Códigos constacíclicos, códigos ciclicamente permutáveis e sequências de protocolo para o canal de colisão sem realimentação

J. S. Lemos-Neto e Valdemar C. da Rocha Jr.

***Resumo*— O primeiro objetivo deste artigo é propor um novo conjunto de códigos ciclicamente permutáveis (códigos CP), derivados de códigos constacíclicos p-ários, usando um método de construção existente na literatura. Para isto, dois novos teoremas são enunciados e uma nova construção de códigos CP é obtida. Tal construção é ótima no sentido que atinge precisamente o limitante superior para o número de classes de equivalência constacíclica. O segundo objetivo deste artigo é avaliar o desempenho da nova construção de códigos CP quando aplicada na construção de sequências de protocolo para o canal de colisão sem realimentação.**

***Palavras-Chave*— Códigos constacíclicos, códigos ciclicamente permutáveis, canal de colisão sem realimentação, sequências de protocolo.**

***Abstract*— The first objective of this paper is to propose a new class of cyclically permutable codes (CPC) which are derived from a known construction of p-ary constacyclic codes. Two new theorems are proved which lead to the construction of a new class of CPC. The proposed construction is optimum in the sense that it achieves the upper bound for the number of constacyclic equivalence classes. As a second objective, the proposed CPC construction is used to generate protocol sequences for the collision channel without feedback and their suitability is assessed for this application.**

***Keywords*— Constacyclic codes, cyclically permutable codes, collision channel without feedback, protocol sequences.**

I. INTRODUÇÃO

O primeiro objetivo deste artigo é propor um novo conjunto de códigos ciclicamente permutáveis (códigos CP) [1], derivados de códigos constacíclicos p-ários [2, p. 303], usando o método de construção apresentado em [3]. Para isto, dois novos teoremas são apresentados. No primeiro, dado um código constacíclico $\mathcal{C}$ gerado pelo polinômio $g(x)$, prova-se uma condição para as raízes de $g(x)$ tal que todas as palavras-código não-nulas de $\mathcal{C}$ possuam ordem constacíclica plena. No segundo, mostra-se como particionar $\mathcal{C}$ em classes de equivalência constacíclica, desde que o polinômio $g(x)$ satisfaça a condição proposta no primeiro teorema. Após particionar $\mathcal{C}$, cada palavra-código de uma classe de equivalência constacíclica distinta é mapeada para binário, seguindo o procedimento proposto em [3], e uma nova construção de códigos CP é obtida. Tal construção é ótima no sentido que atinge precisamente o limitante superior para o número de classes de equivalência constacíclica.

O canal de colisão sem realimentação (CCsR) tem sido um tema de pesquisa recorrente desde sua publicação [4], [5]. Trabalhos recentes sobre o CCsR podem ser vistos nas referências [6]–[8]. Assim, o segundo objetivo deste artigo é avaliar o desempenho da construção de códigos CP proposta como sequências de protocolo para o CCsR. Os parâmetros de desempenho das sequências propostas são comparados aos de outras sequências que seguem uma abordagem semelhante de construção [6], [9], [10].

O restante deste artigo está organizado conforme descrito na sequência. Na Seção II são abordados alguns conceitos de códigos constacíclicos e dois resultados originais são apresentados. Na Seção III, apresenta-se um novo conjunto de códigos ciclicamente permutáveis derivado dos resultados apresentados na Seção II, juntamente com o procedimento descrito em [3] para mapear as palavras de um código constacíclico p-ário para binário. Na Seção IV, um cenário de aplicação dos códigos CP construídos na Seção III é exposto: códigos CP como sequências de protocolo para o CCsR. Por fim, as conclusões são apresentadas na Seção V.

José Sampaio de Lemos Neto e Valdemar C. da Rocha Jr., Grupo de Pesquisa em Comunicações - CODEC, Departamento de Eletrônica e Sistemas, UFPE, Recife, CEP 50740-550. E-mails: {jose.lemosnt, vcr}@ufpe.br. Este trabalho recebeu apoio parcial do CNPq, Proj. 307467/2015-5 e da Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), Proj. IBPG-0288-0.34/10.

II. CÓDIGOS CONSTACÍCLICOS

A. Conceitos básicos

Seja $c(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}$ um polinômio cujos coeficientes pertencem a $\mathrm{GF}(p)$, em que p denota um número primo ímpar. Multiplicar $c(x)$ por x e reduzir o produto módulo $x^n - a$, sendo a um elemento não-nulo de $\mathrm{GF}(p)$, resulta no polinômio $c'(x) = ac_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1}$. Diz-se que $c'(x)$ corresponde a um deslocamento *constacíclico* de $c(x)$ para a direita [2, p. 303]. Assim, um código $\mathcal{C}$ é dito ser constacíclico se qualquer deslocamento constacíclico de uma palavra-código resulta em uma palavra-código.

Neste artigo, o interesse é na construção de códigos constacíclicos de comprimento $n = p + 1$, sendo p um número primo tal que $p > 3$, e com o elemento a de $x^n - a$ sendo um elemento gerador do grupo multiplicativo de $\mathrm{GF}(p)$. Esta escolha deve-se ao fato de que algumas propriedades são conhecidas para códigos constacíclicos com esses parâmetros [11]. Uma descrição da existência de códigos constacíclicos para outros valores de n e a pode ser encontrada em [12].

Para $n = p + 1$, é conhecido [11] que as raízes de $x^{p+1} - a$ pertencem a $\mathrm{GF}(p^2)$ e podem ser escritas na forma

$\alpha^{1+(p-1)i}$, para $0 \leq i \leq p$, ou ainda na forma $\alpha^{p+(p-1)i}$, para $-(p-1)/2 \leq i \leq (p+1)/2$. De acordo com [11], o polinômio $x^{p+1}-a$ é fatorado em $(p+1)/2$ polinômios de grau dois. Logo, as raízes de $x^{p+1}-a$ pertencem a classes conjugadas de cardinalidade dois [13]. Uma consequência deste fato é que o grau dos possíveis polinômios geradores $g(x)$ é um número par, isto é, $n-k$ sempre é par. Como $n=p+1$ também é par, a dimensão do código, k, sempre é um número par no intervalo $2 \leq k \leq p-1$.

Ainda em [11], mostra-se que as raízes de $x^{p+1}-a$ são termos consecutivos de uma progressão geométrica de razão α^{p-1}. Assim é possível escolher um polinômio gerador $g(x)$ de um código constacíclico $\mathcal{C}$ com $2t$ raízes consecutivas, em que t é a capacidade de correção de $\mathcal{C}$. Desta forma, $\mathcal{C}$ tem $d_{\min}=n-k+1$ e é um código *maximum distance separable* (MDS) [14, p. 188].

Por fim, a ordem constacíclica de uma palavra-código é o menor inteiro positivo i tal que $x^i c(x) = c(x) \mod (x^n-a)$. Quando $i=p^2-1$, $c(x)$ possui *ordem constacíclica plena*.

B. Condição para as raízes do polinômio gerador

O Teorema 1, apresentado a seguir, estabelece uma condição sobre as raízes de $g(x)$ que permite gerar códigos constacíclicos de comprimento de bloco $n=p+1$, tal que todas as palavras-código não-nulas possuam ordem constacíclica plena. Seja o polinômio $x^{p+1}-a$, em que p é um número primo, $p>3$, e $a \neq 0$ é um elemento gerador do grupo multiplicativo de $\mathrm{GF}(p)$. Esta condição imposta sobre a assegura que pelo menos um par de raízes conjugadas de $x^{p+1}-a$ tenha ordem multiplicativa p^2-1 [11].

Teorema 1: Todas as palavras-código não-nulas de um código $\mathcal{C}$ constacíclico linear p-ário $(p+1, k, d_{\min})$ possuem ordem constacíclica plena se, e somente se, todas as raízes do polinômio $x^{p+1}-a$ que não têm ordem multiplicativa igual a p^2-1 são escolhidas como raízes do polinômio gerador $g(x)$.

Demonstração: Suponha que todas as raízes de $x^{p+1}-a$ que possuem ordem multiplicativa diferente de p^2-1 estão em $g(x)$. Para que qualquer $c(x) \in \mathcal{C}$ tenha ordem constacíclica plena, o menor valor de i tal que

$$x^i c(x) \quad = \quad c(x) \bmod (x^{p+1}-a)$$

ou, equivalentemente,

$$(x^i-1)c(x) \quad = \quad 0 \bmod (x^{p+1}-a) \qquad (1)$$

tem de ser $i=p^2-1$. Entretanto, pode-se escrever $c(x) = m(x)g(x)$ e substituir $c(x)$ por $m(x)g(x)$ em (1). Logo,

$$(x^i-1)m(x)g(x) \quad = \quad 0 \bmod (x^{p+1}-a). \qquad (2)$$

A condição expressa em (2) implica que todas as raízes do polinômio $x^{p+1}-a$ estão presentes em $(x^i-1)m(x)g(x)$. O polinômio $m(x)$ possui grau máximo $k-1$ e, portanto, poderá ter no máximo $k-1$ raízes com ordem multiplicativa p^2-1. Como grau$[m(x)g(x)] \leq p$, no mínimo uma raiz de x^i-1 terá ordem multiplicativa p^2-1. Consequentemente, $i=p^2-1$ é o valor mínimo para que (2) seja satisfeita e, portanto, todas as palavras-código não-nulas de $\mathcal{C}$ possuem ordem constacíclica plena.

Por outro lado, suponha que todas as palavras-código não nulas de $\mathcal{C}$ possuem ordem constacíclica plena, ou seja, p^2-1 é o menor valor de i que satisfaz (2). Pelos mesmos argumentos já expostos, no mínimo uma raiz de $x^{p+1}-a$ é comum a x^i-1 em (2). Se esta raiz comum, denotada por α^{i_1}, tiver ordem multiplicativa $i_2 < p^2-1$, tal que $\alpha^{i_1 i_2} = \alpha^{p^2-1} = 1$, então (2) é satisfeita para $i=i_2$. Porém, isto implica que pelo menos uma palavra-código possui ordem constacíclica $i_2 < p^2-1$. Como isto não é possível, dada a hipótese assumida que $i=p^2-1$ é o menor valor para o qual (2) é satisfeita, então qualquer raiz com ordem multiplicativa $i < p^2-1$ deve estar no conjunto de raízes de $m(x)$ ou de $g(x)$. Uma vez que o polinômio $m(x)$ pode conter ou não raízes em $\mathrm{GF}(p^2)$, o único modo de garantir a hipótese assumida é que todas as raízes com ordem multiplicativa $i < p^2-1$ devem estar no conjunto de raízes de $g(x)$. ■

Neste ponto, vale ressaltar que para se construir códigos constacíclicos que sejam MDS e que possuam todas as palavras-código com ordem constacíclica plena, as raízes do polinômio $g(x)$ devem satisfazer duas condições: a) serem consecutivas e b) satisfazer o Teorema 1.

C. Classes de equivalência constacíclica

Conforme justificado na sequência, é possível particionar um código constacíclico em *classes de equivalência constacíclica* de modo semelhante ao que foi feito com códigos cíclicos em [15]. Neste caso, considere duas palavras-código $c_1(x)$ e $c_2(x)$ pertencentes a um código constacíclico p-ário $\mathcal{C}$ cujas palavras-código são reduzidas $\mathrm{mod}(x^{p+1}-a)$. Diz-se que $c_1(x)$ e $c_2(x)$ pertencem à mesma classe de equivalência constacíclica se $x^i c_1(x) = c_2(x) \bmod (x^{p+1}-a)$ para $1 \leq i < p^2-1$. Se $c_1(x)$ tem ordem constacíclica igual a j, então a classe de equivalência constacíclica que contém $c_1(x)$ possui j palavras-código, que correspondem aos deslocamentos constacíclicos de $c_1(x)$, e a classe de equivalência constacíclica, da qual $c_1(x)$ agora é denominado *líder*, também tem ordem constacíclica igual a j

O Teorema 2, apresentado a seguir, mostra como obter diretamente cada palavra-código líder de classe de equivalência constacíclica. Em outras palavras, o Teorema 2 provê um modo direto de particionar um código constacíclico em suas respectivas classes de equivalência constacíclica.

Teorema 2: Seja $n=p+1$ e seja $\mathcal{C}$ um código linear constacíclico p-ário $(n, k, d_{\min})$ cujo polinômio gerador $g(x)$ satisfaz o Teorema 1, e seja $h(x)$ o polinômio de verificação de paridade, em que $h(x) = \prod_{j=1}^{k/2} s_j(x)$, e cada $s_j(x)$, $1 \leq j \leq k/2$, tem grau 2 e pertence ao expoente p^2-1, i.e., p^2-1 é o menor número inteiro positivo n para o qual $s_j(x)$ divide x^n-1. As palavras-código não nulas $c(x) \in \mathcal{C}$ são constaciclicamente distintas se elas são selecionadas tal que

$$c(x) = g(x)[1+s_i(x)m_i(x)] \prod_{j=1}^{i-1} s_j(x) \mod x^n - a, \quad (3)$$

em que a é um elemento gerador de $\mathrm{GF}(p)$, $1 \leq i \leq k/2, m_i(x)$ é um polinômio mensagem de grau no máximo $k-1-2i \geq 0$, para $1 \leq i \leq k/2-1$, e $m_{k/2}(x) \triangleq 1$.

O número de classes de equivalência constacíclica gerado por (3) é precisamente $(p^k-1)/(p^2-1)$.

Demonstração: O teorema é provado em três partes. Nas duas primeiras partes prova-se que as palavras-código geradas por (3) são constaciclicamente distintas e, na terceira e última parte, mostra-se quantas classes de equivalência constacíclica são geradas.

Na primeira parte, considere $c(x)$ em (3) para $1 \leq i \leq k/2-1$. Neste caso, sejam $c_1(x) = g(x)[1+s_i(x)m_i(x)]\prod_{j=1}^{i-1} s_j(x)$ e $c_2(x) = g(x)[1+s_l(x)m'_l(x)]\prod_{j=1}^{l-1} s_j(x)$, $1 \leq l \leq k/2-1$, duas palavras-código distintas em $\mathcal{C}$, em que $s_i(x)m_i(x)$ e $s_l(x)m'_l(x)$ possuem grau no máximo igual a $k-1$. Por hipótese, se $c_1(x)$ e $c_2(x)$ pertencem à mesma classe de equivalência constacíclica, então

$$x^t c_1(x) = c_2(x) \bmod x^n - a \tag{4}$$

é satisfeita para algum valor de t tal que $0 < t < p^2-1$.

- Para $i = l$, após algumas simplificações em (4), obtém-se

$$x^t - 1 + s_i(x)[x^t m_i(x) - m'_i(x)] = 0 \bmod s_i(x). \tag{5}$$

  Para (5) ser satisfeita, $s_i(x)$ deve ser um fator de x^t-1, mas isso não é possível visto que $s_i(x)$ pertence ao expoente p^2-1 e $0 < t < p^2-1$. Assim, a hipótese que $c_1(x)$ e $c_2(x)$ pertencem a mesma classe de equivalência constacíclica é falsa para $i = l$ e, portanto, $c_1(x)$ e $c_2(x)$ pertencem a classes de equivalência constacíclica distintas.
- Para $i \neq l$, com $l > i$, após algumas simplificações em (4), obtém-se

$$x^t\,[1+s_i(x)m_i(x)] - [1+s_l(x)m'_l(x)]\prod_{j=i}^{l-1} s_j(x) \tag{6}$$

  igual a 0 módulo $s_l(x)\prod_{j=i}^{l-1} s_j(x)$.
  Para (6) ser satisfeita, $\prod_{j=i}^{l-1} s_j(x)$ deve dividir $x^t\,[1+s_i(x)m_i(x)]$. Como

$$\gcd\left[x^t, \prod_{j=i}^{l-1} s_j(x)\right] = 1,$$

  e uma vez que $\gcd[1+s_i(x)m_i(x), s_i(x)] = 1$, conclui-se que $1+s_i(x)m_i(x)$ não é divisível por $\prod_{j=i}^{l-1} s_j(x)$, pois este último tem $s_i(x)$ como fator. Assim, a hipótese que $c_1(x)$ e $c_2(x)$ pertencem à mesma classe de equivalência constacíclica é falsa para $i \neq l$ e, portanto, $c_1(x)$ e $c_2(x)$ pertencem a classes de equivalência constacíclica distintas.

Na segunda parte, considere $c(x)$ em (3) para $i = k/2$. Sendo $m_{k/2}(x) = 1$, obtém-se

$$c(x) = g(x)\prod_{j=1}^{k/2-1} s_j(x) + g(x)\prod_{j=1}^{k/2} s_j(x) \mod x^n - a.$$

Entretanto, $h(x) = \prod_{j=1}^{k/2} s_j(x)$ e $g(x)h(x) = 0 \mod x^{p^2-1}-1$. Logo,

$$c(x) = g(x)\prod_{j=1}^{k/2-1} s_j(x) \tag{7}$$

para $i = k/2$. Observe que (7) é independente do polinômio $m_{k/2}(x)$, assim, por definição, $m_{k/2}(x) = 1$. De modo direto, pode-se verificar que a classe de equivalência constacíclica gerada por $c(x) = g(x)\prod_{j=1}^{k/2-1} s_j(x)$ não foi gerada previamente por $c(x)$ em (3) para $1 \leq i \leq k/2-1$. A classe de equivalência constacíclica gerada por $g(x)\prod_{j=1}^{k/2-1} s_j(x)$ é obtida diretamente pela divisão do polinômio $x^{p^2-1}-a$ pelo polinômio $s_{k/2}(x)$.

Na terceira e última parte, considere o número total de classes de equivalência constacíclica geradas. Para $1 \leq i \leq k/2-1$ em (3), o grau de $m_i(x)$ é menor ou igual a $k-1-2i$. Logo, existem p^{k-2i} possíveis escolhas para $m_i(x)$. Consequentemente, o número de classes de equivalência constacíclica neste caso é dado por $\sum_{i=1}^{k/2-1} p^{k-2i}$. Para $i = k/2$ em (3), uma única classe de equivalência constacíclica é gerada. Desta forma, o número total de classes de equivalência constacíclica distintas é dado por $\sum_{i=1}^{k/2-1} p^{k-2i} + 1 = \sum_{i=1}^{k/2} p^{k-2i}$. Mas, $\sum_{i=1}^{k/2} p^{k-2i}$ é a soma de $k/2$ termos de uma série geométrica finita de razão p^{-2}. Assim, $\sum_{i=1}^{k/2} p^{k-2i} = \frac{p^k-1}{p^2-1} = (p^k-1)/(p^2-1)$. ■

Exemplo 1: Considere $p = 5$ e $a = 3$. Logo, $x^6-3 = (3+2x+x^2)(3+x^2)(3+3x+x^2)$ sobre GF(5). Os polinômios $3+2x+x^2$ e $3+3x+x^2$ pertencem ao expoente 24, enquanto o polinômio $3+x^2$ pertence ao expoente 8. Assim, considere o código $\mathcal{C}$ gerado por $g(x) = 3+x^2$. Como $n = 6$ e $n-k = 2$, então $k = 4$. Uma vez que $g(x)$ satisfaz o Teorema 1, pode-se aplicar o Teorema 2 a $\mathcal{C}$. Neste caso $k/2 = 2$ e, desta forma, $h(x) = \prod_{j=1}^{2} s_j(x) = s_1(x)s_2(x)$, em que $s_1(x) = 3+2x+x^2$ e $s_2(x) = 3+3x+x^2$, por exemplo. Para $i = 1$,

$$c(x) = g(x)[1+s_1(x)m_1(x)], \tag{8}$$

em que grau$[m_1(x)] \leq 4-1-2 = 1$. Assim, $5^2 = 25$ classes de equivalência constacíclica são geradas. Para $i = 2$, $m_2(x) = 1$ por definição, assim

$$\begin{aligned} c(x) &= g(x)[1+s_2(x)]s_1(x) \mod x^6-3 \\ &= g(x)s_1(x) \end{aligned} \tag{9}$$

e, assim, uma classe de equivalência constacíclica é obtida. Portanto, $(5^4-1)/(5^2-1) = 26$ classes de equivalência constacíclica são geradas por meio de (8) e (9).

III. Códigos ciclicamente permutáveis

Um código ciclicamente permutável (código CP) é um código de bloco binário de comprimento N em que cada palavra-código tem ordem cíclica plena e tal que as palavras-código são ciclicamente distintas [1]. Um código CP de comprimento de bloco N, com M_c palavras-código e distância mínima cíclica d_c é denotado por CCP(N, M_c, d_c) [9].

Para se obter um código CP usando as palavras-código p-árias obtidas por meio do Teorema 2, é preciso mapear as

palavras-código para binário. Em [3], mostra-se como mapear adequadamente as palavras-código de um código constacíclico p-ário em palavras de um código CP. Tal procedimento consiste, resumidamente, nos seguintes passos:

i. Escolha uma representação-$\mathbf{V}$ para os elementos de $\mathrm{GF}(p)$ do seguinte modo: os elementos não-nulos a^i, $i = 0, 1, 2, \ldots, p-2$, são representados pelas $(p-1)$-uplas binárias $\mathbf{S}^i(\mathbf{v})$, em que $\mathbf{v}$ é uma $(p-1)$-upla binária cuja ordem cíclica é igual a $p-1$ e $\mathbf{S}^i$ denota o operador que desloca ciclicamente $\mathbf{v}$ de i posições para a direita. Além disso, o elemento 0 pode ser representado pela $(p-1)$-upla binária não-nula $\mathbf{v}'$ e seus deslocamentos cíclicos tais que $\mathbf{v}' \neq \mathbf{S}^i(\mathbf{v})$ para $0 \leq i \leq p-2$. Em particular, $\mathbf{v}'$ pode ser escolhida como a $(p-1)$-upla toda nula. Os pesos de Hamming de $\mathbf{v}$ e $\mathbf{v}'$ são denotados por $w(\mathbf{v})$ e $w(\mathbf{v}')$ respectivamente;

ii. Cada palavra-código p-ária $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, obtida por meio do Teorema 2, é mapeada em um arranjo bidimensional cujas colunas são as transpostas das $(p-1)-$uplas binárias, definidas pela representação-$\mathbf{V}$, para cada coordenada c_i, $0 \leq i \leq n-1$;

iii. Os arranjos bidimensionais são convertidos adequadamente em N-uplas binárias, de modo que um deslocamento constacíclico de $\mathbf{c}$ corresponda a um deslocamento cíclico de sua respectiva N-upla binária.

Construção 1: Seja p um número primo, $p > 3$, $n = p+1$ e k um número par tal que $4 \leq k \leq p-1$. Escolha uma representação-$\mathbf{V}$ com $\mathbf{v} = (1, 0, 0, \ldots, 0)$ e $w(\mathbf{v}') \geq 3$, e um código $\mathcal{C}$ constacíclico linear p-ário $(p+1, k, p-k+2)$ (MDS) cujo polinômio gerador $g(x)$ satisfaz o Teorema 1. Mapeando para binário cada palavra-código $c(x)$ selecionada de acordo com o Teorema 2, obtém-se um $CCP(N, M_c, d_c)$ com $N = p^2 - 1$, $M_c = (p^k - 1)/(p^2 - 1)$ e com distância mínima cíclica $d_c \geq (p-k+2)d(\mathbf{v})$.

Para um código linear constacíclico p-ário $\mathcal{C}$ com comprimento de bloco $n = p+1$ e cujo polinômio gerador $g(x)$ satisfaz o Teorema 1, o número de classes de equivalência constacíclica distintas é igual a $(p^k - 1)/(p^2 - 1)$. Assim, $(p^k - 1)/(p^2 - 1)$ é o limitante superior para o número de classes de equivalência constacíclica que podem ser geradas neste caso. A Construção 1 tem $M_c = (p^k - 1)/(p^2 - 1)$, portanto, ela é ótima no sentido de que atinge precisamente o limitante superior.

IV. Aplicação: Sequências de protocolo para o canal de colisão sem realimentação

O canal de colisão sem realimentação (CCsR) é um modelo de canal proposto [4], [5] para situações em que um dado número de usuários compartilha o mesmo canal de comunicação para o envio de pacotes de *bits*. No CCsR cada usuário possui uma sequência de protocolo que determina em quais intervalos de tempo o usuário pode enviar seus pacotes. Em [9], demonstra-se que códigos CP constituem uma solução natural para o caso particular de acesso múltiplo no CCsR em que M usuários, de um total de U, estão ativos em um dado quadro. Nesta situação, cada usuário recebe uma palavra-código distinta de um mesmo código CP e a utiliza como sequência de protocolo para controlar suas transmissões. Desta forma, as palavras do código CP constituem um conjunto (U, M, N, σ) de sequências de protocolo, em que U denota o total de usuários que compartilham o canal, M denota o número de usuários ativos por quadro, cujo comprimento é denotado por N, e σ denota o número mínimo de pacotes por quadro que podem ser recebidos livres de colisão. A taxa máxima total de informação obtida nesta situação é dada por

$$R_{\mathrm{sum}} = \frac{M\sigma}{N} \quad \text{(pacotes/intervalo de tempo).} \tag{10}$$

Teorema 3 ([6]): Seja CCP$(N, M_c = U, d_c)$ um código CP de peso não-constante, de valor mínimo $w_{\min}$ e valor máximo $w_{\max}$. Para um número inteiro σ, $1 \leq \sigma \leq w_{\max}$, um CCP$(N, M_c = U, d_c)$ é um conjunto de sequências de protocolo, representadas por (U, M, N, σ), para

$$M \geq \min\left\{U, \left\lfloor \frac{w_{\min} - 1}{w_{\max} - d_c/2} \right\rfloor, \left\lfloor \frac{w_{\min} - \sigma}{w_{\max} - d_c/2} \right\rfloor + 1 \right\}, \tag{11}$$

em que $\lfloor x \rfloor$ é o maior número inteiro positivo tal que $\lfloor x \rfloor \leq x$.

A. Sequências-Constacíclicas baseadas na Construção 1

De acordo com a Construção 1, os parâmetros (U, M, N, σ) das sequências baseadas em códigos CP de peso não-constante são $U = (p^k - 1)/(p^2 - 1), N = p^2 - 1$ e M em função de σ é dado por

$$M \geq \min\left\{U, \left\lfloor \frac{w_{\min} - 1}{w_{\max} - d_c/2} \right\rfloor, \left\lfloor \frac{w_{\min} - \sigma}{w_{\max} - d_c/2} \right\rfloor + 1 \right\}, \tag{12}$$

em que p é um número primo tal que $p \geq 5$ e k é um número inteiro par tal que $4 \leq k \leq p-1$. As sequências de protocolo são palavras de um código CP, de peso não-constante, com $w_{\min} = p+1$, $w_{\max} = (p-k+2) + (k-1)w(\mathbf{v}')$ e $d_c \geq (p-k+2)d(\mathbf{v})$, em que $w(\mathbf{v}')$, $w(\mathbf{v}') \geq 3$, denota o peso da $(p-1)$-upla que representa o elemento 0 na representação-$\mathbf{V}$ e $d(\mathbf{v})$ denota sua distância mínima.

B. Comparação das Sequências de Protocolo

De acordo com [6], a avaliação de sequências de protocolo não é simples e o resultado depende, em geral, da natureza da aplicação pretendida. No entanto, os seguintes parâmetros são comumente considerados.

a) O número de usuários, M, ativos por quadro;
b) A taxa total de informação transmitida (R_{sum});
c) O número máximo de sequências distintas;
d) O comprimento do quadro, N, utilizado pelos usuários;
e) Suporte a usuários com diferentes fatores de trabalho;
f) Uso de cabeçalhos de identificação dos usuários.

Em [6], foram apresentadas as Sequências-Constacíclicas, tipo-I e tipo-II, e foi realizada uma comparação entre elas e as Sequências-RS e Sequências-BCH. Portanto, resta apenas comparar as sequências baseadas na Construção 1, proposta neste artigo. A Tabela I é uma versão atualizada da Tabela I em [6], com a inclusão das sequências baseadas na Construção 1, e resume os parâmetros utilizados na comparação.

As sequências de protocolo baseadas na Construção 1 são obtidas por meio de códigos CP, logo é possível distinguir os usuários ativos sem a necessidade de cabeçalhos de

TABELA I

Parâmetros de comparação para as sequências de protocolo. Sequências-Constacíclicas com $p \geq 5$, $4 \leq k \leq p-1$ e $w(\mathbf{v}') \geq 3$. Sequências-RS e Sequências-BCH com $p \geq 5$, $3 \leq k \leq p-1$ e $r > 1$. $(*)$ A_{p+1} denota o número de palavras-código de peso $p+1$ de um código MDS [14, p. 189].

Critérios	**Sequências**				
	Construção 1	tipo-I[3]	tipo-II[3]	RS[9]	BCH[10]
Limitante inferior para R_{sum}	$\frac{1}{4(k-1)w(\mathbf{v}')}$	$\frac{1}{4(k-1)w(\mathbf{v}')}$	$\frac{1}{4(k-1)}$	$\frac{1}{4(k-1)}$	$\frac{1}{4(k-1)}$
Limitante superior para M	$\lfloor p/3 \rfloor$	$\lfloor p/3 \rfloor$	$\lfloor p/3 \rfloor$	$\lfloor p/2 \rfloor$	$\lfloor p/2 \rfloor$
Nº de sequências geradas (U)	$\frac{p^k-1}{p^2-1}$	p^{k-2}	$\frac{A^{(*)}_{p+1}}{N}$	p^{k-2}	$p^{(k-2)r}$
Comprimento do quadro (N)	p^2-1	p^2-1	p^2-1	p^2-p	$p(p^r-1)$
Diferentes fatores de trabalho	*sim*	*sim*	*não*	*não*	*não*

identificação [6]. Assim como as Sequências-Constacíclicas tipo-I, as sequências baseadas na Construção 1 também dão suporte a usuários com diferentes fatores de trabalho [6].

O valor de U das sequências baseadas na Construção 1 é maior do que o respectivo valor para as Sequências-Constacíclicas tipo-I e as Sequências-RS, pois $(p^k-1)/(p^2-1) > p^{k-2}$ para $k > 2$. Desta forma, O valor de U das sequências baseadas na Construção 1 é apenas inferior ao valor de U das Sequências-BCH à medida que o valor de r aumenta. Porém, para valores elevados de r, o valor de N para as Sequências-BCH também torna-se elevado, e valores elevados de N aumentam a complexidade de decodificação por intervalo de tempo [10]. No caso das sequências baseadas na Construção 1, é possível aumentar o valor de U (aumentando o valor de k) mantendo o mesmo valor para N.

Sequências-Constacíclicas tipo-I, tipo-II e as sequências baseadas na Construção 1 possuem o mesmo limitante, $M \leq \lfloor p/3 \rfloor$, que é menor que o limitante superior para as Sequências-RS e Sequências-BCH dado por $M \leq \lfloor p/2 \rfloor$. Porém, a diferença entre os valores dos limitantes é cada vez menor à medida que o valor de p aumenta.

Pela Tabela I, as Sequências-Constacíclicas tipo-II possuem o mesmo limitante inferior das Sequências-RS e das Sequências-BCH para R_{sum}. Já as Sequências-Constacíclicas tipo-I e as sequências baseadas na Construção 1 possuem um limitante inferior que é menor que o correspondente das demais sequências por um fator de $\frac{1}{w(\mathbf{v}')}$, $w(\mathbf{v}') \geq 3$. Esta diminuição é devida ao fato dos códigos CP usados serem de peso não-constante e o valor de $w(\mathbf{v}')$ influenciar diretamente no peso das palavras-código. Como há usuários com variados fatores de trabalho, o número de usuários ativos por quadro pode diminuir. Porém, as Sequências-Constacíclicas tipo-I e as sequências baseadas na Construção 1 são as únicas na literatura, obtidas por meio de códigos CP, que comportam usuários com diferentes fatores de trabalho.

V. Conclusões

Este artigo propõe um novo conjunto de códigos CP, derivados de códigos constacíclicos p-ários, cujas palavras-código podem ser usadas como sequências de protocolo para o CCsR. Os teoremas 1 e 2 são a versão para códigos constacíclicos dos teoremas 1 e 2 em [15] para códigos cíclicos. A Construção 1 é ótima no sentido que atinge precisamente o limitante superior para o número de classes de equivalência constacíclica dos códigos usados. No que diz respeito às Sequências-Constacíclicas baseadas na Construção 1, o desempenho delas mostrou-se satisfatório e com destaque para dois parâmetros: o número total de usuários U e a flexibilidade de utilização para usuários com diferentes fatores de trabalho.

Referências

[1] E. N. Gilbert, "Cyclically permutable error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 9, pp. 175–182, July 1963.

[2] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[3] V. C. da Rocha and J. S. Lemos-Neto, "New cyclically permutable codes," *IEEE Information Theory Workshop (ITW)*, Rio de Janeiro-RJ, Brazil, pp. 693–697, Oct. 2011.

[4] J. L. Massey, "The capacity of the collision channel without feedback," Abstracts of Papers, *IEEE Int. Symp. Inform. Theory*, p. 101, 1982.

[5] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 192-204, Mar. 1985.

[6] J. S. Lemos-Neto and V. C. da Rocha, "Sequências de protocolo para o canal de colisão sem realimentação," *Anais do XXXI Simpósio Brasileiro de Telecomunicações (XXXI SBrT)*, Fortaleza-CE, Brasil, pp. 1–5, Setembro 2013.

[7] L. Salaün, C. S. Chen, Y. Chen and W. S. Wong, "Constant delivery delay protocol sequences for the collision channel without feedback, " *2016 19th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Shenzhen, Chine, pp. 429–434, Nov. 2016.

[8] Y. Zhang, Y. Chen, Y. H. Lo and W. S. Wong, "The zero-error capacity of a collision channel with successive interference cancellation," *IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, pp. 1653–1657, June 2017.

[9] N. Q. A, L. Györfi and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol.38, no.3, pp. 940–949, May 1992.

[10] L. Györfi and I. Vajda, "Constructions of protocol sequences for multiple access collision channel without feedback," *IEEE Trans. Inform. Theory*, vol.39, no.5, pp. 1762–1765, Sept. 1993.

[11] V. Da Rocha, "Maximum distance separable multilevel codes," *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 547–548, May 1984.

[12] A. Krishna and D.V. Sarwate, "Pseudocyclic maximum-distance-separable codes," *IEEE Trans. Inform. Theory*, vol. IT-36, no. 4, pp. 880-884, July 1990.

[13] J. S. Lemos-Neto and V. C. da Rocha, "Códigos ciclicamente permutáveis derivados de códigos constacíclicos," *Anais do XXIX Simpósio Brasileiro de Telecomunicações (XXIX SBrT)*, Curitiba-PR, Brasil, pp. 1–5, Outubro 2011.

[14] S. B. Wicker, *Error Control Systems*, Prentice Hall, 1995.

[15] J. S. Lemos-Neto and V. C. da Rocha, "Cyclically permutable codes specified by roots of generator polynomial," *Electronics Letters*, vol. 50, no. 17, pp. 1202–1204, Aug. 2014.