Constructions of Binary Constant-Weight Quasi-Cyclic Codes and Quasicyclically Permutable Codes

Valdemar Cardoso da Rocha Jr., José Sampaio de Lemos-Neto and Maria de Lourdes Melo Guedes Alcoforado

***Abstract*—A theorem is proven showing how to obtain a constant-weight binary quasi-cyclic code from a p^r-ary linear cyclic code, where p is a prime and r is a positive integer, $r > 1$, by using a representation of the elements of a Galois field, $\mathrm{GF}(p^r)$, as cyclic shifts of a binary p^r-tuple. From this theorem, constructions are derived for two classes of constant-weight binary quasi-cyclic codes. These two classes are shown to achieve the Johnson upper bound on the number of codewords asymptotically for long blocklengths. A quasicyclically permutable (QCP) code is a binary code such that the codewords are quasicyclically distinct and have cyclic order equal to the code blocklength. A technique is described for selecting virtually the maximum number of cyclically distinct codewords of full cyclic order from Reed-Solomon (RS) codes and from Berlekamp-Justesen (BJ) codes, both known to be maximum distance separable codes. Those cyclically distinct codewords of full cyclic order from RS codes and from BJ codes are mapped to binary to produce two classes of asymptotically optimum constant-weight quasi-cyclic codes and two classes of asymptotically optimum constant-weight QCP codes. An application of QCP codes is introduced to construct protocol-sequence sets for the M-active-out-of-T users collision channel without feedback, allowing more users than strict cyclically permutable codes with the same blocklength and minimum distance.**

***Index Terms*—Cyclic codes, binary constant-weight quasi-cyclic codes, binary constant-weight quasicyclically permutable codes, collision channel without feedback.**

I. Introduction

This paper presents new constructions of constant-weight binary quasi-cyclic codes [1, p. 506] and introduces quasicyclically permutable (QCP) codes as a generalization of cyclically permutable (CP) codes. The usual practice in the coding literature is to refer to a *cyclic code* meaning a block code that is both *linear* and *invariant* to cyclic shifting of its codewords. In the sequel, and following [2], whenever we refer to a *cyclic code* we mean a block code that is invariant to a cyclic shift of any of its codewords. In order to avoid ambiguity, we call a *linear cyclic code* a block code which is linear and whose set of codewords is closed with respect to the operation of cyclic shifting of every codeword. By a *constant-weight* code we mean a block code whose codewords have the same Hamming weight. Consequently, every constant-weight binary cyclic code is a nonlinear code, except the trivial code containing only the all-zero codeword. Constant-weight codes find application in practice, for example, in visible light communication, random access communication and construction of protocol sequences for the collision channel without feedback [4], [7].

The problem of mapping non-binary block codes to binary block codes is relevant in practice and has been addressed earlier in the literature [1, pp. 298-301] - [3]. The main interest, however, concentrates on mapping non-binary cyclic codes to either binary cyclic codes or binary quasi-cyclic codes. By a *quasi-cyclic code* [1, p. 506] we mean a block code whose set of codewords is closed with respect to cyclic shifts of codewords by at least s positions, or integer multiples of s, where s is a positive integer, $s > 1$, and we call s the cyclic step of the code. If $s = 1$ such a block code is called a *cyclic code*. After an early attempt to obtain binary cyclic codes from non-binary cyclic codes MacWilliams [3] more or less discouraged further research on this problem. This situation changed later with the publication of [2], showing how to construct various classes of constant-weight binary cyclic codes from p-ary linear cyclic codes, where p is a prime, by employing a representation of the elements of $\mathrm{GF}(p)$ as cyclic shifts of a binary p-tuple. When a binary cyclic representation of $\mathrm{GF}(p)$ was introduced in [2] the authors remarked that only cyclic codes over $\mathrm{GF}(p)$, where p is a prime, can be mapped to binary cyclic codes because the additive group of $\mathrm{GF}(p)$ is cyclic. Furthermore, it is also remarked in [2] that this is not the case for cyclic codes defined over $\mathrm{GF}(p^r)$, where r denotes a positive integer, $r > 1$, because the additive group of $\mathrm{GF}(p^r)$ is not cyclic.

Another contribution of this paper is the construction of constant-weight QCP codes based on our constructions of constant-weight binary cyclic codes. A CP code was defined by Gilbert [8] to be a binary block code of blocklength N such that each codeword has N distinct cyclic shifts and such that no codeword can be obtained by the cyclic shifting, one or more times, of another codeword. As a natural generalization of CP codes we define a QCP code to be a binary code

Valdemar C. da Rocha Jr. and José Sampaio de Lemos-Neto are with the Communications Research Group, Department of Electronics and Systems, Federal University of Pernambuco, Recife, 50.740-550, PE, Brazil. (E-mails: {vcr, jose.lemosnt}@ufpe.br), ORCID: 0000-0002-1416-479X and 0009-0000-5636-694X.

Maria de Lourdes M. G. Alcoforado is with the Post-Graduate Program in Systems Engineering, Polytechnic School of Pernambuco, University of Pernambuco, Rua Benfica, 455, Recife, 50.720-001, PE, Brazil. E-mail: mlmga@poli.br, ORCID: 0000-0002-6311-1600.

Valdemar C. da Rocha Jr. acknowledges partial support of this work by the Brazilian National Council for Scientific and Technological Development (CNPq) - Grant No. 303790/2019-9 and Maria de Lourdes M. G. Alcoforado expresses her thanks to the Coordination for the Improvement of Higher Education Personnel (CAPES) - Finance Code 001, PVEX 88881.171292/2018-01.

Digital Object Identifier: 10.14209/jcis.2024.11

of blocklength N such that each codeword has N/s distinct cyclic shifts by s positions and such that no codeword can be obtained by the cyclic shifting by s positions or multiples of s of another codeword, i.e., such that the codewords are quasicyclically distinct and have cyclic order equal to the code blocklength.

II. A BINARY REPRESENTATION OF $\mathrm{GF}(p^r)$

Let $\mathbf{b}$ denote an N-tuple defined over an arbitrary finite alphabet, and let N be a positive integer. Let $S^{(i)}(\mathbf{b})$ denote a rightward cyclic shift of $\mathbf{b}$ by i positions. The *cyclic order* of an N-tuple $\mathbf{b}$ is defined as the least positive integer i such that $S^{(i)}(\mathbf{b}) = \mathbf{b}$. As a consequence the cyclic order of an N-tuple is always a divisor of N [2]. Thus, if p is a prime and r is a positive integer, $r \geq 1$, for $N = p^r$ an N-tuple can have cyclic order $1, p, p^2, \ldots, p^r$, only.

Two distinct N-tuples $\mathbf{b}$ and $\mathbf{b}'$, which are codewords in a quasi-cyclic code of cyclic step s, are said to be in the same *quasi-cyclic equivalence class* if $S^{(i)}(\mathbf{b}) = \mathbf{b}'$ for some i, $i = as$, $a \in \{1, 2, \ldots, (N/s) - 1\}$. If $\mathbf{b}$ has cyclic order N then the quasi-cyclic equivalence class containing $\mathbf{b}$ is defined as having order N/s and has a total of N/s N-tuples.

We consider next a binary representation of the elements of a Galois field, $\mathrm{GF}(p^r)$, that employs a binary p^r-tuple $\mathbf{v}$ of full cyclic order and its cyclic shifts, as explained in the sequel.

Definition 1. *For any binary p^r-tuple $\mathbf{v}$ having full cyclic order, we define the* binary $\mathbf{v}$-representation *of $\mathrm{GF}(p^r)$ as the representation in which the element γ_i of $\mathrm{GF}(p^r)$ is represented by the p^r-tuple $S^{(i)}(\mathbf{v})$, the i-th rightward cyclic shift of $\mathbf{v}$, $0 \leq i \leq p^{r-1} - 1$.*

Let $v(x)$ denote the polynomial representation of a p^r-tuple $\mathbf{v}$, i.e., $v(x)$ is a polynomial of degree at most $p^r - 1$ and its nonzero coefficients v_i, $0 \leq i \leq p^r - 1$, correspond to the respective nonzero entries $v_i = 1$ in $\mathbf{v}$. We denote by $v^{(i)}(x)$ a rightward cyclic shift of $v(x)$ by i places corresponding to $S^{(i)}(\mathbf{v})$, $0 \leq i \leq p^r - 1$, assuming $v^{(0)}(x) = v(x)$ and $S^{(0)}(\mathbf{v}) = \mathbf{v}$.

Lemma 1. *In the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$, where p is a prime, r is a positive integer, and $\mathbf{v}$ is a binary p^r-tuple of full cyclic order, the element γ_i of $\mathrm{GF}(p^r)$ is represented by the i-th rightward cyclic shift of $\mathbf{v}$, denoted as $S^{(i)}(\mathbf{v})$, $0 \leq i \leq p^{r-1} - 1$.*

Proof. The truth of this lemma is a consequence of the definition of the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$ and the fact that, for given values of p and r, there is at least one binary p^r-tuple of full cyclic order. For example, the binary p^r-tuple of Hamming weight 1. □

A. A theorem for constructing constant-weight binary quasi-cyclic codes

For the finite fields $\mathrm{GF}(p^r)$, where p is a prime and r is a positive integer, Reed-Solomon (RS) codes exist with blocklength n that divides $p^r - 1$, having k information digits and minimum Hamming distance $d = n - k + 1$, i.e., they are maximum distance separable (MDS) codes [1, pp. 294-301]. For the finite fields $\mathrm{GF}(q)$ where q is a power of 2, Berlekamp and Justesen (BJ) [13] have given constructions of q-ary Bose-Chaudhuri-Hocquenghem (BCH) codes of blocklength $n = q + 1$ that are MDS. An extension of their results to an arbitrary finite field was obtained later by da Rocha [14], and we will refer to them also as BJ codes.

Theorem 1. *Let p be a prime, let r be a positive integer and let $\mathbf{C}$ be a p^r-ary (n, k, d) linear cyclic code. Let each codeword $\mathbf{c} = [c_0, c_1, \ldots, c_i, \ldots, c_{n-1}]$ in $\mathbf{C}$ be represented by a binary word $\mathbf{b}$ of length $p^r n$, in a manner that c_i is replaced by a binary p^r-tuple of Hamming weight w in the binary $\mathbf{v}$-representation of the i-th component of $\mathbf{c}$, $0 \leq i \leq n - 1$ (see Definition 1). The set $\mathcal{B}$ of cardinality p^{rk}, containing the binary N-tuples $\mathbf{b}$ corresponding in this manner to the p^{rk} codewords $\mathbf{c} \in \mathbf{C}$, constitutes a binary quasi-cyclic code of blocklength $N = np^r$ and cyclic step $s = p^r$, whose p^{rk} codewords have constant-weight $w_c = nw$ and minimum distance $d_{\min}$ satisfying $d_{\min} \geq dd(\mathbf{v})$, with equality when the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$ is equidistant.*

Proof. Because $\mathbf{C}$ is linear and cyclic, a rightward cyclic shifting of a codeword $\mathbf{c}$ by produces a codeword in $\mathbf{C}$. It thus follows that the corresponding set of p^{rk} binary N-tuples $\mathbf{b}$ is closed with respect to the operation of rightward cyclic shifting by $s = p^r$ cyclic steps. Since all elements in the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$ have the same Hamming weight w, it follows that all N-tuples $\mathbf{b}$ have the same Hamming weight $w_c = nw$ and thus a constant-weight quasi-cyclic code with cyclic step $s = p^r$ results.

Comparing p^r-tuples in corresponding positions in two distinct binary codewords, $\mathbf{b}$ and $\mathbf{b}'$, obtained from two distinct p^r-ary codewords $\mathbf{c}$ and $\mathbf{c}'$, respectively, we conclude that at least $d(\mathbf{c}, \mathbf{c}')$ p^r-tuples are distinct, where $d(\mathbf{c}, \mathbf{c}')$ denotes the Hamming distance between $\mathbf{c}$ and $\mathbf{c}'$. It follows from the $\mathbf{v}$-representation that two p^r-tuples differ in at least $d(\mathbf{v})$ positions. Thus, two distinct binary codewords, $\mathbf{b}$ and $\mathbf{b}'$, will differ by at least $d(\mathbf{c}, \mathbf{c}')d(\mathbf{v})$ positions, with equality if the binary $\mathbf{v}$-representation is equidistant. Finally, we notice that $d(\mathbf{c}, \mathbf{c}') \geq d$, with equality for some codewords in $\mathbf{C}$. □

III. CONSTRUCTIONS OF CONSTANT-WEIGHT BINARY QUASI-CYCLIC CODES

As mentioned in Section II, a block code is called *quasi-cyclic* if there is some smallest positive integer s such that every s cyclic shifts applied to a codeword preserves the code, i.e., produces again a codeword [1, p. 506], and we call s the code cyclic step. If $s = 1$ the quasi-cyclic code is actually a cyclic code. The *cyclic minimum distance* of a quasi-cyclic code is defined as the minimum Hamming distance between a codeword and its own distinct cyclic shifts by steps of size s or some cyclic shift by steps of size s of another codeword.

Construction 1. *Let p be a prime and let r be a positive integer, $r \geq 1$. Let $\mathbf{C}$ be a p^r-ary linear cyclic (n, k, d) RS code of blocklength n, where n divides $p^r - 1$, having k information digits, $1 \leq k < n$, and minimum Hamming*

distance d. Let each codeword $\mathbf{c} = [c_0, c_1, \ldots, c_i, \ldots, c_{n-1}]$ in $\mathbf{C}$ be represented by a binary word $\mathbf{b}$ of length $p^r n$, in a manner that c_i is replaced by the binary p^r-tuple of Hamming weight $w = 1$ in the binary $\mathbf{v}$-representation of the i-th component of $\mathbf{c}$, $0 \leq i \leq n-1$ (see Definition 1 and Theorem 1). The set $\mathcal{B}$ of cardinality p^{rk}, containing the binary N-tuples $\mathbf{b}$ corresponding in this manner to the p^{rk} codewords $\mathbf{c} \in \mathbf{C}$, constitutes a binary quasi-cyclic code of blocklength $N = p^r n$, with cyclic step $s = p^r$, whose p^{rk} codewords have constant-weight $w_c = n$ and minimum distance $d_{\min}$ satisfying $d_{\min} = 2(n - k + 1)$.

Proof. The proof of the validity of this construction is entirely similar to the proof given for the validity of Theorem 1, and thus will be omitted. The minimum Hamming distance $d_{\min} = 2(n - k + 1)$ results because the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$ considered is equidistant with $d(\mathbf{v}) = 2$. □

Construction 2. *This construction is similar to* Construction 1 *except that code $\mathbf{C}$ is chosen to be a BJ code, i.e., the blocklength n is a divisor of $p^r + 1$.*

IV. Constructions of constant-weight binary quasicyclically permutable codes

A quasicyclically permutable (QCP) code of cyclic step s can equivalently be defined as a binary block code of blocklength $N = sz$, where z denotes a positive integer, such that each codeword has cyclic order N and lies in a distinct quasi-cyclic equivalence class containing z N-tuples. The *cyclic minimum distance*, d_c, of a QCP code is defined as the minimum Hamming distance between a codeword and its own distinct cyclic shifts by steps of size s or some cyclic shift by steps of size s of another codeword. It turns out that d_c coincides with the minimum Hamming distance, $d_{\min}$, of the binary code the codebook of which consists of all N-tuples belonging to the quasi-cyclic equivalence classes of the QCP code.

A convenient result published in Peterson & Weldon [10, p. 387] is revisited next and adapted to select virtually the maximum number of cyclically distinct codewords of full cyclic order from a p^r-ary linear cyclic code. Our proof however follows along the lines employed to prove Theorem 2 in [11].

Theorem 2. *Let p be a prime and let r be a positive integer $r \geq 1$. Let $\mathbf{C}$ denote a (n, k, d) p^r-ary linear cyclic code with generator polynomial $g(x)$, where n divides $p^r - 1$. Let $h(x) = (x - \beta)f(x)$, where β is a root with multiplicative order n in $\mathrm{GF}(p^r)$ and $h(x) = (x^n - 1)/g(x)$. Every codeword $c(x) \in \mathbf{C}$ has the form $c(x) = i(x)g(x)$, where $i(x)$ is a polynomial of degree less than k. By restricting $i(x)$ to have the form $i(x) = 1 + (x - \beta)m(x)$, where $m(x)$ denotes a message polynomial of degree less than $k - 1$, the $p^{r(k-1)}$ codewords in the subset generated by $c'(x) = (1 + (x - \beta)m(x))g(x)$ are cyclically distinct and have full cyclic order.*

Proof. Suppose a codeword $c'(x) = (1 + (x - \beta)m(x))g(x)$ has cyclic order i, $1 \leq i \leq n$, i.e.,

$$x^i c'(x) = c'(x) \bmod (x^n - 1),$$

or, equivalently,

$$(x^i - 1)c'(x) = 0 \bmod (x^n - 1). \tag{1}$$

Substituting $(1 + (x - \beta)m(x))g(x)$ for $c'(x)$ in (1) it follows that

$$(x^i - 1)(1 + (x - \beta)m(x))g(x) = 0 \bmod g(x)h(x), \tag{2}$$

which is equivalent to

$$(x^i - 1)(1 + (x - \beta)m(x)) = 0 \bmod h(x), \tag{3}$$

obtained from (2) after division by $g(x)$, or, equivalently,

$$(x^i - 1)(1 + (x - \beta)m(x)) = 0 \bmod (x - \beta)f(x). \tag{4}$$

Because $\gcd(1 + (x - \beta)m(x), (x - \beta)) = 1$, the remainder obtained by dividing the lefthand side in (4) by $x - \beta$ can, equivalently, be written as

$$x^i - 1 = 0 \mod (x - \beta). \tag{5}$$

Moreover, by hypothesis β has multiplicative order n in $\mathrm{GF}(p^r)$ and thus the smallest value of i for which (5) is satisfied is $i = n$. Therefore, the codewords in the subset generated by $c'(x) = (1 + (x - \beta)m(x))g(x)$ have full cyclic order. Since $x - \beta$ is a monomial, we conclude that the number of full cyclic order codewords selected is $p^{r(k-1)}$ because $m(x)$ has degree less than $k - 1$. In order to show that codewords selected in this manner are cyclically distinct, let $c'_1(x) = (1 + (x - \beta)m_1(x))g(x)$ and $c'_2(x) = (1 + (x - \beta)m_2(x))g(x)$, $m_1(x) \neq m_2(x)$, be two distinct codewords in $\mathbf{C}$ and assume that they lie in the same cyclic equivalence class, i.e.,

$$x^i c'_2(x) = c'_1(x) \bmod (x^n - 1), \tag{6}$$

for some value of i, $0 < i < n$. Replacing $c'_1(x)$ by $(1 + (x - \beta)m_1(x))g(x)$ and $c'_2(x)$ by $(1 + (x - \beta)m_2(x))g(x)$ in (6) and simplifying, we obtain

$$x^i - 1 + (x - \beta)(x^i m_2(x) - m_1(x)) = 0 \bmod h(x). \tag{7}$$

Because $h(x)$ is divisible by $x - \beta$, the remainder obtained after dividing the lefthand side in (7) by $x - \beta$ can, equivalently, be written as

$$x^i - 1 = 0 \mod (x - \beta). \tag{8}$$

For (8) to be satisfied $x - \beta$ must divide $x^i - 1$. However, this is impossible because β has multiplicative order n in $\mathrm{GF}(p^r)$ and i is less than n, i.e., $0 < i < n$. Thus, (8) is not satisfied and we conclude that codewords $c'_1(x)$ and $c'_2(x)$ can not lie in the same cyclic equivalence class and are therefore cyclically distinct. □

Construction 3. *Let p be a prime, let r be a positive integer, $r \geq 1$, and let $\mathbf{C}$ be a p^r-ary (n, k, d) RS code, where the blocklength n divides $p^r - 1$, having k information digits, $2 \leq k < n$, and minimum Hamming distance d. Select in $\mathbf{C}$ a subset $\mathbf{C}'$ of codewords $c(x) = (1 + (x - \beta)m(x))g(x)$ of full cyclic order as described in Theorem 2, represented in vector*

form as $\mathbf{c} = [c_0, c_1, \ldots, c_i, \ldots, c_{n-1}]$. *Let each codeword* $\mathbf{c}$ *in* $\mathbf{C}'$ *be represented by a binary word* $\mathbf{b}$ *of length* $p^r n$, *in a manner that* c_i *is replaced by the binary* p^r*-tuple of Hamming weight* $w = 1$ *in the binary* $\mathbf{v}$*-representation of the* i*-th component of* $\mathbf{c}$, $0 \leq i \leq n-1$ *(see Definition 1 and Theorem 2). Then the set* $\mathcal{B}$ *containing* $p^{r(k-1)}$ *binary* N*-tuples* $\mathbf{b}$, *corresponding in this manner to the* $p^{r(k-1)}$ *codewords of* $\mathbf{C}'$, *is a constant-weight* $w_c = n$, (N, M_c, d_c) *QCP code with cyclic step* $s = p^r$, $M_c = p^{r(k-1)}$ *and minimum Hamming distance* $d_c = 2(n-k+1)$.

Proof. As we discussed earlier it suffices to show that each N-tuple in $\mathcal{B}$ has cyclic order $N = np^r$ and that the $p^{r(k-1)}$ N-tuples in $\mathcal{B}$ are distinct when cyclically shifted in steps of size $s = p^r$. Let $\mathbf{c}$ be the codeword in the subset $\mathbf{C}'$ corresponding to $\mathbf{b}$. We note that $\mathbf{c}^* = S^{(i)}(\mathbf{c})$ represents i rightward cyclic shifts of $\mathbf{c}$ and corresponds to the codeword $\mathbf{b}^* = S^{(ip^r)}(\mathbf{b})$, $1 \leq i \leq n$, i.e., a rightward cyclic shift of $\mathbf{b}$ by ip^r steps. Thus, $\mathbf{b}$ has cyclic order $N = p^r n$ and belongs to a quasi-cyclic equivalence class in $\mathcal{B}$ containing n entries. The minimum Hamming distance $d_c = 2(n-k+1)$ results because the binary $\mathbf{v}$-representation of $\mathrm{GF}(p^r)$ considered is equidistant with $d(\mathbf{v}) = 2$.

We show next that the codewords in $\mathcal{B}$ are quasicyclically distinct or, equivalently, if $\mathbf{b} \in \mathcal{B}$, $\mathbf{b}' \in \mathcal{B}$ and $\mathbf{b} \neq \mathbf{b}'$, then $S^{(ip^r)}(\mathbf{b}') \neq \mathbf{b}$, for $1 \leq i < n$. Denoting by polynomials $b'(x)$ and $b(x)$ the codewords $\mathbf{b}'$ and $\mathbf{b}$ in $\mathcal{B}$, respectively, suppose that

$$x^{ip^r} b'(x) = b(x) \mod (x^N - 1), \tag{9}$$

which corresponds to

$$x^i c'(x) = c(x) \mod (x^n - 1), \tag{10}$$

recalling that the codewords in $\mathbf{C}'$ are cyclically distinct and their mapping into binary codewords is reversible. Therefore, equality in (10) will hold only for $i = n$ (see Theorem 2), which implies $b'(x) = b(x)$ in (9), i.e., $\mathbf{b}' = \mathbf{b}$. Thus, the codewords in $\mathcal{B}$ are quasicyclically distinct and form a QCP code of blocklength $N = p^r n$, with cyclic step $s = p^r$. This completes the proof of the validity of *Construction 3*.

□

Construction 4. *This construction is similar to* Construction 3 *except that code* $\mathbf{C}$ *is chosen to be a BJ code, i.e., the blocklength* n *is a divisor of* $p^r + 1$.

V. Efficiency of the code constructions presented

The essential difference between the codes of *Construction 1* and *Construction 2* is that the latter codes are two p^r-ary digits longer when n is chosen as large as possible for the same p^r. The quasi-cyclic codes given by *Construction 1* with $n = p^r - 1$ and by *Construction 2* with $n = p^r + 1$ are *asymptotically optimum* constant-weight codes in the sense that, for fixed k, they meet the Johnson upper bound [1, Corollary 5, p. 527], with equality as $p \to \infty$, as explained next. For a given even number d, the Johnson upper bound states that

$$A(N, d, w) \leq \prod_{i=0}^{w-d/2} \frac{N-i}{w-i}, \tag{11}$$

and since the minimum distance of a constant-weight binary code is always even, the requirement of even d does not represent a restriction.

The QCP codes given by *Construction 3* with $n = p^r - 1$ and by *Construction 4* with $n = p^r + 1$ are *asymptotically optimum* constant-weight codes in the sense that, for fixed k, they meet the RS code upper bound and the BJ code upper bound, respectively, on the number of distinct cyclic equivalence classes with equality as $p \to \infty$, as explained next.

As well known, for an (n, k, d) cyclic code over a p^r-ary alphabet the ratio p^{rk}/n gives an upper bound on the number of distinct cyclic equivalence classes. Moreover, by considering $n = p^r - 1$ in *Construction 3* it follows that, for the resulting binary quasi-cyclic codes, an upper bound on the number of distinct cyclic equivalence classes is given by the ratio $p^{rk}/(p^r - 1)$, which asymptotically approaches $p^{r(k-1)}$ for large p and fixed k. Similarly, by considering $n = p^r + 1$ in *Construction 4* it follows that, for the resulting binary quasi-cyclic codes, an upper bound on the number of distinct cyclic equivalence classes is given by the ratio $p^{rk}/(p^r + 1)$, which asymptotically approaches $p^{r(k-1)}$ for large p and fixed k.

A. Construction 1

For an (n, k, d) RS code over $\mathrm{GF}(p^r)$ with $n = p^r - 1$ we have $N = p^r(p^r - 1)$, $w = p^r - 1$, $d = 2(p^r - k)$ and the righthand side of the Johnson upper bound in (11) gives

$$\begin{aligned} A(N, d, w) &= \prod_{i=0}^{k-1} \frac{p^r(p^r-1) - i}{(p^r-1) - i} = \prod_{i=0}^{k-1} \frac{p^r - i/(p^r-1)}{1 - i/(p^r-1)} \\ &= p^{rk}(1 + O(p)), \end{aligned}$$

where $O(p) \to 0$ as $p \to \infty$. The codes of *Construction 1* have precisely p^{rk} codewords and therefore can be said to be *asymptotically optimum* with respect to the Johnson upper bound.

B. Construction 2

Using an argument similar to that employed in subsection V-A, the codes in *Construction 2* with $n = p^r + 1$ can be said to be *asymptotically optimum* in the same sense.

C. Construction 3

For an (n, k, d) RS code $\mathbf{C}$ over $\mathrm{GF}(p^r)$ with $n = p^r - 1$ an upper bound on the number of distinct cyclic equivalence classes selected from $\mathbf{C}$ is $p^{rk}/n = p^{rk}/(p^r - 1) \approx p^{r(k-1)}$, for large p and fixed k. The QCP codes of *Construction 3* have $p^{r(k-1)}$ codewords and therefore can be said to be *asymptotically optimum* for large p and fixed k.

D. Construction 4

Using an argument similar to that employed in subsection V-C, the codes in *Construction 4* with $n = p^r + 1$ can be said to be *asymptotically optimum* in the same sense.

VI. New Protocol-Sequence Sets

Constant-weight CP codes were shown to provide a natural solution to an interesting random-accessing problem in [2]. In this section we show that constant-weight QCP codes also contribute a natural solution to this random-accessing problem, extending what was already known when CP codes were employed.

The binary quasi-cyclic codes produced from MDS cyclic codes in Section III were used in Section IV to construct QCP codes where subsets of codewords are considered as protocol sequences for the users of a collision channel without feedback [16]. Tsybakov [17] and Pinsker [18] formulated the random-accessing problem where in each received frame at most M out of the total T of users can be active in the sense of sending at least one packet in this frame. The set of T binary sequences of length N, $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_T\}$, is said to be a (T, M, N, σ) protocol-sequence set if each frame-active user can be identified by the receiver and at least σ of the packets transmitted by each frame-active user are sent without collision, when these sequences are used as protocol sequences for the T users and provided that at most M of the users are active in each received frame. Theorem 4 in Reference [2] was originally proved regarding constant-weight CP codes, i.e., it shows how constant-weight CP codes can be used as (T, M, N, σ) protocol-sequence sets, but its proof remains valid when we consider instead constant-weight QCP codes, and is restated as follows.

Theorem 3. *For any integer σ with $1 \leq \sigma \leq w$, a binary constant-weight w QCP code $(N, M_c = T, d_c)$ is a (T, M, N, σ) protocol-sequence set for M satisfying the condition*

$$M = \min\{T, \lfloor (w-1)/(w-d_c/2) \rfloor, \lfloor (w-\sigma)/(w-d_c/2) \rfloor + 1\}. \tag{12}$$

The coding of packets is next briefly examined, i.e., how the users can code their packets so that each user can send σ information packets in each frame of his activity and the receiver can correctly decode these packets. Each user employs an $(n' = w, k' = \sigma, d' = w - \sigma + 1)$ shortened RS code over $\mathrm{GF}(Q)$ to code his σ information packets into his w transmitted packets. Such a code exists provided only that $w \leq Q + 1$ when we use doubly-extended RS codes [9, p. 221]. If a user is frame-active and has σ successful packet transmissions, the decoding problem at the receiver is equivalent to having erasures in the at most $w - \sigma$ positions where this user's packets suffer collisions. Because $d' = w - \sigma + 1$, the receiver can always correct these erasures by a standard erasure-correcting algorithm for the RS code and hence, can correctly recover the σ information packets from this user. Because a (T, M, N, σ) protocol-sequence set allows each of the M active users to send σ information packets successfully in a frame of N slots when the users code their packets as described earlier, it follows that R_{sum}, the total information transmission rate that can be achieved, is

$$R_{\text{sum}} = (M\sigma)/N(\text{packets/slot}). \tag{13}$$

Example 1. *Taking $p = 13$, $r = 2$, $n = 170$ and $k = 3$ in Construction 4 yields a binary, constant-weight $w = 170$, QCP code $(N = 28730, M_c = 28561, d_c = 340)$. By Theorem 3, this code can be used as a $(T = 28561, M, N = 28730, \sigma = 60)$ protocol-sequence set for $M = \min\{28561, 84, 55\} = 55$. In other words, provided that at most $M = 55$ out of the $T = 28561$ users are active in each received frame of $N = 28730$ slots, each frame-active user will be guaranteed at least $\sigma = 60$ collision-free packet transmissions among the $w = 170$ packets that he sends in a frame. A sum rate of*

$$R_{sum} = (55 \times 60)/28730 = 330/2873 \approx 0.11 \quad (\textit{packets/slot})$$

can be achieved.

VII. Conclusion

The code constructions presented in this paper can be seen as complementary to the code constructions presented in [2]. The constant-weight binary quasi-cyclic codes introduced here are asymptotically optimum relative to the Johnson upper bound on the number of codewords in *Construction 1* and *Construction 2*. Regarding binary QCP codes, by Theorem 2, for fixed k and $p \to \infty$, *Construction 3* and *Construction 4* are asymptotically optimum because their respective number of quasicyclically equivalence classes is equal to the upper bound on the corresponding number of distinct cyclic equivalence classes for the RS code and the BJ code, respectively. Consequently, for the same blocklength and minimum distance, binary constant-weight QCP codes have more codewords than the binary constant-weight CP codes given by Construction V and Construction VI in [2]. The practical application of QCP codes to construct protocol-sequence sets for the M-active-out-of-T users collision channel without feedback allows more users than those protocol-sequence sets obtained when strict cyclically permutable codes with the same blocklength and minimum distance are employed.

We hope the reader will be challenged to advance other code constructions based on Theorem 1 by exploring different choices of the sequence $\mathbf{v}$ used in the $\mathbf{v}$-representation of the elements of $\mathrm{GF}(p^r)$ and by different choices of the p^r-ary linear cyclic code $\mathbf{C}$. As an application of constant-weight QCP codes, we have considered their use as protocol-sequence sets for the M-active-out-of- T-users collision channel without feedback but expect other applications will be found regarding problems of an essentially asynchronous nature.

References

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

[2] N. Q. A, L. Györfi and J. L. Massey,"Constructions of Constant-Weight Binary Cyclic Codes and Cyclically Permutable Codes", *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 940-949, 1992, doi: 10.1109/18.135636.

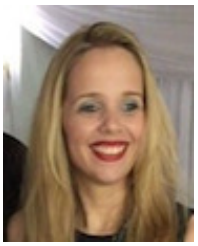
[3] F. J. MacWilliams, "On Binary Cyclic Codes Which are also Cyclic Codes Over $\mathrm{GF}(2^s)$", *SIAM Journal on Applied Mathematics*, vol. 19, no. 1, pp. 75-95, 1970, http://www.jstor.org/stable/2099332.

[4] S. H. Lee, M. Zhang and J. K. Kwon, "Bit Error Probability Performance of Binary Dimmable Visible Light Communication Systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9118-9131, 2021, doi: 10.1109/TVT.2021.3100587.

[5] H. A. Inan, S. Ahn, P. Kairouz and A. Ozgur, "A Group Testing Approach to Random Access for Short-Packet Communication," *IEEE Int. Symp. Inf. Theory* (ISIT), pp. 96 -100, Paris, France, 2019, doi: 10.1109/ISIT.2019.8849823.
[6] Y. Zhang, Y. -H. Lo, W. S. Wong and F. Shu, "Protocol Sequences for the Multiple-Packet Reception Channel Without Feedback," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1687-1698, 2016, doi: 10.1109/TCOMM.2016.2538259.
[7] V. C. da Rocha Jr., "Protocol Sequences for Collision Channel Without Feedback", *IET Electronics Letters*, vol. 36, no. 10, pp. 2010 - 2012, 2000, doi: 10.1049/el:20001427.
[8] E. N. Gilbert, "Cyclically Permutable Error-Correcting Codes", *IEEE Trans. Inf. Theory*, vol. 9, no. 3, pp. 175-182, 1963, doi: 10.1109/TIT.1963.1057840.
[9] R. E. Blahut, *Theory and Practice of Error Control Codes*, Reading. MA, Addison-Wesley, 1984.
[10] W. W. Peterson and E. J. Weldon Jr.: *Error-Correcting Codes*, MIT Press, 2nd edition, 1972.
[11] J. S. Lemos-Neto and V. C. da Rocha, Jr.: "Cyclically Permutable Codes Specified by Roots of Generator Polynomials", *IET Electron. Lett.*, vol. 50, no. 17, pp. 1202 - 1204, 2014, doi: 10.1049/el.2014.0296.
[12] V. C. da Rocha, Jr. and J. S. Lemos-Neto, "New Cyclically Permutable Codes", IEEE Inf. Theory Workshop, ITW-2011, pp. 693-697, 2011, doi: 10.1109/ITW.2011.6089586.
[13] E. R. Berlekamp and J. Justesen, "Some Long Cyclic Linear Binary Codes are not so Bad," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 351-356, 1974, doi: 10.1109/TIT.1974.1055222.
[14] V. C. da Rocha, Jr., "Maximum Distance Separable Multilevel Codes," *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 547-548, 1984, doi: 10.1109/TIT.1984.1056909.
[15] J. L. Massey, "The Capacity of the Collision Channel Without Feedback," Abstracts of Papers, *IEEE Int. Symp. Inf. Theory* (ISIT), p. 101, Les Arcs, France, 1982.
[16] J. L. Massey and P. Mathys, "The Collision Channel Without Feedback," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 192-204, 1985, doi: 10.1109/TIT.1985.1057010.
[17] B. S. Tsybakov and N. B. Likhanov, "Packet Communication on a Channel Without Feedback," Probl. Inform. Transm., vol. XIX, no. 2, pp. 69-84, 1983.
[18] L. A. Bassalygo and M. S. Pinsker, "Limited Multiple-Access of a Non-Synchronous Channel," (in Russian) Probl. Inform. Transm., vol. XIX, no. 4, pp. 92-96, 1983.

Valdemar Cardoso da Rocha Jr. was born in Jaboatão, Pernambuco, Brazil, on August 27, 1947. He received his BSc degree in electrical and electronics engineering from Escola Politécnica, Recife, Brazil, in 1970, and his PhD degree in electronics from the University of Kent, England, in 1976. In 1976, he joined the faculty of the Federal University of Pernambuco, Recife, Brazil, founded the Electrical Engineering Postgraduate Program, and since 1993 is Professor of Telecommunications. He has been a consultant to the Brazilian Ministry of Education, the Ministry of Science and Technology, and the Ministry of Defense on postgraduate education and research in electrical engineering. He was Chairman of the Electrical Engineering Committee in the Brazilian National Council for Scientific and Technological Development for two terms. He is a founding member, former President, and Emeritus Member of the Brazilian Telecommunications Society. He is also a Life Senior Member of the IEEE Communications Society and the IEEE Information Theory Society. He is a former Member of the IEEE Alexander Graham Bell Medal Committee and from 1992 to 2022 he was a Fellow of the Institute of Mathematics and its Applications. He has been a Visiting Professor at various institutions, including the Swiss Federal Institute of Technology-Zurich, the University of Leeds and Lancaster University. He has published over 100 engineering and scientific papers, including journal and conference papers, and the books Elements of Algebraic Coding Systems, Momentum Press, 2014, Principles of Applied Digital Information Theory (in Portuguese), Interciencia, 2018, and is a co-author of the book Communication Systems (Springer, 2022, 3rd Edition).

José Sampaio de Lemos Neto was born in Bezerros, Pernambuco, Brazil, on November 27, 1980. He received the B.Sc. (2004), M.Sc. (2011) and D.Sc. (2015) degrees, all in electrical and electronics engineering from the Federal University of Pernambuco, Recife, Brazil. In 2015 he joined the faculty of the Federal University of Pernambuco, Recife, Brazil, as an Associate Professor. He was a research assistant in the project "Cryptographic Security Based on Noisy Physical Elements" developed by Dr. D. P. B. A. Camara and supervised by Prof. V. C. da Rocha, Jr.. He joined in the Brazilian Telecommunications Society in 2010. His professional experience includes research and teaching. Dr. Lemos-Neto's research interests are in applied digital information theory, error-correcting codes, digital communications, digital signal processing and applied mathematics.



Maria de Lourdes Melo Guedes Alcoforado received her B.Sc. degree in electrical and electronics Engineering (1995), M.Sc. (2000) and D.Sc. degrees (2005) in Electrical Engineering from the Federal University of Pernambuco, Brazil. She was a researcher (2013-2016) in the project entitled Coding and Security Advanced Techniques for Wideband Wireless Communications, involving the School of Computing and Communications, Lancaster University and the Communications Research Group, Federal University of Pernambuco. Since 2001 she is with the University of Pernambuco, dedicated to researching and teaching in Undergraduate and Post Graduate courses. She was the Coordinator of the Post Graduate Program in Systems Engineering (2016-2021) and currently she is a Sector Coordinator for Post Graduate Studies and Research at the Polytechnic School of Pernambuco. Her research interests include polar codes, turbo codes, multiple access channel, modulation and cryptography.