New completely regular $q$-ary codes based on Kronecker products

J. Rifà, V.A. Zinoviev

Abstract

For any integer $\rho \geq 1$ and for any prime power $q$, the explicit construction of an infinite family of completely regular (and completely transitive) $q$-ary codes with $d = 3$ and with covering radius $\rho$ is given. The intersection array is also computed. Under the same conditions, the explicit construction of an infinite family of $q$-ary uniformly packed codes (in the wide sense) with covering radius $\rho$, which are not completely regular, is also given. In both constructions the Kronecker product is the basic tool that has been used.

Index Terms

Completely regular codes, completely transitive codes, covering radius, Kronecker product, intersection numbers, uniformly packed codes.

I. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field of the order $q$. Let $\text{wt}(v)$ denote the Hamming weight of a vector $v \in \mathbb{F}_q^n$ and let $d(v, u) = \text{wt}(v - u)$ denote the Hamming distance between two vectors $v, u \in \mathbb{F}_q^n$. We say that two vectors $v$ and $u$ are neighbors if $d(v, u) = 1$. A $q$-ary linear $[n, k, d]_q$-code $C$ is a

This work has been partially supported by the Spanish MEC and the European FEDER Grants MTM2006-03250 and TSI2006-14005-C02-01 and also by the Russian fund of fundamental researches (the number of project 06 - 01 - 00226). Part of the material in Section III was presented at the 2nd International Castle Meeting on Coding Theory and Applications (2ICMCTA), Medina del Campo, Spain, September 2008.

Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol’shoy Karetnyi per. 19, GSP-4, Moscow, 101447, Russia
$k$-dimensional subspace of $F_n^q$, where $n$ is the length, $N = q^k$ is the cardinality of $C$ and $d$ is the minimum distance,

$$d = \min\{d(v, u) : v, u \in C, v \neq u\}.$$  

The error correcting capability of a code $C$ with minimum distance $d$ is given by $e = \lfloor (d-1)/2 \rfloor$.

Given any vector $v \in F_n^q$, its distance to the code $C$ is $d(v, C) = \min_{x \in C} \{d(v, x)\}$ and the covering radius of the code $C$ is

$$\rho = \max_{v \in F_n^q} \{d(v, C)\}.$$  

Let $D = C + x$ be a coset of $C$, where $+$ means the component-wise addition in $F_q$. The weight $\text{wt}(D)$ of $D$ is the minimum weight of the codewords of $D$. For an arbitrary coset $D$ of $C$ of weight $s = \text{wt}(D)$ denote by $\mu(D) = (\mu_0(D), \mu_1(D), ..., \mu_n(D))$ its weight distribution, where $\mu_j(D), j = 0, \ldots, n$ denotes the number of words of $D$ of weight $j$. Notice that $\mu_j(D) = 0$ for all $j < s$.

**Definition 1:** A $q$-ary linear code $C$ with covering radius $\rho$ is called completely regular if the weight distribution of any coset $D$ of $C$ of weight $i$, $i = 0, 1, \ldots, \rho$ is uniquely defined by the minimum weight of $D$, i.e. by the number $i = \text{wt}(D)$.

**Definition 2:** Let $C$ be a $q$-ary code of length $n$ and let $\rho$ be its covering radius. We say that $C$ is uniformly packed in the wide sense, i.e. in the sense of [1], if there exist rational numbers $\alpha_0, \ldots, \alpha_\rho$ such that for any $v \in F_n^q$

$$\sum_{k=0}^{\rho} \alpha_k f_k(v) = 1,$$

where $f_k(v)$ is the number of codewords at distance $k$ from $v$.

The case $\rho = e + 1$ corresponds to uniformly packed codes, suggested in [10], and the case $\rho = e+1$ and $\alpha_{\rho-1} = \alpha_\rho$ corresponds to uniformly packed codes in the narrow sense or sometimes called strongly uniformly packed codes, suggested in [18]; see more special cases of such codes in [7], [9], [10], [18]. It is well known (see, for example, [5]) that any completely regular code is uniformly packed in the wide sense. In turn, uniformly packed codes with $\rho = e + 1$ are completely regular [10], [18], including some extended such codes [1], [2], [18]. But till now, the only known examples of uniformly packed codes, which are not completely regular, were the known binary (primitive in narrow sense) BCH codes of length $n = 2^m - 1$ (m odd) with
minimum distance \( d = 7 \) [6] and the \( \mathbb{Z}_4 \)-linear Goethals-like codes of length \( n = 2^m - 1 \) \((m \text{ even})\) with minimum distance \( d = 7 \) [12] (including extended codes for both families of codes). In both cases the codes have covering radius \( \rho = e + 2 = 5 \), and \( \rho = e + 3 = 6 \) for extended codes.

It has been conjectured for a long time that if \( C \) is a completely regular code and \( |C| > 2 \), then \( e \leq 3 \). For the special case of linear completely transitive codes [16], the analogous conjecture was solved in [3] and [4] proving that for \( e \geq 4 \) such nontrivial codes do not exist. Hence, the existing completely regular codes and completely transitive codes have an small error correcting capability. In respect of the covering radius, Solé in [16] uses the direct sum of \( \ell \) copies of fixed perfect binary 1-code of length \( n \) to construct infinite families of binary completely regular codes of length \( n \cdot \ell \) with covering radius \( \rho = \ell \). Thus, using [16], the covering radius of the resulting code is growing to infinity with the length of the code.

One of the main purpose in the current paper is to describe a method of constructing linear completely regular and completely transitive codes with arbitrary covering radius, which is constant when the length of the resulting code is growing to infinity. More exactly, for any prime power \( q \) and for any natural number \( \ell \) we give, in Theorem 1, an explicit construction of an infinite family of linear \( q \)-ary completely regular and completely transitive codes with lengths \( n = (q^m - 1)(q^\ell - 1)/(q - 1)^2 \) and with fixed covering radius \( \rho = \ell \), where \( m \geq \ell \) is any integer (a previous approach in this direction can be found in [15]). The intersection array for these completely regular codes is computed in Theorem 2.

Under the same conditions (i.e. for any prime power \( q \) and for any natural number \( \ell \)) we give the explicit construction of an infinite family of \( q \)-ary linear uniformly packed codes (in the wide sense) with lengths \( n = (\ell + 1)(q^m - 1)/(q - 1) \) and with covering radius \( \rho = \ell \), where \( m, \ell \geq 2 \) are any integers. All these codes (with the exception \( q = \ell = 2 \)) are not completely regular.

II. Preliminary results

For a given \( q \)-ary code \( C \) with covering radius \( \rho = \rho(C) \) define

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

We also use the following alternative standard definition of completely regularity [14].
Definition 3: A code $C$ 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 $C(l + 1)$. Also, define $a_l = (q - 1) \cdot n - b_l - c_l$ and note that $c_0 = b_0 = 0$. Refer to $(b_0, \ldots, b_{\rho - 1}; c_1, \ldots, c_{\rho})$ as the intersection array of $C$.

For a $q$-ary $[n, k, d]_q$-code $C$ with weight distribution $\mu(C) = (\mu_0, \ldots, \mu_n)$ define the outer distance $s = s(C)$ as the number of nonzero coordinates $\mu_i^\perp$, $i = 1, \ldots, n$ of the vector $(\mu_0^\perp, \ldots, \mu_n^\perp)$ obtained by the MacWilliams transform of $\mu(C)$ [8]. Hence, since $C$ is a linear code, $s(C)$ is the number of different nonzero weights of codewords in the dual code $C^\perp$.

Lemma 1 ([8]): For any code $C$ with covering radius $\rho(C)$ and with outer distance $s(C)$ we have $\rho(C) \leq s(C)$.

Lemma 2: Let $C$ be a code with minimum distance $d = 2e + 1$, covering radius $\rho$ and outer distance $s$. Then:

1) Code $C$ is uniformly packed in the wide sense if and only if $\rho = s$ ([2]).

2) If $C$ is completely regular then it is uniformly packed in the wide sense ([5]).

3) If $C$ is uniformly packed in the wide sense and $\rho = e + 1$, then it is completely regular ([18], [10]).

Let $C$ be a linear code of length $n$ over $\mathbb{F}_q$, a finite field of size a prime power $q$. Following [13], if $q = 2$, the automorphism group $Aut(C)$ of $C$ is a subgroup of the symmetric group $S_n$ consisting of all $n!$ permutations of the $n$ coordinate positions which send $C$ into itself.

Let $M$ be a monomial matrix, i.e. a matrix with exactly one nonzero entry in each row and column. If $q$ is prime, then $Aut(C)$ consists of all $n \times n$ monomial matrices $M$ over $\mathbb{F}_q$ such that $cM \in C$ for all $c \in C$. If $q$ is a power of a prime number, then $Aut(C)$ also contains all the field automorphisms of $\mathbb{F}_q$ which preserve $C$.

The group $Aut(C)$ induces an action on the set of cosets of $C$ in the following way: for all $\phi \in Aut(C)$ and for every vector $v \in \mathbb{F}_q^n$ we have $\phi(v + C) = \phi(v) + C$.

In [16] it was introduced the concept of completely transitive binary linear code and it can be generalized to the following definition, which also corresponds to the definition of coset-completely transitive code in [11].

Definition 4: Let $C$ be a linear code over $\mathbb{F}_q$ with covering radius $\rho$. Then $C$ is completely transitive if $Aut(C)$ has $\rho + 1$ orbits when acts on the cosets of $C$. 
Since two cosets in the same orbit should have the same weight distribution, it is clear that any completely transitive code is completely regular.

III. KRONECKER PRODUCT CONSTRUCTION

In this section we describe a new construction which provides for any natural number \( \rho \) and for any prime power \( q \) an infinite family of \( q \)-ary linear completely regular codes with covering radius \( \rho \).

Definition 5: For two matrices \( A = [a_{r,s}] \) and \( B = [b_{i,j}] \) over \( \mathbb{F}_q \) define a new matrix \( H \) which is the Kronecker product \( H = A \otimes B \), where \( H \) is obtained by changing any element \( a_{r,s} \) in \( A \) by the matrix \( a_{r,s}B \).

Consider the matrix \( H = A \otimes B \) and let \( C_A \) and \( C_B \) be the codes over \( \mathbb{F}_q \) which have, respectively, \( H \), \( A \) and \( B \) as a parity check matrices. Assume that \( A \) and \( B \) have size \( m_a \times n_a \) and \( m_b \times n_b \), respectively. For \( r \in \{1, \cdots, m_a\} \) and \( s \in \{1, \cdots, m_b\} \) the rows in \( H \) look as

\[
(a_{r,1}b_{s,1}, \cdots, a_{r,1}b_{s,n_b}, a_{r,2}b_{s,1}, \cdots, a_{r,2}b_{s,n_b}, \cdots, a_{r,2}b_{s,n_b}, \cdots, a_{r,n_a}b_{s,1}, \cdots, a_{r,n_a}b_{s,n_b}).
\]

Arrange these rows taking blocks of \( n_b \) coordinates as columns such that the vectors \( c \in C \) are presented as matrices of size \( n_b \times n_a \):

\[
c = \begin{bmatrix}
c_{1,1} & \cdots & c_{1,n_a} \\
c_{2,1} & \cdots & c_{2,n_a} \\
& \vdots & \vdots \\
c_{n_b,1} & \cdots & c_{n_b,n_a}
\end{bmatrix} = \begin{bmatrix}
c_1 \\
c_2 \\
\vdots \\
c_{n_b}
\end{bmatrix},
\]

(2)

where \( c_{i,j} = a_{r,j}b_{s,i} \) and \( c_r \) denotes the \( r \)-th row vector of this matrix.

We will call matrix representation the above way to present the vectors \( c \in C \).

Let us go to a further view on the codewords of \( C \), the code over \( \mathbb{F}_q \) which has \( H = A \otimes B \) as a parity check matrix. Consider vector \( c \in C \) and use the representation in (2), hence \( c = (c_1, c_2, \cdots, c_{n_b})^t \), where \((\cdot)^t\) means the transpose vector. Now compute the syndrome vector which leads us to a \( (m_b \times m_a) \) matrix that we will equal to zero. We have

\[
B(Ac_1^t, Ac_2^t, \ldots, Ac_{n_b}^t)^t = 0 \quad \text{and so,} \quad B(Ac^t)^t = B \cdot c \cdot A^t = 0.
\]

(3)

With this last property it is easy to note that any \( (n_b \times n_a) \) matrix with codewords of \( C_A \) as rows belong to the code \( C \) and also any \( (n_b \times n_a) \) matrix with codewords of \( C_B \) as columns belongs...
to the code $C$. Vice versa, all the codewords in $C$ can always be seen as linear combinations of matrices of both types above.

Moreover, it is straightforward to state the following well-known fact.

**Lemma 3**: Codes defined by the parity check matrices $A \otimes B$ and $B \otimes A$ are permutation equivalent.

From now on, we assume that matrix $A$ (respectively, $B$) is a parity check matrix of a Hamming code with parameters $[n_a, k_a, 3]_q$ (respectively, $[n_b, k_b, 3]_q$), where $n_a = (q^{m_a} - 1)/(q - 1) \geq 3$ (respectively, $n_b = (q^{m_b} - 1)/(q - 1) \geq 3$) and $k_a = n_a - m_a$ (respectively, $k_b = n_b - m_b$).

Denote by $H_m$ the parity check matrix of a perfect Hamming $[n, k, 3]_q$-code $C$ over $\mathbb{F}_q$, where $n = (q^m - 1)/(q - 1)$. Let $\xi_0 = 0, \xi_1 = 1, \ldots, \xi_{q-1}$ denote the elements of $\mathbb{F}_q$. Then the matrix $H_m$ can be expressed, up to equivalence, through the matrix $H_{m-1}$ as follows [17]:

$$H_m = \begin{bmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 & \cdots & \xi_{q-1} & \cdots & \xi_{q-1} & 1 \\ \hline H_{m-1} & H_{m-1} & \cdots & H_{m-1} & \cdots & H_{m-1} & \cdots & H_{m-1} & \cdots & H_{m-1} \\ \hline 0 & \cdots & 0 & 1 & \cdots & 1 & \cdots & \xi_{q-1} & \cdots & \xi_{q-1} & 1 \\ \end{bmatrix},$$

where $0$ is the zero column and where $H_1 = [1]$. Note that, under such construction, the following lemmas are straightforward (see, for example, [17]).

**Lemma 4**: Matrix $H_m$ contains as columns, among other, all the $m$ possible binary vectors of length $m$ and of weight 1.

**Lemma 5**: For $i = 1, \ldots, m$, let $r_i$ denote the $i$-th row of $H_m$. Let $g = \sum_{i=1}^m \xi_i r_i$, with $\xi_i \in \mathbb{F}_q$, be any linear combination of the rows of $H_m$. If $\text{wt}(g) \neq 0$, then $\text{wt}(g) = q^{m-1}$.

Throughout this work we will consider the columns in $A$ and $B$ ordered in such a way that the one-weighted vectors will be placed in the first $m_a$ (respectively, $m_b$) positions.

Any codeword $c \in C$, which has nonzero elements only in one row (or only in one column) will be called a **line**. Since $A$ and $B$ are parity check matrices of Hamming codes (i.e. they have minimum distances 3), there are lines of weight 3. For example, a row line $L_r = (\alpha_1, \alpha_2, \alpha_3)_{(s_1, s_2, s_3)}$ (respectively, a column line $L_s = (\alpha_1, \alpha_2, \alpha_3)_{(r_1, r_2, r_3)}$) means that the codeword $c$ of weight 3, whose nonzero $r$th row (respectively, nonzero $s$th column) has nonzero elements $\alpha_1, \alpha_2, \alpha_3$ in columns $s_1$, $s_2$, $s_3$ (respectively, in rows $r_1$, $r_2$, $r_3$). Recall that this means the following equality for the corresponding columns $a_{s_1}$, $a_{s_2}$, and $a_{s_3}$ of matrix.
A (respectively, for the columns \(b_{r_1}, b_{r_2}, \) and \(b_{r_3}\) of matrix \(B)\):

\[
\sum_{i=1}^{3} \mu_i a_{s_i} = 0 \quad \text{(respectively, } \sum_{j=1}^{3} \lambda_j b_{r_j} = 0). \tag{4}
\]

Define the set of row indices as \(R = \{1, \ldots, n_b\}\) (respectively, of column indices as \(S = \{1, \ldots, n_a\}\)) and assume that the first \(m_b\) indices (respectively, the first \(m_a\)) corresponds to the column vectors in \(A\) (respectively, in \(B)\) of weight one. By definition of perfect codes, for a fixed row index \(r \in R\) (respectively, column index \(s \in S)\), for any two nonzero elements \(\alpha_1, \alpha_2 \in \mathbb{F}_q\) and for any two different \(s_1, s_2 \in S\) (respectively, \(r_1, r_2 \in R)\) there is a unique row line \(L_r = (\alpha_1, \alpha_2, \alpha_3)_{s_1, s_2, s_3}\) (respectively, column line \(L_s = (\alpha_1, \alpha_2, \alpha_3)_{r_1, r_2, r_3}\)) for some nonzero element \(\alpha_3 \in \mathbb{F}_q\) and for some \(s_3 \in S\) (respectively, \(r_3 \in R)\).

It is well known that the linear span of the vectors of weight three in a Hamming code gives all the code. Hence, the linear span of the row lines of weight three and the column lines of weight three gives all the codewords of \(C\).

Given a vector \(v \in \mathbb{F}_q^{n_b \cdot n_a}\) let \(v = [v_{ij}]\) be its matrix representation. We will call main submatrix the \((m_b \times m_a)\) matrix containing the first \(m_b\) rows and \(m_a\) columns of the matrix representation. It is easy to see that, after simplifying (i.e. passing lines through the points placed out of the main submatrix), we can obtain a new vector \(v'\) in the same coset \(v + C\) such that its matrix representation has zero elements everywhere except into the main submatrix \(M_v\).

**Lemma 6:** Let \(v \in \mathbb{F}_q^{n_b \cdot n_a}\) be a vector and let \(M_v\) be its main submatrix representation. Then:

1) Vector \(v\) is in \(C\) if and only if \(M_v = 0\).

2) For each \(v\) the main submatrix representation \(M_v\) is unique.

**Proof:** First of all, take a nonzero \((m_b \times m_a)\) matrix \(M)\). Each column (respectively, row) is not a line, indeed, we would have a line \(L_r = (\alpha_1, \ldots, \alpha_{m_a})_{s_1, \ldots, s_{m_a}}\) involving only independent vectors of weight one, which is impossible. Hence, the conclusion is that it is impossible that such a nonzero main submatrix \(M\) is a codeword. Vice versa, given a vector \(v \in C\) and doing the simplification operations described above we will obtain a zero main submatrix representation.

The second point is a corollary of the first one.

Given a vector \(v \in \mathbb{F}_q^{n_b \cdot n_a}\) let \(v = [v_{ij}]\) be its matrix representation. Compute the syndrome \(S_v\) like in (3) which is a \((m_b \times m_a)\) matrix. Note that adding \((n_a - m_a)\) zero columns and
zero rows to this syndrome matrix we obtain the above main submatrix representation \( M_v \) for \( v \).

Hence, in other words:

**Lemma 7:** Given a vector \( v \in \mathbb{F}_{q^{n_b \cdot n_a}} \) let \( v = [v_{ij}] \) be its matrix representation. Then:

\[
(A \otimes B)(v) = S_v = B[v_{ij}]A^t = BM_vA^t
\]

Consider \( m_b \geq m_a \) (in the contrary case we will do the same but reverting the role of matrices \( A \) and \( B \)). Take a vector \( e \in \mathbb{F}_{q^{n_b \cdot n_a}} \) such that all the elements in the matrix representation are zeroes, except one. So, there are two specific values \( 1 \leq \lambda \leq n_b, 1 \leq \mu \leq n_a \) such that \( e = [e_{ij}] ; \quad e_{\lambda \mu} = e \) and \( e_{ij} = 0 \) for all \( i \neq \lambda \) and \( j \neq \mu \).

Using (4), we can pass a column line across the point \((\lambda, \mu)\) obtaining one or more aligned points in the first \( m_b \) rows. Again, passing row lines across these last points we obtain the main submatrix representation which is as follows:

\[
M_{\mu \otimes \lambda} = e \cdot \begin{bmatrix}
\mu_1 \lambda_1 & \mu_2 \lambda_1 & \cdots & \mu_{m_a} \lambda_1 \\
\mu_1 \lambda_2 & \mu_2 \lambda_2 & \cdots & \mu_{m_a} \lambda_2 \\
\vdots & \vdots & \ddots & \vdots \\
\mu_1 \lambda_{m_b} & \mu_2 \lambda_{m_b} & \cdots & \mu_{m_a} \lambda_{m_b}
\end{bmatrix},
\tag{5}
\]

where \( a_\mu = \sum_{i=1}^{m_a} \mu_i a_i ; \ b_\lambda = \sum_{i=1}^{m_b} \lambda_i b_{r_i} \) and \( a_i, b_{r_i} \) are the one weighted vectors of length \( m_a \) and \( m_b \), respectively.

**Remark 1:** Note that the first nonzero indexes in \( \{\mu_1, \mu_2, \cdots, \mu_{m_a}\} \) and \( \{\lambda_1, \lambda_2, \cdots, \lambda_{m_b}\} \) are \( \mu_{f_\mu} = 1 \) and \( \lambda_{f_\lambda} = 1 \), respectively.

It is important to point out that given a \((m_b \times m_a)\) matrix \( M \) the \( \text{rank}(M_{\mu \otimes \lambda} + M) \) differs from \( \text{rank}(M) \) in one unit, at the most.

**Proposition 1:** Let \( v \in \mathbb{F}_{q^{n_b \cdot n_a}} \) be a vector and \( M_v \) be its main submatrix representation. Then the distance of \( v \) to code \( C \) is \( d(v, C) = \text{rank}(M_v) \).

**Proof:** Let \( \text{rank}(M_v) = s \). Doing simplifications passing lines across the rows of \( M_v \) we will obtain a representation vector with nonzero elements in, at maximum, \( s \) columns. Again passing lines across these columns we obtain a representation matrix for the given vector \( v \) with not more that \( s \) nonzero coordinates. Hence, \( d(v, C) \leq s \).
Now, we are going to prove that $s \leq d(v, C)$. Consider the vector $c \in C$ with the same coordinates as $v$ and, moreover the new $d(v, C)$ coordinates that we need to add to $v$ to obtain that vector $c$ in $C$.

For each one of the coordinates $v_{ij}$ in which $v$ and $c$ differ we do the same consideration as in (5) and so, we see that the rank of the main submatrix representation of $v + v_{ij}$ differs from the previous in one unit, at the most. That is, after adding all the necessary coordinates to $v$ to obtain $c$, the rank of the main submatrix representation varied in, at the most, $d(v, C)$ units obtaining the final value of zero. Hence, the initial rank $s$ must be necessarily less or equal to $d(v, C)$.

The following theorem shows that the code constructed by the Kronecker product is a completely transitive code and, therefore, is a completely regular code.

**Theorem 1:** Let $C$ be the code over $\mathbb{F}_q$ which has $H = A \otimes B$ as a parity check matrix, where $A$ and $B$ are parity check matrices of Hamming codes $[n_a, k_a, 3]_q$ and $[n_b, k_b, 3]_q$, respectively, where $n_a = (q^{m_a} - 1)/(q - 1) \geq 3$; $n_b = (q^{m_b} - 1)/(q - 1) \geq 3$; $k_a = n_a - m_a$ and $k_b = n_b - m_b$. Then:

1) Code $C$ has length $n = n_a \cdot n_b$, dimension $k = n - m_a \cdot m_b$ and minimum distance $d = 3$.

2) The covering radius of $C$ is $\rho = \min\{m_a, m_b\}$.

3) Code $C$ is completely transitive and, therefore, a completely regular code.

**Proof:** It is straightforward to check that the code $C$ has length $n = n_a \cdot n_b$, dimension $k = n - m_a \cdot m_b$ and minimum distance $d = 3$.

In respect of the covering radius, take a vector $v \in \mathbb{F}_q^{n_a \cdot n_b}$ and use Proposition 1. Matrix $M_v$ is a $(m_b \times m_a)$ matrix, so this rank is an integer value from 0 to $\min(m_a, m_b)$.

To prove that $C$ is a completely transitive code it is enough to show that starting from two vectors $x, y \in C(\ell)$, there exists a monomial matrix $\phi \in Aut(C)$ such that $\phi(x) \in y + C$ or, in other words, $(A \otimes B)(\phi(x)) = (A \otimes B)(y)$.

First of all, let $\phi_1$ be any monomial $(n_a \times n_a)$ matrix and $\phi_2$ be any monomial $(n_b \times n_b)$ matrix. It is clear that

$$(A\phi_1) \otimes (B\phi_2) = (A \otimes B)(\phi_1 \otimes \phi_2)$$

and $\phi_1 \otimes \phi_2$ is a monomial $(n_a n_b \times n_a n_b)$ matrix. Moreover, we have that $Aut(A \otimes B) = Aut((A \otimes B)^\perp) = Aut(C)$ and so $Id \otimes \phi \in Aut(C)$. Hence, if $\phi$ is an automorphism in $Aut(B)$
then $Id \otimes \phi \in Aut(C)$.

The two given vectors $x, y$ belong to $C(\ell)$ and so, $rank(S_x) = rank(S_y)$, where $S_x$ and $S_y$ are the syndrome of $x$ and $y$, respectively. To prove that $C$ is a completely transitive code we will show that there exists an automorphism $\phi \in Aut(B)$ such that $(A \otimes B)(y) = (A \otimes B\phi)(x) = (A \otimes B)(\phi(x))$.

Assume $m_b \geq m_a$ (otherwise, we will do the same construction reverting $A$ and $B$). It is straightforward to find an invertible $(m_b \times m_b)$ matrix $K$ over $\mathbb{F}_q$ such that $S_x^t K = S_y^t$. Since $B$ is the parity check matrix of a Hamming code, the matrix $K^t B$ is again a parity check matrix for a Hamming code and $K^t B = B\phi$ for some monomial matrix $\phi$. Moreover, if $G_B$ is the corresponding generator matrix for this Hamming code, i.e. $BG_B^t = 0$, then $(B\phi)G_B^t = (K^t B)G_B^t = 0$ and so $\phi \in Aut(B)$.

Finally,

$$(A \otimes B)(y) = S_y = K^t S_x = K^t (Bx^t) = B\phi x^t A^t = (A \otimes B\phi)(x) = (A \otimes B)(\phi(x)).$$

The following goal is to compute the intersection array for this completely regular code $C$.

**Theorem 2:** Let $C_A$ and $C_B$ be two Hamming codes of parameters $[n_a, k_a, 3]_q$ and $[n_b, k_b, 3]_q$, respectively, where $n_a = (q^{m_a} - 1)/(q - 1) \geq 3$; $n_b = (q^{m_b} - 1)/(q - 1) \geq 3$ with dimension $k_a = n_a - m_a$ and $k_b = n_b - m_b$, respectively. Let $A$ (respectively, $B$) be a parity check matrix for the code $C_A$ (respectively, $C_B$). Then the matrix $H = A \otimes B$, the Kronecker product of $A$ and $B$, is a parity check matrix of a $q$-ary completely regular $[n, k, d]_q$-code $C$ with covering radius $\rho$, where

$$n = n_a \cdot n_b, \quad k = n - m_a \cdot m_b, \quad d = 3, \quad \rho = \min\{m_a, m_b\},$$

and with intersection numbers for $\ell = 0, 1, \ldots, \rho$:

$$b_\ell = (q - 1) \left( n_a - \frac{q^\ell - 1}{q - 1} \right) \left( n_b - \frac{q^\ell - 1}{q - 1} \right),$$

$$c_\ell = \frac{q^\ell - 1}{q - 1} q^{\ell - 1},$$

$$a_\ell = (q - 1) \cdot n_a \cdot n_b - c_\ell - b_\ell$$
Proof: Let $\mathbf{x} \in C(\ell)$ and $\mathbf{y} = \mathbf{x} + \mathbf{e}$, where $\mathbf{e}$ is a $(n_b \times n_a)$ matrix which has one nonzero position, say $e_{\lambda,\mu}$, where $\lambda \in R$, $\mu \in S$ and $e_{\lambda,\mu} = e \in \mathbb{F}_q^*$. 

As we said before, after doing simplifications we can always think that $\mathbf{x} = [x_{i,j}]$ has $\ell$ non zero positions at the main diagonal of value 1 and the corresponding $\ell$ column vectors $\mathbf{b}_j$ (respectively $\mathbf{a}_j$) are linear independent. Let $R_1$ be the set of these column vectors $\mathbf{b}_j$ (respectively, let $S_1$ be the set of these column vectors $\mathbf{a}_j$).

The case $\ell = 0$ follows immediately (any location of $e_{\lambda,\mu}$ contributes clearly only to the number $b_0$):

\[
a_0 = 0, \ b_0 = (q - 1) \cdot n_a \cdot n_b.
\]

Now consider the general case: $1 \leq \ell \leq \rho$.

First of all, assume that $\mathbf{e} = [e_{\lambda,\mu}]$ and that the vector $\mathbf{b}_\lambda$ is linearly independent from the vectors in $R_1$ (respectively, $\mathbf{a}_\mu$ is linearly independent from the vectors in $S_1$). The only contribution is $b_\ell$ and so it is easy to find that:

\[
b_\ell = (q - 1) \left( n_a - \frac{q^\ell - 1}{q - 1} \right) \left( n_b - \frac{q^\ell - 1}{q - 1} \right).
\]

Now, we are going to the case where $\mathbf{a}_\mu$ linearly depends from the set $S_1$ and $\mathbf{b}_\lambda$ from $R_1$. From (5) and Proposition 1 we can assume that $\mathbf{a}_\mu$ is linearly dependent from the vectors in $S_1$ and also $\mathbf{b}_\lambda$ from the vectors in $R_1$. So, $\mathbf{a}_\mu = \sum_{i=1}^{m_a} \mu_i \mathbf{a}_{i\mu}$; $\mathbf{b}_\lambda = \sum_{j=1}^{m_b} \lambda_j \mathbf{b}_{j\lambda}$ and $\mathbf{a}_\mu$, $\mathbf{b}_\lambda$ are the one weighted vectors of length $m_a$ and $m_b$, respectively.

We want to count in how many ways the following matrix has rank $\ell - 1$:

\[
Id_\ell + M_{\mu \otimes \lambda} = \begin{bmatrix}
1 + \mu_1 \lambda_1 e & \mu_2 \lambda_1 e & \cdots & \mu_\ell \lambda_1 e & \cdots & \mu_{m_a} \lambda_1 e \\
\mu_1 \lambda_2 e & 1 + \mu_2 \lambda_2 e & \cdots & \mu_\ell \lambda_2 e & \cdots & \mu_{m_a} \lambda_2 e \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\mu_1 \lambda_\ell e & \mu_2 \lambda_\ell e & \cdots & 1 + \mu_\ell \lambda_\ell e & \cdots & \mu_{m_a} \lambda_\ell e \\
\mu_1 \lambda_{\ell+1} e & \mu_2 \lambda_{\ell+1} e & \cdots & \mu_\ell \lambda_{\ell+1} e & \cdots & \mu_{m_a} \lambda_{\ell+1} e \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\mu_1 \lambda_{m_b} e & \mu_2 \lambda_{m_b} e & \cdots & \mu_\ell \lambda_{m_b} e & \cdots & \mu_{m_a} \lambda_{m_b} e
\end{bmatrix}
\]

(7)

If $\lambda_{f_\lambda} = \mu_{f_\mu} = 1$ (see Remark 1) are such that $f_\lambda > \ell$ or $f_\mu > \ell$ then the rank of the above matrix $Id_\ell + M_{\mu \otimes \lambda}$ would be greater than $\ell - 1$. Hence, we can transform the above matrix in
the following one, which has the same rank:

\[
\begin{array}{cccccc}
1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e & \mu_2 \lambda_1 e & \cdots & \mu_\ell \lambda_1 e & \cdots & \mu_m \lambda_1 e \\
0 & 1 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & \cdots & 0 \\
-\lambda_{\ell+1} e / \lambda_1 & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
-\lambda_m / \lambda_1 e & 0 & \cdots & 0 & \cdots & 0
\end{array}
\]

\[ (8) \]

It is easy to see that the rank of the above matrix is \( \ell - 1 \) plus the rank of \( P \), where

\[
P = \begin{bmatrix}
1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e & \mu_{\ell+1} \lambda_1 e & \cdots & \mu_m \lambda_1 e \\
-\lambda_{\ell+1} e / \lambda_1 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
-\lambda_m / \lambda_1 e & 0 & \cdots & 0
\end{bmatrix}
\]

\[ (9) \]

We are interested in to count in how many ways the rank of \( P \) is zero. It happens when all the \( \mu_i = 0 \) for \( \ell + 1 \leq i \leq m_a \), \( \lambda_i = 0 \) for \( \ell + 1 \leq i \leq m_b \), and \( 1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e = 0 \).

Now, note that when we fix a specific values for \( \lambda_1, \lambda_2, \ldots, \lambda_\ell \), with \( \lambda_{f_a} = 1 \) we want to count how many solutions \( (\mu_1, \mu_2, \ldots, \mu_m) \) has the equation \( 1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e = 0 \) with the restrictions \( \lambda_{f_a} = \mu_{f_a} = 1 \) (see Remark [1]).

We know that \( e \) is any value in \( \mathbb{F}_q^* \) and, on the other side, \( \mu_{f_a} = 1 \). Hence, each solution \( (\mu_1, \mu_2, \ldots, \mu_m) \) to the equation \( 1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e = 0 \) with the quoted restrictions could be transformed in to solution of \( 1 + \sum_{i=1}^{\ell} \mu_i \lambda_i = 0 \) without any restriction for \( \mu_{f_a} \).

Finally, given a specific values for \( \lambda_1, \lambda_2, \ldots, \lambda_\ell \), with \( \lambda_{f_a} = 1 \), our problem consist of counting how many solutions \( (\mu_1, \mu_2, \ldots, \mu_m) \) the equation \( 1 + \sum_{i=1}^{\ell} \mu_i \lambda_i e = 0 \) has, without any restriction for \( \mu_{f_a} \). It is easy to see that this value is \( q^{\ell-1} \).

Doing the above account for all the \( \frac{q^\ell - 1}{q - 1} \) possibilities when you choose the specific values for \( \lambda_1, \lambda_2, \ldots, \lambda_\ell \) we reach the statement.

**IV. Kronecker Product Construction of Uniformly Packed Codes**

The following theorem describes the explicit construction of infinite family of \( q \)-ary linear uniformly packed codes (in the wide sense) with fixed covering radius \( \rho \), where \( q \) is any prime
power, and where $\rho \geq 2$ is an arbitrary natural number. The interesting fact here is that these codes are not completely regular.

Recall that a trivial $q$-ary repetition $[n, 1, n]_q$-code is a perfect code, if and only if $q = 2$ and $n$ is odd.

**Theorem 3:** Let $C_A$ and $C_B$ be two linear codes: the repetition $[n_a, 1, n_a]_q$-code $C_A$ of length $n_a \geq 3$ and the $q$-ary perfect Hamming $[n_b, k_b, 3]_q$-code $C_B$ of length $n_b = (q^m - 1)/(q - 1) \geq q + 1$, where $n_a \leq n_b$. Let $A$ (respectively, $B$) be a parity check matrix of code $C_A$ (respectively, $C_B$). Then the matrix $H = A \otimes B$, the Kronecker product of $A$ and $B$, is a parity check matrix of a $q$-ary uniformly packed (in the wide sense) $[n, k, d]_q$-code $C$ with covering radius $\rho$, where

$$n = n_a \cdot n_b, \quad k = n - m \cdot (n_a - 1), \quad d = 3, \quad \rho = n_a - 1.$$

Furthermore, code $C$ is not completely regular with an exception for the case $q = 2$ and $n_b = 3$.

**Proof:** Let $a_i$ (respectively, $b_j$) denotes the $i$-th column of $A$ (respectively, the $j$-th column of $B$).

Remark that $A$ is a $(n_a - 1 \times n_a)$-matrix:

$$A = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 & -1 \\
0 & 1 & 0 & \cdots & 0 & -1 \\
0 & 0 & 1 & \cdots & 0 & -1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & -1
\end{bmatrix}.$$

Hence, the matrix $H = A \otimes B$ has a very simple structure:

$$H = \begin{bmatrix}
B & 0 & 0 & \cdots & 0 & -B \\
0 & B & 0 & \cdots & 0 & -B \\
0 & 0 & B & \cdots & 0 & -B \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & B & -B
\end{bmatrix},$$

where 0 denotes the zero matrix of size $m \times n_b$.

Any $q$-ary vector $x$ of length $n - k = m \cdot (n_a - 1)$ can be presented as follows: $x = (x_1 | \ldots | x_{n_a - 1})$ where $x_i$ is a $q$-ary vector of length $m$ for any $i = 1, \ldots, n_a - 1$. Matrix $B$ contains as columns, up to multiplicative scalar, any vector over $\mathbb{F}_q$ of length $n_b - k_b = m$. 

Hence for any $x_i$, $i = 1, \ldots, n_a - 1$ there is a column $b_{j_i}$ of $B$ such that $x_i^t = \xi_i b_{j_i}$ for some $\xi_i \in \mathbb{F}_q^*$. Since $a_i \otimes b_j$ is a column of $H$, and since $x_i^t$ can be written as $x_i^t = \sum_{i=1}^{n_a-1} \xi_i b_{j_i}$, we deduce that $\rho \leq n_a - 1$. To see that $\rho \geq n_a - 1$ it is enough to choose as a vector $x$ a vector with all nonzero mutually different component vectors $x_i$, $i = 1, \ldots, n_a - 1$. Such a choice is possible, since $q^m - 1 \geq n_b \geq n_a$. We conclude that $\rho = n_a - 1$.

Now we turn to the outer distance $s = s(C)$ of $C$ (i.e. the number of different nonzero weights of codewords in $C^\perp$).

Matrix $B$ is the parity check matrix of a Hamming code so, after Lemma 5, we conclude that all the nonzero linear combinations of the rows in $A$ have the same weight $q^{m-1}$.

Now consider any linear combination over $\mathbb{F}_q$ of rows of $H$. It is easy to see, by the shape of $H$ that the number of different nonzero weights go from $2 \cdot q^{m-1}$ until $n_a \cdot q^{m-1}$ so, the number of different nonzero values for the weight of the codewords in the code $C^\perp$ generated by the matrix $H$ is equal to $n_a - 1$. Hence, the outer distance $s(C)$ of $C$ is equal to $n_a - 1$ and so, $\rho(C) = s(C)$. Now, using Lemma 2, we conclude that the code $C$ is uniformly packed in the wide sense, i.e. in the sense of [1].

To finish the proof we have only to show that $C$ is not completely regular, with only one exception: when $A$ is the trivial binary repetition $[3, 1, 3]_2$-code which, at the same time, is the trivial Hamming code of length 3. But this last case (i.e. the case $q = 2$ and $n_b = 3$) is included in Theorem 2. Hence we have only to show that in all other cases the code $C$ is not completely regular.

Consider the next possible binary repetition code. When $n_a = 4$ and $\rho = 3$ we have the repetition $[4, 1, 4]_2$-code $C_A$. Choose as the code $C_B$ the binary Hamming $[7, 4, 3]_2$-code. We claim that the resulting $[28, 19, 3]_2$-code $C$ (after applying Theorem 3) is not a completely regular code. Let $H = A \otimes B$, i.e. $H$ looks as

$$
H = \begin{bmatrix}
B & 0 & 0 & B \\
0 & B & 0 & B \\
0 & 0 & B & B
\end{bmatrix},
$$
where $B$ is the following matrix:

$$B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$ 

Consider two different vectors $x_1$ and $x_2$ of weight 2, which belong to $C(2)$. Let

$$x_1 = (1000000|1000000|0000000|0000000)$$

and

$$x_2 = (1000000|0100000|0000000|0000000).$$

It is easy to see that both vectors $x_1$ and $x_2$ are from $C(2)$ and we obtain immediately the intersection numbers $c_2 = 4$ for $x_1$ and $c_2 = 2$ for $x_2$. Thus, code $C$ is not completely regular. Clearly the same contra-example works for $q = 2$ and for larger values $n_b \geq 5$.

For the cases $q \geq 3$ these above contra-examples should be slightly modified. For the smallest case $q = 3$ and $n_b = 3$ choose as the code $C_B$ the Hamming $[4,2,3]$ code with parity check matrix $B$ and let $A$ be a parity check matrix of the repetition $[3,1,3]$ code $C_A$, where $\mathbb{F}_3 = \{0,1,2\}$,

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \end{bmatrix}.$$ 

Take the following vectors $x_1$ and $x_2$ from $C(2)$:

$$x_1 = (1000|2000|0000) \quad \text{and} \quad x_2 = (1000|0100|0000).$$

We obtain the intersection numbers $c_2 = 4$ for $x_1$ and $c_2 = 2$ for $x_2$. Hence, the resulting $[12,8,3]$ code $C$ is not completely regular. The same contra-example works for the rest of cases $q \geq 3$ and $n_b \geq 3$.

Now, the proof of the theorem is complete.

**REFERENCES**

[1] L.A. Bassalygo, G.V. Zaitsev & V.A. Zinoviev, “Uniformly packed codes,” *Problems Inform. Transmiss.*, vol. 10, no. 1, pp. 9-14, 1974.

[2] L.A. Bassalygo & V.A. Zinoviev, “Remark on uniformly packed codes,” *Problems Inform. Transmiss.*, vol. 13, no. 3, pp. 22-25, 1977.
[3] J. Borges, J. Rifa, "On the Nonexistence of Completely Transitive Codes", *IEEE Trans. on Information Theory*, vol. 46, no. 1, pp. 279-280, 2000.

[4] J. Borges, J. Rifa & V.A. Zinoviev "Nonexistence of Completely Transitive Codes with Error-Correcting Capability e > 3", *IEEE Trans. on Information Theory*, vol. 47, no. 4, pp. 1619-1621, 2001.

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

[6] P. Charpin & V.A. Zinoviev, *On coset weight distributions of the 3-error-correcting BCH codes*, SIAM J. Discrete Math., vol. 10, No. 1, pp. 128-145, February 1997.

[7] G. Cohen, I. Honkala, S. Litsyn & A. Lobstein, *Covering Codes*, North-Holland, Elsevier, Amsterdam - Lausanne - New York - Oxford - Shannon - Tokyo, 1997.

[8] P. Delsarte, "An algebraic approach to the association schemes of coding theory," Philips Research Reports Supplements, vol. 10, 1973.

[9] J.M. Goethals & S.L. Snover, "Nearly perfect codes," *Discrete Math.*, vol. 3, pp. 65-88, 1972.

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

[11] M. Giudici, C.E. Praeger, "Completely Transitive Codes in Hamming Graphs", Europ. J. Combinatorics 20, pp. 647662, 1999.

[12] T. Helleseth, V.A. Zinoviev, *On coset weight distributions of the Z4-Linear Goethals Codes*, IEEE Trans. Inform. Theory, vol. 47, No. 5, pp. 1758-1772, 2001.

[13] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*. North-Holland, New York, 1977.

[14] A. Neumaier, "Completely regular codes," *Discrete Maths.*, vol. 106/107, pp. 335-360, 1992.

[15] J. Rifa, V. Zinoviev, "On the Kronecker product construction of completely transitive q-ary codes", Proceedings of 2nd International Castle Meeting on Coding Theory and Applications (2ICMCTA), LNCS 5228, pp. 163-170, 2008.

[16] P. Solé, "Completely Regular Codes and Completely Transitive Codes," *Discrete Maths.*, vol. 81, pp. 193-201, 1990.

[17] N.V. Semakov, V.A. Zinoviev & G.V. Zaitsev, "Class of maximal equidistant codes," *Problems of Information Transmission*, vol. 5, no. 2, pp. 84–87, 1969.

[18] N.V. Semakov, V.A. Zinoviev & G.V. Zaitsev, "Uniformly packed codes," *Problems Inform. Transmiss.*, vol. 7, no. 1, pp. 38-50, 1971.