \]

3 The new construction of completely regular codes

Let $H_m$ be the parity-check matrix of a $q$-ary Hamming code $H_m$ of length $n = (q^m - 1)/(q - 1)$, where $m > 1$. Take a non-empty subset of $n_A < n$ columns of $H_m$ as the parity-check matrix of a code $A$. Call $B$ the supplementary code that has as parity-check matrix the remaining $n_B = n - n_A$ columns of $H_m$. In this section, we see that if $A$ or $B$ is a completely regular code with covering radius $\rho(A) \leq 2$, then so is the supplementary code, under certain conditions.

For the rest of this section, we write $n_j = (q^j - 1)/(q - 1)$, for any integer value $j > 0$.

3.1 The case $\rho(A) = 1$

Since there are no two linearly dependent columns in $H_m$, we have that, for $n_A \geq 3$, the minimum distance of $A$ (and of $B$, for $n_A \leq n - 3$) is at least three and thus, the packing radius is at least 1. If $\rho(A) = 1$ (hence $n_A \neq 2$),

7
then \( e = \rho(A) = 1 \) for \( n_A \geq 3 \), by Theorem 2.3. Therefore, \( A \) is a perfect Hamming code for \( n_A > 1 \).

For \( u \in \{1, \ldots, m - 1\} \), \( H_m \) can be written as:

\[
H_m = \begin{bmatrix} H_u^* \\ H_{u,m} \end{bmatrix},
\]

where the first \( u \) rows of \( H_u^* \) are as the parity-check matrix of \( \mathcal{H}_u \) and the remaining \( m - u \) rows are all-zero vectors. For the case \( u = 1 \), the matrix \( H_u^* \) is simply the column vector \((1, 0, \ldots, 0)^T\). We call \( B_{u,m} = B \) the code that has parity-check matrix \( H_{u,m} \). Note that for \( n_A > 1 \), we have \( A = \mathcal{H}_u \).

**Lemma 3.1.** The dual code of \( B_{u,m} \), i.e. the code \( B_{u,m}^\perp \) generated by \( H_{u,m} \) has exactly two nonzero weights, namely, \( w_1 = q^{m-1} \) and \( w_2 = q^{m-1} - q^{u-1} \).

**Proof.** Clearly, \( H_u^* \) generates the simplex code, i.e. the dual of the Hamming code, of length \( n_u = (q^u - 1)/(q - 1) \). Hence any vector generated by \( H_u^* \) has weight 0 or \( q^{u-1} \). Since any nonzero vector generated by \( H_m \) has weight \( q^{m-1} \), the result follows.

**Proposition 2.** The code \( B_{u,m} \) has parameters

\[
[n_B = (q^m - q^u)/(q - 1), k = (q^m - q^u)/(q - 1) - m, d; \rho = 2]_q, \quad \text{where}
\]

\[
d = \begin{cases} 
4 & \text{if } u = m - 1, q = 2; \\
3 & \text{otherwise}.
\end{cases}
\]

**Proof.** The length \( n_B \) of \( B_{u,m} \) is simply the length of \( H_m \) minus the number of columns of \( H_u^* \). The dimension \( k \) is the length of \( B_{u,m} \) minus the number of rows of \( H_{u,m} \) (or \( H_m \)).

Of course, \( H_{u,m} \) has no scalar multiple columns, hence \( d > 2 \). Given two columns \( h_i \) and \( h_j \) of \( H_{u,m} \) we know that there is a column \( h_\ell \) in \( H_m \) which is linearly dependent with \( h_i \) and \( h_j \). If \( u < m - 1 \) or \( q > 2 \), we can choose...
\( \mathbf{h}_i \) and \( \mathbf{h}_j \) such that the last \( m - u \) entries are linearly independent, then \( \mathbf{h}_i \) cannot be one of the first \( n_u \) columns of \( H_m \). Indeed, those columns have zeros in the last \( m - u \) entries. Hence, \( B_{u,m} \) contains codewords of weight 3. For the case \( u = m - 1 \) and \( q = 2 \), the previous argument does not work since the last row of \( H_{u,m} \) is the all-ones vector. Thus, \( H_m \) can be written as:

\[
H_m = \begin{bmatrix} H_u & H_u & 0^T \\ 0 & 1 & 1 \end{bmatrix}.
\] (2)

In fact, in this case, \( B_{u,m} \) is the binary extended Hamming code of length \( 2^u \) and, therefore, it has minimum weight 4.

Finally, since \( B_{u,m} \) is not perfect, \( \rho > e = 1 \) and, by Lemma 3.1, \( B_{u,m} \) has external distance \( s = 2 \), hence \( \rho \leq 2 \) by Theorem 2.3.

**Lemma 3.2.** The number of vectors at distance 1 and at distance 2 from \( B_{u,m} \) are, respectively:

\[
|B_{u,m}(1)| = q^{n_B-m}(q^m - q^u), \quad \text{and} \quad |B_{u,m}(2)| = q^{n_B-m}(q^u - 1),
\]

where \( n_B = (q^m - q^u)/(q - 1) \) is the length of \( B_{u,m} \).

**Proof.** The number of vectors of weight 1 is \((q - 1)n_B\). All these vectors are at distance 1 from exactly one codeword (the zero vector). Thus, \( |B_{u,m}(1)| = (q - 1)n_B|B_{u,m}| = q^{n_B-m}(q^m - q^u) \).

Since the covering radius of \( B_{u,m} \) is \( \rho = 2 \), we have that

\[
|B_{u,m}(2)| = |\mathbb{F}_q^{n_B}| - |B_{u,m}(1)| - |B_{u,m}| = q^{n_B} - q^{n_B-m}(q^u - 1) - q^{n_B-m} = q^{n_B-m}(q^u - 1).
\]
Corollary 1. The code $B_{u,m}$ is quasi-perfect uniformly packed (hence completely regular) with intersection array:

$$IA = \{q^m - q^u, q^u - 1; 1, q^m - q^u\}.$$

Proof. Since $s = \rho = e + 1$, $B_{u,m}$ is a quasi-perfect uniformly packed code, by Theorem 2.3. Since $d \geq 3$, it is clear that $b_0 = (q - 1)n_B = q^m - q^u$ and $c_1 = 1$. Given a vector $x$ of weight 1, the vectors $y$ of weight 2 covering $x$ not at distance one from $B_{u,m}$ are those which are covered by codewords of $H_m$ of weight 3, but not in $B_{u,m}$, hence with the third nonzero coordinate in the first $n_u$ positions. In other words, for $x$ we can choose anyone of these $n_u$ first positions and, for each of these positions, anyone of the $q - 1$ multiples. Therefore $x$ is covered by $(q - 1)n_u = q^u - 1$ vectors of weight 2 at distance 2 from $B_{u,m}$. Thus, we obtain $b_1 = q^u - 1$.

By Lemma 2.1 we know that $b_1|B_{u,m}(1)| = c_2|B_{u,m}(2)|$. Applying Lemma 3.2 we obtain:

$$c_2 = \frac{(q^u - 1)q^{n_u}m(q^m - q^u)}{q^{n_u}m(q^u - 1)} = q^m - q^u.$$

Remark 2. It is not difficult to prove directly that given a vector $x \in B_{u,m}(2)$, any neighbor of $x$ must be in $B_{u,m}(1)$, obtaining the value of $c_2$.

Denote by $(x \mid x') = (x_1, \ldots, x_{n_u} \mid x'_{n_u+1}, \ldots, x'_{n_m})$ a vector in $\mathbb{F}_q^{n_m}$ such that $x \in \mathbb{F}_q^{n_u}$ and $x' \in \mathbb{F}_q^{n_m-n_u}$. Let $e_j$ denote any one-weight vector with its nonzero coordinate at position $j$.

Lemma 3.3. The number of cosets of $B_{u,m}$ of minimum weight 2 is $q^u - 1$. Moreover, for any vector $x' \in \mathbb{F}_q^{n_m-n_u}$ in one such coset, the vector $(0 \mid x')$ is contained in a coset of weight 1 of $H_m$ with leader $e_j$, which has its nonzero coordinate at position $j \in \{1, \ldots, n_u\}$. 

10
Proof. The total number of cosets of $B_{u,m}$ is $q^{n_u} / q^{n_u-m} = q^m$. Since there are one coset of minimum weight 0 (the code $B_{u,m}$) and $(q-1)n_B = q^m - q^u$ cosets of minimum weight 1, we obtain that the number of cosets of minimum weight 2 is $q^m - (q^m - q^u) - 1 = q^u - 1$.

Since $d(x',B_{u,m}) = 2$, we have that there is some codeword $c' \in B_{u,m}$ such that $y' = x' - c'$ has weight 2. Hence, $(0 \mid y')$ is covered by some codeword (of weight 3) $(e_j \mid y') \in \mathcal{H}_m$. Thus, $(0 \mid y') = (0 \mid x' - c') \in \mathcal{H}_m - e_j$. Note that $(0 \mid c') \in \mathcal{H}_m$. Then, $(0 \mid x' - c') + (0 \mid c') \in \mathcal{H}_m - e_j$, implying $(0 \mid x') \in \mathcal{H}_m - e_j$.

The matrix $H_m$ (1) can be written as:

$$H_m = \begin{bmatrix} H_u & H_u & \cdots & H_u & 0_{u,n_{m-u}} \\ 0_{m-u,n_u} & G_1 & \cdots & G_{q^m-u-1} & H_{m-u} \end{bmatrix},$$

where $0_{i,j}$ stands for the all-zero matrix of size $i \times j$ and $G_1,\ldots,G_{q^m-u-1}$ are $m-u \times n_u$ matrices, each one with identical nonzero columns and such that no two columns of distinct $G'_i$s are equal. To see that the matrix (3) is equivalent to the matrix (1), note that no two columns of the matrix (3) are linearly dependent. Therefore, the matrix (3) is a parity-check matrix for $\mathcal{H}_m$. Indeed the total number of columns is $q^m - u_n + n_{m-u} = n_m$.

For $i = 0,\ldots,q^{m-u}$, we call $i$-block of coordinate positions the set $\{in_u + 1,\ldots,(i+1)n_u\}$. Thus, the first block, or 0-block, corresponds to $\{1,\ldots,n_u\}$. For $i = 1,\ldots,q^{m-u} - 1$, the $i$-block corresponds to the set of coordinates of the matrix $G_i$. Finally, the last block, or $q^{m-u}$-block, corresponds to the coordinates of the matrix $H_{m-u}$.

Lemma 3.4. If $\alpha \in \text{Aut}(\mathcal{H}_u)$ (acting on the coordinates $\{1,\ldots,n_u\}$), then there exists $\beta \in \text{Aut}(B_{u,m})$ (acting on the coordinates $\{n_u+1,\ldots,n_m\}$) such that $\gamma = (\alpha \mid \beta) \in \text{Aut}(\mathcal{H}_m)$.
Proof. Given $\alpha \in \text{Aut}(\mathcal{H}_u)$, consider $\gamma = (\alpha \mid \alpha_1 \mid \cdots \mid \alpha_{q^{m-u}-1} \mid \text{id})$, where the action of each $\alpha_i$ is identical to the action of $\alpha$ but on the corresponding $i$-block of coordinate positions, and $\text{id}$ is the identity on the last block of coordinates. Clearly, $\gamma \in \text{Aut}(\mathcal{H}_m^\perp)$ and $\beta = (\alpha_1 \mid \cdots \mid \alpha_{q^{m-u}-1} \mid \text{id}) \in \text{Aut}(B_{u,m}^\perp)$. By Lemma 1.2, the result follows.

Proposition 3. The automorphism group $\text{Aut}(B_{u,m})$ is transitive (on the set of one-weight vectors with coordinates in $\{n_u + 1, \ldots, n_m\}$).

Proof. Recall that the automorphism group of a Hamming code $\mathcal{H}_m$ is isomorphic to $\text{GL}(m, q)$, which acts transitively on the set of one-weight vectors.

Consider the parity-check matrix of $\mathcal{H}_m$ given in (2). Consider the $m \times m$ matrices $H_{K,M,N}$, where $K, M$ are $u \times u$, $(m - u) \times (m - u)$, nonsingular matrices, respectively, and $N$ is a $u \times (m - u)$ matrix.

$$H_{K,M,N} = \begin{pmatrix} K & N \\ 0 & M \end{pmatrix}.$$ 

The matrices $H_{K,M,N}$ are in $\text{GL}(m, q)$ and act on $H_m$ as monomial automorphisms, stabilising the Hamming code $\mathcal{H}_a$, so we can consider these matrices as automorphisms of $B_{u,m}$. Now, we want to show that these matrices assure the transitivity of $\text{Aut}(B_{u,m})$. Take the $i$th and $j$th columns, say $\mathbf{h}_i$ and $\mathbf{h}_j$, respectively, where $i, j \in \{n_u + 1, \ldots, n_m\}$. We want to find appropriate matrices $K, M, N$ such that $H_{K,M,N}(\mathbf{h}_i) = \lambda \mathbf{h}_j$, for any $\lambda \in \mathbb{F}_q$.

Take the projections of both $\mathbf{h}_i$, $\mathbf{h}_j$ on the first $u$ coordinates, say $\mathbf{h}_i^{(u)}$ and $\mathbf{h}_j^{(u)}$, respectively. And also let $\mathbf{h}_i^{(m-u)}$ and $\mathbf{h}_j^{(m-u)}$ be the respective projections on the last $m - u$ coordinates.

First of all, consider the case when $i$ and $j$ are not in the last block of coordinate positions, so that $\mathbf{h}_i^{(u)}$ and $\mathbf{h}_j^{(u)}$ are nonzero vectors. Now, take $N = 0$, take the matrix $K$ such that $K(\mathbf{h}_i^{(u)}) = \lambda \mathbf{h}_j^{(u)}$ and the matrix $M$
such that $M(h_i^{(m-u)}) = \lambda h_j^{(m-u)}$. Indeed, we can do these last assignments since the matrix $K$ is in $\text{GL}(u, q)$, the matrix $M$ is in $\text{GL}(m - u, q)$ and the monomial automorphism group of a $q$-ary Hamming code is transitive on the set of one-weight vectors. Hence, we have $H_{K, M, N}(h_i) = \lambda h_j$.

Secondly, consider the case when $i$ and $j$ belong to the last block of coordinate positions. Then, $h_i^{(u)}$ and $h_j^{(u)}$ are the all-zeros vector. Now, take $N = 0$, any nonsingular matrix $K$ and the matrix $M$ such that $M(h_i^{(m-u)}) = \lambda h_j^{(m-u)}$. Hence, we have $H_{K, M, N}(h_i) = \lambda h_j$.

Finally, consider the case when $i$ is in the last block of coordinate positions and $j$ is not. In this case, $h_i^{(u)}$ is the all-zeros vector and $h_j^{(u)}$ is a nonzero vector. Now, take as matrix $K$ any nonsingular matrix and the matrix $M$ such that $M(h_i^{(m-u)}) = \lambda h_j^{(m-u)}$. Let $\ell$ be anyone of the nonzero coordinates of $h_i^{(m-u)}$ and say $\gamma$ its value. Take the matrix $N$ with all columns equal to the all-zeros vector, except the $\ell$th column which is $\lambda \gamma^{-1} h_j^{(u)}$. Hence, we have $H_{K, M, N}(h_i) = \lambda h_j$. For the inverse case, when $h_i^{(u)}$ is a nonzero vector and $h_j^{(u)}$ is the all-zeros vector, we can use the same argumentation and finally take the inverse matrix of $H_{K, M, N}$.

Remark 3. In fact, Proposition 3 shows that the action of $\text{MAut}(B_{u, m})$ on the set of one-weight vectors is transitive. As a consequence, see Remark 7, the full automorphism group $\text{Aut}(B_{u, m})$ is also transitive.

Corollary 2. The code $B_{u, m}$ is completely transitive.

Proof. By Proposition 2, $\rho(B_{u, m}) = 2$. Hence, we have to see that the cosets of weight $i$ are in the same orbit, for $i = 1$ and $i = 2$.

Since $\text{Aut}(B_{u, m})$ is transitive by Proposition 3 we have that all the cosets of $B_{u, m}$ with minimum weight one are in the same orbit.

By Lemma 3.4 it follows that $\text{Aut}(\mathcal{H}_u) = \text{GL}(u, q)$ acting on the first $n_u$ coordinates is contained in $\text{Aut}(\mathcal{H}_m) = \text{GL}(m, q)$, acting on the full set.
of $n_m$ coordinate positions. Let $B_{u,m} + x$ and $B_{u,m} + y$ be two cosets of minimum weight 2, where we assume that $x$ and $y$ have weight two. Let $\mathcal{H}_m + e_i$ and $\mathcal{H}_m + e_j$, with $i, j \in \{1, \ldots, n_u\}$, be the corresponding cosets of $\mathcal{H}_m$, according to Lemma 3.3. Since $\text{Aut}(\mathcal{H}_u) = \text{GL}(u, q)$ is transitive, and by Lemma 3.4, there is an automorphism $\gamma \in \text{Aut}(\mathcal{H}_m)$ fixing setwise the first $n_u$ coordinates (and the last $n_m - n_u$) such that $\gamma(\mathcal{H}_m + e_i) = \mathcal{H}_m + e_j$.

By Lemma 3.4, it is clear that the action of $\gamma$ in the last $n_m - n_u$ coordinates sends $B_{u,m} + x$ to $B_{u,m} + y$. Indeed, if $\gamma(\mathcal{H}_m + x) = \mathcal{H}_m + z$, for some $z$ of weight two, then $e_j + y$ and $e_j + z$ are codewords in $\mathcal{H}_m$. Thus, $y$ and $z$ are in the same coset. Therefore, all the cosets of $B_{u,m}$ of weight two are in the same orbit.

### 3.2 The case $\rho(A) = 2$

For this case, we have the following result.

**Theorem 3.5.** If the code $A$ has dimension $n_A - m$ and is completely regular with $\rho(A) = 2$, then the supplementary code $B$, of length $n_B$, is completely regular with $\rho(B) \leq 2$.

**Proof.** If $A$ is completely regular with $\rho(A) = 2$ then, by Theorem 2.3, the external distance of $A$ is $s(A) = 2$. Hence, $A^\perp$ has two nonzero weights, say $w_1$ and $w_2$. Consider any nonzero vector $z = (x \mid y) \in \mathcal{H}_m^\perp$, where $x \in A^\perp$ and $y \in B^\perp$. Since $z$ is a nonzero codeword of the simplex code of length $n_m$, we know that the weight of $z$ is $\text{wt}(z) = q^{m-1}$. Also, $\text{wt}(z) = \text{wt}(x) + \text{wt}(y)$ and thus we obtain that $\text{wt}(y) = q^{m-1} - w_1$ or $\text{wt}(y) = q^{m-1} - w_2$. Note that $x$ cannot be the zero vector because the dimension of $A^\perp$ is $m$. We conclude that $B^\perp$ has at most two nonzero weights (if $w_1$ or $w_2$ equals $q^{m-1}$, then $B^\perp$ has only one nonzero weight). Therefore $s(B) \leq 2$, implying $\rho(B) \leq 2$, by
Theorem 2.3

If \( s(B) = 1 \), then \( B \) is the trivial code of length 1, \( B = \{(0)\} \), or \( B \) is a Hamming code, by Theorem 2.3. In any case, \( B \) is completely regular. In fact, if \( s(B) = 1 \), we are in the situation of Section 3.1 interchanging the roles of \( A \) and \( B \).

If \( s(B) = 2 \) and \( \rho(B) = 2 \), then \( B \) is a quasi-perfect uniformly packed code, by Theorem 2.3. Therefore, \( B \) is completely regular by Proposition 1.

Finally, note that \( s(B) = 2 \) and \( \rho(B) = 1 \) is not possible:

(i) If \( n_B = 1 \), then \( s(B) \) cannot be 2.

(ii) If \( n_B = 2 \), then \( B = \{(0,0)\} \), which has \( \rho(B) = 2 \).

(iii) If \( n_B \geq 3 \), then \( B \) has packing radius \( e \geq 1 \). Since \( e \leq \rho(B) \), if we assume \( \rho(B) = 1 \), then we have \( e = \rho(B) < s(B) \) contradicting Theorem 2.3.

Remark 4. If the length of \( A \) verifies \( n_A > n_{m-1} \), then the zero vector cannot be a row of the parity-check matrix of \( A \), otherwise \( H_m \) would have two linearly dependent columns. Hence, the zero vector could not be generated by the rows of the parity-check matrix of \( A \) and, as a consequence, the dimension of \( A^\perp \) would be \( m \). Therefore, the condition \( n_A > n_{m-1} \) implies that the dimension of \( A \) is \( n_A - m \). Note that the converse statement is not true (see the next example).

Example 1. Let \( A \) be the ternary Golay \([11,6,5;2]_3 \) code. Consider the ternary matrix \( H_5 \), which is the parity-check matrix of a ternary Hamming \([121,116,3;1]_3 \) code. Let \( B \) be the supplementary code which has length \( n_B = 110 \).
Since $A$ is perfect (so completely regular) with covering radius $\rho(A) = 2$, we have that $B$ is a completely regular code. Clearly, $B$ is not perfect, thus $\rho(B) = 2$. Therefore, the parameters of $B$ are $[110, 105, 3; 2]_3$. Moreover, we have computationally verified that $B$ is completely transitive and with intersection array

$$IA = \{220, 20; 1, 200\}.$$  

Note that the hypothesis about the dimension of $A$ in Theorem 3.5 cannot be relaxed, as the next example shows.

**Example 2.** Let $A$ be the punctured ternary Golay $[10, 6, 4; 2]_3$ code. As in Example 1, consider $H_5$, the parity-check matrix of a ternary Hamming $[121, 116, 3; 1]_3$ code. Now, let $B$ be the supplementary code with length $n_B = 111$. In this case, the dimension of $A$ is $6 \neq n_A - m = 5$.

The code $A$ is completely regular and completely transitive with intersection array

$$IA = \{20, 18; 1, 6\}.$$  

The code $B$ has parameters $[111, 106, 3; 2]_3$ and it is not completely regular since its external distance is $s(B) = 4$.

**Remark 5.** The construction described in Theorem 3.5 does not work for covering radius $\rho(A) = 3$. For example, let $A$ be the extended ternary Golay code and consider the ternary matrix $H_6$, which is the parity-check matrix of a ternary Hamming $[364, 258, 3; 1]_3$ code. Let $B$ be the supplementary code.

The code $A$ is completely transitive with $\rho(A) = 3$. The code $B$ has parameters $[352, 346, 3; 2]_3$ and it is not completely regular since its external distance is $s(B) = 3$.

We also give the expressions of the intersection numbers of $A$ and $B$ in terms of the lengths $n_A$ and $n_B$ and the parameter $b_1$.  

16
Corollary 3. Assume that the code $A$ is completely regular with dimension $n_A - m$, covering radius $\rho(A) = 2$, and the supplementary code $B$ has also covering radius $\rho(B) = 2$.

(i) The code $B$ is completely regular with dimension $n_B - m$.

(ii) The code $A$ has intersection array

$$IA(A) = \{b_0, b_1; c_1, c_2\} = \{(q - 1)n_A, b_1; 1, \frac{n_A}{n_B}b_1\}.$$ 

(iii) The code $B$ has intersection array

$$IA(B) = \{b'_0, b'_1; c'_1, c'_2\} = \{(q - 1)n_B, (q - 1)n_A - \frac{n_A}{n_B}b_1; 1, (q - 1)n_B - b_1\}.$$ 

Proof. For (i), we already know that $B$ is completely regular, by Theorem 3.5. Assume that the dimension of $B$ is less than $n_B - m$. Hence, the parity-check matrix of $B$ can be written containing at least one zero row. Since $s(B) = \rho(B) = 2$, the dual code $B^\perp$ contains two nonzero weights, say $w_1$ and $w_2$. But, in this case, $A^\perp$ would contain three nonzero weights: $q^{m-1}$, $q^{m-1} - w_1$ and $q^{m-1} - w_2$; leading to a contradiction because $A$ has external distance $s(A) = 2$.

For (ii) and (iii), with similar computations as in Lemma 3.2, we have:

$$|A(1)| = (q - 1)n_A|A|,$$

$$|A(2)| = q^{n_A} - (q - 1)n_A|A| - |A|.$$ 

By Lemma 2.1 we obtain

$$b_1(q - 1)n_A|A| = c_2(q^{n_A} - ((q - 1)n_A + 1)|A|).$$ 

Taking into account that $|A| = q^{n_A - m}$ and $n_B = n_m - n_A$, the expression simplifies to

$$b_1n_A = c_2n_B.$$ 

(4)
By (i), we have that $|B| = q^{n_B-m}$, thus we symmetrically obtain
\[ b'_1 n_B = c'_2 n_A. \tag{5} \]

Let $J_A$ (respectively $J_B$) be the set of $n_A$ (resp. $n_B$) coordinate positions corresponding to the code $A$ (resp. $B$). Define $X_A$ (resp. $X_B$) as the set of one-weight vectors with coordinates in $J_A$ (resp. $J_B$). Define also $Y_A$ (resp. $Y_B$) as the set of two-weight vectors in $A(2)$ (resp. $B(2)$) with coordinates in $J_A$ (resp. $J_B$). Consider the bipartite graph $\Gamma_A$ (resp. $\Gamma_B$) with vertex set $X_A \cup Y_A$ (resp. $X_B \cup Y_B$) and edges joining pairs of vertices $x, y$, where $x \in X_A$, $y \in Y_A$ (resp. $x \in X_B$, $y \in Y_B$), if $d(x, y) = 1$.

The degree of any vertex in $X_A$ (resp. $X_B$) is $b_1$ (resp. $b'_1$) by definition. Hence, the total number of edges in $\Gamma_A$ (resp. $\Gamma_B$) is $b_1(q-1)n_A$ (resp. $b'_1(q-1)n_B$).

Consider the set of all two-weight vectors with one nonzero coordinate in $J_A$ and one nonzero coordinate in $J_B$. There are $(q-1)^2 n_An_B$ such vectors. If $e_i + e_j$ is one of these vectors ($i \in J_A$, $j \in J_B$), then there is exactly one codeword $z \in \mathcal{H}_m$ of weight three which covers $e_i + e_j$, say $z = e_i + e_j + e_k$. If $k \in J_A$, then $e_i + e_k \in A(2)$ and $e_i + e_k$ is a neighbor of $e_i$. Else, if $k \in J_B$, then $e_j + e_k \in B(2)$ and $e_j + e_k$ is a neighbor of $e_j$. Therefore, the vector $e_i + e_j$ induces either one edge of $\Gamma_A$, or one edge of $\Gamma_B$.

We conclude that
\[ b_1 n_A(q-1) + b'_1 n_B(q-1) = (q-1)^2 n_A n_B, \]
which simplifies to
\[ b_1 n_A + b'_1 n_B = (q-1)n_A n_B. \tag{6} \]

The values $b_0 = (q-1)n_A$, $b'_0 = (q-1)n_B$, $c_1 = c'_1 = 1$ are trivial since $A$ and $B$ have minimum distance at least three. From Equation (6), we obtain
\[ c_2 = n_A b_1 / n_B. \] Using Equation (6), we compute \( b'_1 = (q - 1) n_A - n_A b_1 / n_B, \)
and by Equation (5), \( c'_2 = (q - 1) n_B - b_1. \)

Finally, we will also show that the codes \( A \) and \( B \), under the hypothesis of Corollary 3, are both completely transitive or both are not.

**Proposition 4.** Assume that the code \( A \) has dimension \( n_A - m \), covering radius \( \rho(A) = 2 \), and let \( B \) be the supplementary code. Then \( \text{Aut}(A) \) is a subgroup of \( \text{Aut}(B) \).

**Proof.** Let \( \phi \in \text{Aut}(A) \). Let \( H_A \) (respectively \( H_B \)) be the parity-check matrix of \( A \) (resp. \( B \)). Note that since the dimension of \( A \) is \( n_A - m \), the minimum distance of \( A \) is not less than three. Let \( h_1, \ldots, h_s \) be a set of \( s \) columns in \( H_A \) such that \( \sum_{i=1}^s \alpha_i h_i = 0 \), where \( \alpha_i \in \mathbb{F}_q \). Hence, we are assuming that the columns \( h_1, \ldots, h_s \) are the support of a codeword in \( A \). Since \( \phi \) is an automorphism of \( A \) we should have \( \sum_{i=1}^s \alpha_i \phi(h_i) = 0 \) and so the action of \( \phi \) is linear over the columns in \( H_A \). Since the dimension of \( A \) is \( n_A - m \) we can extend, by linearity, the action of \( \phi \) over all columns in \( H_m \) obtaining \( \phi^{(c)} \in \text{Aut}(H_m) \). The projection of \( \phi^{(c)} \) over the columns of \( H_B \) gives \( \phi^{(c)}_B \in \text{Aut}(B) \). It is clear that if \( \phi, \psi \in \text{Aut}(A) \) with \( \phi \neq \psi \), then \( \phi^{(c)}_B \neq \psi^{(c)}_B \).

**Corollary 4.** If the dimension of \( A \) is \( n_A - m \) and the dimension of \( B \) is \( n_B - m \) then \( \text{Aut}(A) \) and \( \text{Aut}(B) \) are isomorphic as abstract groups.

**Theorem 3.6.** If the code \( A \) is completely transitive with dimension \( n_A - m \) and covering radius \( \rho(A) = 2 \), then the supplementary code \( B \) is also completely transitive.

**Proof.** From Theorem 3.5, when \( A \) is a completely regular code with \( \rho(A) = 2 \), then \( B \) is completely regular with \( \rho(B) \leq 2 \). When \( \rho(B) = 1 \) the code \( B \) is a completely transitive code, so we are interested in proving that \( B \) is a
completely transitive code in the case when $\rho(B) = 2$. Since $A$ is completely regular, we have that the dimension of $B$ is $n_B - m$, by Corollary 3. Hence, the minimum distances of $A$ and $B$ are not less than three.

Take two pairs of columns in the parity-check matrix $H_B$ of the code $B$. Say $h_{i1}, h_{i2}$ and $h_{j1}, h_{j2}$. Each pair represents a vector of weight two and we assume that both vectors are at distance two from $B$ and also they are not in the same coset (modulo the code $B$). Therefore, we obtain two different columns $h_i, h_j$ in $H_A$ (the parity-check matrix of $A$), in such a way that both triples $h_{i1}, h_{i2}, h_{i}$ and $h_{j1}, h_{j2}, h_{j}$ are the support of codewords of weight three in $\mathcal{H}_m$. Since $A$ is completely transitive, there exists $\phi \in \text{Aut}(A)$ taking one of these columns to the other and, from Proposition 4, we have an automorphism in $\text{Aut}(B)$ taking the pair $h_{i1}, h_{i2}$ to $h_{j1}, h_{j2}$. Now, to finish the proof we need to show that taking $h_i, h_j$ two different columns in $H_B$, we have an automorphism in $\text{Aut}(B)$ which leads $h_i$ to $h_j$. It is easy to see that there are $\frac{n-1}{2}(q-1)^2$ codewords of minimum weight in the Hamming code $\mathcal{H}_m$ containing in its support the coordinate position corresponding to $h_i$. Of those codewords, there are $(a'_1 - (q - 2))(q - 1)/2$ such that they are also codewords of weight three in $B$ ($a'_1$ is the corresponding parameter of the code $B$ in Definition 1.1). Also there are $b'_1(q - 1)$ codewords sharing exactly two coordinates with the support of the code $B$. Hence,

$$
\frac{n-1}{2}(q-1)^2 - b'_1(q-1) - \frac{(a'_1 - (q - 2))(q - 1)}{2} = \\
\frac{q-1}{2} [(n - 1)(q - 1) - 2b'_1 - (n_B(q - 1) - b'_1 - 1 - (q - 2))] = \\
\frac{q-1}{2} [(n_A - 1)(q - 1) - b'_1 + (q - 1)] = \\
\frac{q-1}{2} [n_A(q - 1) - b'_1] = \frac{(q - 1) n_A b'_1}{2 n_B} = \frac{(q - 1)c}{2}
$$

(7)

is the number of codewords of weight three from $\mathcal{H}_m$ with the coordinate
corresponding to \( h \), in its support and the other two coordinates in the support of the code \( A \). The code \( B \) will be a completely transitive code when Equation (7) gives a number greater than or equal to one, which is obvious. This proves the statement. \( \square \)

It is worth mentioning that, in some cases, the construction used here can be equivalent to the construction described in [4]. But this is not always the case as the following examples show.

**Example 3.** Consider the binary matrix \( H_6 \), which the parity-check matrix of the binary Hamming code of length 63. Take 35 columns of \( H_6 \) following the procedure described in [3], as the parity-check matrix of the code \( A \). The code \( A \) has parameters \([35, 29, 3; 2; 2]\) and the supplementary code \( B \) has parameters \([28, 22, 3; 2]\). Computationally, we have verified that both codes are completely regular but not completely transitive.

**Example 4.** Now, consider the binomial code \( A' = C^{(7,4)} \), whose parity-check matrix \( H^{(7,4)} \) contains as columns all the binary vectors of length 7 and weight 4 (see [12]). Note that adding all the rows of \( H^{(7,4)} \) gives the zero vector, hence the dimension of \((A')^\perp\) is 6. The code \( A' \) has parameters \([35, 29, 3, 2; 2]\) and the supplementary code \( B' \) has parameters \([28, 22, 3; 2]\). In this case, we have computationally verified that both codes are completely regular and also completely transitive.

The codes \( A \) and \( A' \) (respectively \( B \) and \( B' \)) in Example 3 and Example 4 are completely regular codes with the same parameters. However, \( A \) and \( A' \) (resp. \( B \) and \( B' \)) are not equivalent since \( A' \) (resp. \( B' \)) is completely transitive, but \( A \) (resp. \( B \)) is not.
Acknowledgements

This work has been partially supported by the Spanish grants TIN2016-77918-P, (AEI/FEDER, UE). The research of the third author was carried out at the IITP RAS at the expense of the Russian Fundamental Research Foundation (project no. 19-01-00364).

References

[1] L.A. Bassalygo, G.V. Zaitsev, V.A. Zinoviev, Uniformly packed codes. Problems Inform. Transmiss, 10, (1974), 9–14.

[2] J. Borges, J. Rifà and V.A. Zinoviev, On completely regular codes by concatenation constructions, in WCC2017-10th International Workshop on Coding and Cryptography 2017, 2017.

[3] J. Borges, J. Rifà and V.A. Zinoviev, On completely regular codes by concatenating Hamming codes, Advances in Mathematics of Communications, 12 (2018), 337–349.

[4] J. Borges, J. Rifà and V.A. Zinoviev, On new infinite families of completely regular and completely transitive binary codes, in ACCT2018-16th International Workshop on Algebraic and Combinatorial Coding Theory 2018, 2018.

[5] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-Regular Graphs, Springer, 1989.

[6] R. Calderbank and W. Kantor, The geometry of two-weight codes, Bulletin of the London Mathematical Society, 18 (1986), 97–122.
[7] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Thesis, 1973.

[8] M. Giudici and C. E. Praeger, Completely transitive codes in hamming graphs, *European Journal of Combinatorics*, 20 (1999), 647–662.

[9] J. Goethals and H. VanTilborg, Uniformly packed codes, *Philips Research Reports*, 30 (1975), 9–36.

[10] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[11] J. Koolen, D. Krotov and B. Martin, Completely regular codes, https://sites.google.com/site/completelyregularcodes.

[12] K. Lindström, All nearly perfect codes are known, *Information and Control*, 35 (1977), 40–47.

[13] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.

[14] A. Neumaier, Completely regular codes, *Discrete mathematics*, 106 (1992), 353–360.

[15] J. Rifà and V. Zinoviev, On a class of binary linear completely regular codes with arbitrary covering radius, *Discrete mathematics*, 309 (2009), 5011–5016.

[16] N. Semakov, V. A. Zinoviev and G. Zaitsev, Uniformly packed codes, *Problemy Peredachi Informatsii*, 7 (1971), 38–50.

[17] P. Solé, Completely regular codes and completely transitive codes, *Discrete Mathematics*, 81 (1990), 193–201.
[18] E. R. van Dam, J. H. Koolen and H. Tanaka, Distance-regular graphs, \textit{arXiv preprint arXiv:1410.6294}.

[19] H. C. A. van Tilborg, \textit{Uniformly packed codes}, Technische Hogeschool Eindhoven, 1976.