Códigos ciclicamente permutáveis derivados de códigos constacíclicos

José Sampaio de Lemos Neto e Valdemar C. da Rocha Jr.

***Resumo*— Um código ciclicamente permutável (código CP) é um código de bloco binário cujas palavras-código são ciclicamente distintas e possuem ordem cíclica plena. O objetivo deste artigo é construir códigos CP por meio de códigos constacíclicos lineares p-ários, em que p denota um número primo. É utilizado um método eficiente para selecionar palavras de um código constacíclico que são constaciclicamente distintas e que possuem ordem constacíclica plena. Por intermédio de uma representação cíclica para os elementos de $\mathrm{GF}(p)$ e por meio de uma relação entre arranjos bidimensionais e N-uplas, as palavras selecionadas do código constacíclico produzem o dicionário de um código CP. Os códigos ciclicamente permutáveis propostos podem ser aplicados em sistemas de marca d'água de áudio e/ou de video.**

***Palavras-Chave*— Códigos ciclicamente permutáveis, códigos constacíclicos, marca d'água.**

***Abstract*— A cyclically permutable code (CP code) is a binary code whose codewords are cyclically distinct and have full cyclic order. The purpose of this paper is to construct CP codes by means of linear p-ary constacyclic codes, where p denotes a prime number. An efficient method is used to select codewords from a constacyclic code which are constacyclically distinct and have full constacyclic order. Through a cyclic representation for the elements of $\mathrm{GF}(p)$ and by a correspondence of two-dimensional arrays and N-tuples, the codewords selected produce the codebook of a CP code. The cyclically permutable codes proposed can be applied to audio and/or video watermarking systems.**

***Keywords*— Cyclically permutable codes, constacyclic codes, watermark.**

I. Introdução

O objetivo deste artigo é apresentar um modo de construir códigos ciclicamente permutáveis (códigos CP) por meio de códigos constacíclicos p-ários [1], [2]. Gilbert [3] definiu um *código ciclicamente permutável* como um código de bloco binário de comprimento N, tal que suas palavras-código tenham ordem cíclica N e tal que elas sejam ciclicamente distintas.

A construção de códigos CP proposta neste artigo é baseada no método proposto por A, Györfi e Massey [4]. A principal diferença entre as duas construções está relacionada à classe de códigos utilizada. Em [4] utiliza-se códigos Reed-Solomon (RS) p-ários e neste artigo utiliza-se a classe de códigos constacíclicos p-ários. A construção proposta neste artigo apresenta duas vantagens com relação àquela proposta em [4]. A primeira delas é uma maior eficiência obtida e a segunda vantagem é que, enquanto os códigos CP propostos em [4] são necessariamente de peso constante, os códigos CP propostos neste artigo podem ser ou não de peso constante.

José Sampaio de Lemos Neto e Valdemar C. da Rocha Jr., Grupo de Pesquisa em Comunicações - CODEC, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, CEP 50711-970, Caixa Postal 7800. E-mails: jose.lemosnt@ufpe.br, vcr@ufpe.br. Este trabalho foi parcialmente financiado pelo CNPq, Proj. 304696/2010-2.

Na Seção II são apresentados alguns conceitos básicos de códigos constacíclicos. Na Seção III e na Seção IV são abordadas, respectivamente, uma representação cíclica para os elementos de $\mathrm{GF}(p)$ por meio de $(p-1)$-uplas binárias e uma correspondência entre arranjos bidimensionais e N-uplas. Utilizando os resultados da Seção III e da Seção IV, prova-se, na Seção V, um teorema que estabelece como obter códigos cíclicos binários não-lineares por meio de códigos constacíclicos p-ários. Na Seção VI, o método para selecionar as palavras de um código constacíclico que são constaciclicamente distintas e que possuem ordem constacíclica plena é apresentado. O método citado, em combinação com os resultados da Seção V, possibilita enunciar a construção de códigos CP proposta neste artigo. Finalmente, na Seção VII é sugerida uma possível aplicação dos códigos ciclicamente permutáveis aqui construídos, para serem empregados como códigos corretores de erro de sistemas de *marca d'água* digital visando aumentar a resistência desses sistemas contra ataques de corte (*clipping attack*) [6], [7], [8], [9].

II. Códigos constacíclicos

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. 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 [1].

Denote por $\mathcal{C}$ um código de bloco linear p-ário (n, k, d), em que n, k e d representam, respectivamente, seu comprimento, sua dimensão e sua distância mínima de Hamming. Se o deslocamento constacíclico de qualquer palavra-código de $\mathcal{C}$ resulta em uma palavra desse código, então $\mathcal{C}$ é denominado de *código constacíclico*. Dado um corpo finito $\mathrm{GF}(p)$, a escolha dos parâmetros n, k e do elemento a, $a \in \mathrm{GF}(p),\ a \neq 0$, para gerar um código constacíclico não é arbitrária. Em [10] e [11] demonstram-se algumas possíveis escolhas para os valores n, k e a que permitem gerar códigos constacíclicos. Sem perda de generalidade essencial, daqui por diante os códigos constacíclicos discutidos possuem comprimento $n = p + 1$, k é um número par tal que $2 \leq k \leq p - 1$ e a é um elemento primitivo do grupo multiplicativo de $\mathrm{GF}(p)$. Vale destacar que os resultados apresentados podem ser estendidos para alguns outros valores de n, k e a de acordo com [11].

Sendo p um número primo, um resultado conhecido [10] é que as raízes do polinômio $x^{p^2-1}-1$ pertencem a $\mathrm{GF}(p^2)$ e $x^{p^2-1}-1 = \prod_{i=1}^{p-1}(x^{p+1}-i)$. Além do mais, sendo $\phi(.)$ a função de Euler, as $\phi(p^2-1)$ raízes primitivas de $x^{p^2-1}-1$ pertencem aos binômios $x^{p+1}-a$ para os quais a é um elemento primitivo do grupo multiplicativo de $\mathrm{GF}(p)$. Cada binômio $x^{p+1}-a$ é fatorado em $(p+1)/2$ polinômios mínimos de grau 2. Quando a é um elemento primitivo do grupo multiplicativo de $\mathrm{GF}(p)$, $[\phi(p^2-1)]/[2\phi(p-1)]$ desses polinômios mínimos são primitivos e de grau 2.

Exemplo 1: Considere $p = 13$. O polinômio $x^{168}-1$ possui $\phi(168) = 48$ raízes primitivas e é fatorado em 12 polinômios da forma $x^{14}-a$, em que $a \neq 0$ e $a \in \mathrm{GF}(13)$. Para $a \in \{2, 6, 7, 11\}$, $x^{14}-a$ possui 6 polinômios primitivos de grau 2 como fatores.

A. Ordem constacíclica das palavras-código

Considere um código constacíclico linear p-ário $(p+1, k, d)$ em que as palavras-código são reduzidas módulo $(x^{p+1}-a)$.

Definição 1: A *ordem constacíclica* de uma palavra-código é o menor número inteiro positivo i tal que $x^i c(x) = c(x) \bmod (x^{p+1}-a)$.

Quando o menor valor de i, tal que $x^i c(x) = c(x) \bmod (x^{p+1}-a)$, é $i = p^2-1$, diz-se que a palavra-código $c(x)$ possui *ordem constacíclica plena*. 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 $\bmod (x^{p+1}-a)$.

Definição 2: 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 $0 \leq i \leq p^2-1$. 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.

Decorre da Definição 2 que a palavra-código toda nula, denotada por $\mathbf{0}$, constitui uma classe de equivalência constacíclica de ordem igual a 1. Além do mais, qualquer palavra-código pertencente a uma mesma classe de equivalência pode ser definida como líder de sua classe.

III. Representação cíclica para os elementos de $\mathrm{GF}(p)$

O objetivo dessa seção é expor uma maneira apropriada [5] para representar os elementos de $\mathrm{GF}(p)$ por intermédio de N-uplas binárias. Neste ponto, vale lembrar que a *ordem cíclica* de uma N-upla $\mathbf{b}$ é o menor número inteiro positivo i para o qual $\mathbf{S}^i(\mathbf{b}) = \mathbf{b}$, em que $\mathbf{S}^i$ denota o operador que desloca ciclicamente de i posições para a direita uma N-upla qualquer. Assim, a ordem cíclica de uma N-upla é igual a N ou igual a um dos seus divisores. Sendo p um número primo tal que $p > 3$, $N = p-1$ é um número par e, assim, sempre existe uma $(p-1)$-upla binária de ordem cíclica igual a 2 que corresponde à $(p-1)$-upla de peso igual a $(p-1)/2$ cujas coordenadas assumem valores alternados 0 ou 1, isto é, $(1,0,1,0,\ldots,1,0)$ ou $(0,1,0,1,\ldots,0,1)$. Além do mais, sempre existe pelo menos uma $(p-1)$-upla binária de ordem cíclica $p-1$ que corresponde à $(p-1)$-upla de peso unitário. Porém, pode haver outras $(p-1)$-uplas com ordem cíclica igual a $p-1$, além da que foi citada, e que não tenham peso igual a 1.

Definição 3: Seja $\mathbf{v}$ uma $(p-1)$-upla binária cuja ordem cíclica é igual a $p-1$. Define-se a *representação*-$\mathbf{V}$, como sendo uma representação para os elementos de $\mathrm{GF}(p)$ por intermédio de $(p-1)$-uplas binárias tal que 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 a é um elemento gerador do grupo multiplicativo de $\mathrm{GF}(p)$. 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.

Exemplo 2: Seja $p = 5$, $a = 3$, $\mathbf{v}' = (1,0,1,0)$ e $\mathbf{v} = (1,1,0,0)$. Assim, a representação-$\mathbf{V}$ para $\mathrm{GF}(5)$ é $0 \leftrightarrow (1,0,1,0)$ ou $0 \leftrightarrow (0,1,0,1)$, $3^0 \leftrightarrow (1,1,0,0)$, $3^1 \leftrightarrow (0,1,1,0)$, $3^2 \leftrightarrow (0,0,1,1)$ e $3^3 \leftrightarrow (1,0,0,1)$.

IV. Arranjos bidimensionais e N-uplas

A seguir é descrita uma correspondência um-a-um entre arranjos bidimensionais e N-uplas [5]. Os arranjos bidimensionais considerados são semelhantes ao arranjo A da Equação (1), cujos elementos $a_{(i,j)}$, $i = \{0, 1, \ldots, m-1\}$ e $j = \{0, 1, \ldots, n-1\}$, pertencem a um alfabeto arbitrário. A referida correspondência é geral no sentido de que não é necessário que m e n sejam números primos entre si.

$$A = \begin{bmatrix} a_{(0,0)} & a_{(0,1)} & \cdots & a_{(0,n-1)} \\ a_{(1,0)} & a_{(1,1)} & \cdots & a_{(1,n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(m-1,0)} & a_{(m-1,1)} & \cdots & a_{(m-1,n-1)} \end{bmatrix}. \quad (1)$$

Para m e n inteiros positivos, a relação que estabelece uma correspondência um-a-um entre o arranjo A da Equação (1) e N-uplas da forma $\mathbf{b} = (b_0, b_1, \ldots, b_{mn-1})$, ambos com elementos pertencentes a um mesmo alfabeto, é dada por

$$b_{in+j} = a_{(i,j)},\ 0 \leq i \leq m-1 \text{ e } 0 \leq j \leq n-1. \quad (2)$$

Exemplo 3: O arranjo

$$A = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

corresponde, pela relação dada em (2), à 9-upla $\mathbf{b} = (a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3)$.

Definição 4: O *operador constacíclico* $\mathbf{DB}$ atua sobre um arranjo bidimensional A, produzindo o arranjo A'', da seguinte forma:

1) o operador $\mathbf{DB}$, inicialmente, desloca *ciclicamente* todas as colunas do arranjo A uma posição para a direita produzindo um novo arranjo A';
2) depois, o operador $\mathbf{DB}$ desloca ciclicamente uma posição para baixo a coluna mais à esquerda do arranjo A' produzindo o arranjo A''.

Exemplo 4: Aplicando o operador $\mathbf{DB}$ da Definição 4 ao arranjo A do Exemplo 3 obtém-se

$$A = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \rightarrow A'' = \begin{bmatrix} a_9 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix}. \quad (3)$$

A 9-upla $\mathbf{b}'' = (a_9, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ é obtida aplicando a relação dada na Equação (2) ao arranjo A'' do Exemplo 4. Nota-se que $\mathbf{b}''$ corresponde a um deslocamento cíclico para direita da 9-upla $\mathbf{b} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9)$ do Exemplo 3, ou seja, $\mathbf{S}(\mathbf{b}) = \mathbf{b}''$. Essa propriedade é explorada no teorema a seguir.

Teorema 1: Considere um conjunto $\mathcal{X}$ formado por arranjos bidimensionais $m \times n$ cujos elementos pertencem a um alfabeto arbitrário. O conjunto $\mathcal{X}$ será fechado em relação à operação realizada por $\mathbf{DB}$ se e somente se o conjunto correspondente de mn-uplas for fechado em relação à operação realizada por $\mathbf{S}^i$.

Demonstração: Seja A um arranjo bidimensional pertencente ao conjunto $\mathcal{X}$ e seja $\mathbf{b}$ a mn-upla binária correspondente ao arranjo A de acordo com a Equação (2). Seja A'' um arranjo bidimensional tal que $\mathbf{DB}(A) = A''$. A relação entre os elementos dos arranjos A e A'' para $0 \leq i \leq m-1$ é dada por

$$a''_{(i,j)} = a_{(i \bmod m, j-1 \bmod n)}, 1 \leq j \leq n-1, \text{e} \quad (4)$$
$$a''_{(i,0)} = a_{(i-1 \bmod m, n-1)}, j = 0, \quad (5)$$

em que $l \bmod y$ denota o resto da divisão quando l é dividido por y. Sendo $\mathbf{S}(\mathbf{b}) = \mathbf{b}'$, a relação entre os elementos das mn-uplas $\mathbf{b}$ e $\mathbf{b}'$ para $0 \leq i \leq m-1$ é tal que

$$b'_{in+j \bmod mn} = b_{in+j-1 \bmod mn}, 0 \leq j \leq n-1. \quad (6)$$

A mn-upla $\mathbf{b}''$ é obtida aplicando-se a relação dada pela Equação (2) ao arranjo A''. Logo, usando as Equações (4) e (5) e para $0 \leq i \leq m-1$ obtém-se

$$b''_{in+j \bmod mn} = b_{in+j-1 \bmod mn},\ 1 \leq j \leq n-1,\ \text{e} \quad (7)$$
$$b''_{in+j \bmod mn} = b_{in-1 \bmod mn},\ j = 0. \quad (8)$$

Comparando as Equações (7) e (8) com a Equação (6), conclui-se que $\mathbf{b}' = \mathbf{b}''$ e, assim, $\mathbf{S}(\mathbf{b}) = \mathbf{b}''$. Portanto, uma condição suficiente para o conjunto $\mathcal{X}$ ser fechado com relação à operação realizada por $\mathbf{DB}$ é o conjunto de mn-uplas ser fechado com relação à operação realizada por $\mathbf{S}^i$. De maneira análoga, pode-se mostrar que uma condição necessária para o conjunto $\mathcal{X}$ ser fechado com relação à operação realizada por $\mathbf{DB}$ é o conjunto de mn-uplas ser fechado em relação à operação realizada por $\mathbf{S}^i$. ■

V. Códigos cíclicos binários não-lineares

Nessa seção, o intuito é construir códigos cíclicos binários não-lineares. Para isto, são utilizados os códigos constacíclicos lineares p-ários (n, k, d) definidos na Seção II. Juntamente com esses códigos, utiliza-se a representação cíclica definida para os elementos de $\mathrm{GF}(p)$, Seção III, e a relação entre arranjos bidimensionais e N-uplas, Seção IV.

A ideia para construir os códigos cíclicos binários não-lineares é descrita a seguir. Primeiro, cada palavra-código p-ária $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, pertencente ao código constacíclico, é mapeada em um arranjo bidimensional cujas colunas são as transpostas das $(p-1)$-uplas binárias, dadas pela representação-$\mathbf{V}$, para cada coordenada c_i, $0 \leq i \leq n-1$. Depois, os arranjos bidimensionais são convertidos em N-uplas binárias por meio da relação dada na Equação (2).

Antes de enunciar o Teorema 2, que estabelece o principal resultado utilizado para gerar códigos cíclicos binários, vale ressaltar que, na representação-$\mathbf{V}$ da Definição 3, o elemento 0 é representado por uma $(p-1)$-upla $\mathbf{v}'$ e seus deslocamentos cíclicos, logo uma palavra-código p-ária $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ que tenha uma ou mais coordenadas nulas, $c_i = 0$ para $0 \leq i \leq n-1$, pode ser associada a mais de um arranjo bidimensional e, consequentemente, a mais de uma N-upla binária. Sendo assim, deve-se ter um cuidado especial para que as p^k palavras do código constacíclico representem exatamente p^k N-uplas binárias correspondendo às palavras do código cíclico binário. Para isto, as palavras do código constacíclico devem ser separadas em classes de equivalência constacíclica conforme a Definição 2. Depois, seleciona-se arbitrariamente uma palavra-código $\mathbf{c}$ para ser líder de sua respectiva classe de equivalência constacíclica e a ela associa-se um arranjo bidimensional A. Se $\mathbf{c}$ possui todas as coordenadas não-nulas, o mapeamento de $\mathbf{c}$ para A é um-a-um e, portanto, não há problemas. Entretanto, se $\mathbf{c}$ possui uma ou mais coordenadas nulas, o mapeamento de $\mathbf{c}$ para A é feito escolhendo-se, inicialmente, uma $(p-1)$-upla $\mathbf{v}'$ arbitrária para representar o elemento 0. Os demais arranjos associados às palavras-código, que pertencem à mesma classe de equivalência constacíclica de $\mathbf{c}$, são obtidos aplicando-se o operador constacíclico $\mathbf{DB}$ ao arranjo A de modo que a palavra-código $\mathbf{c}'$, correspondente ao i-ésimo deslocamento constacíclico de $\mathbf{c}$, é representada pelo arranjo bidimensional Z obtido ao aplicar o operador constacíclico $\mathbf{DB}$ i vezes ao arranjo A. Daqui em diante, faz-se referência a esse processo como *geração biunívoca de arranjos*.

Teorema 2: Seja p um número primo, $p > 3$, e $\mathcal{C}$ um código constacíclico linear p-ário de parâmetros (n, k, d). Considere que cada palavra-código $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ líder de classe de equivalência constacíclica determine um arranjo bidimensional A de modo que a i-ésima coluna de A seja a transposta de uma $(p-1)$-upla binária que corresponde à representação-$\mathbf{V}$ da i-ésima componente de $\mathbf{c}$. Defina $\mathbf{b}$ como sendo a N-upla, com $N = (p-1)n$, que corresponde ao arranjo A por meio da relação dada na Equação (2). Além do mais, considere que as demais palavras-código são mapeadas em N-uplas binárias com o auxílio do processo de *geração biunívoca de arranjos*. Então, o conjunto de p^k N-uplas binárias correspondentes às p^k palavras-código de $\mathcal{C}$ formam um código cíclico binário de distância mínima $d_{\min} \geq dd(\mathbf{v})$ com igualdade se a representação-$\mathbf{V}$ de $\mathrm{GF}(p)$ for equidistante.

Demonstração: Seja $\mathbf{c} \in \mathcal{C}$ uma palavra-código líder de classe de equivalência constacíclica e seja A o arranjo bidimensional correspondente a $\mathbf{c}$. Uma vez que $\mathcal{C}$ é um código linear constacíclico, deslocar constaciclicamente para a direita a palavra-código $\mathbf{c}$ produz uma palavra-código $\mathbf{c}' \in \mathcal{C}$ cujo arranjo bidimensional, denotado por A', é tal que

$\mathbf{DB}(A) = A'$. Sendo assim, os p^k arranjos bidimensionais, correspondentes às palavras-código de $\mathcal{C}$, formam um conjunto $\mathcal{Y}$ fechado em relação à operação realizada pelo operador $\mathbf{DB}$. Segue do Teorema 1 que o conjunto de p^k N-uplas binárias $\mathbf{b}$, com $N = (p-1)n$, obtidas ao se aplicar a relação dada pela Equação (2) aos arranjos bidimensionais do conjunto $\mathcal{Y}$, é um conjunto fechado em relação à operação realizada pelo operador $\mathbf{S}^i$ e, portanto, é um código cíclico binário.

Para concluir a demonstração, resta deduzir o limitante inferior dado para $d_{\min}$. Como o código $\mathcal{C}$ tem distância mínima d, duas palavras-código distintas $\mathbf{c}_1$ e $\mathbf{c}_2$ diferem em d coordenadas no mínimo, isto é, a distância de Hamming entre elas satisfaz $d(\mathbf{c}_1, \mathbf{c}_2) \geq d$. Sendo assim, as N-uplas binárias $\mathbf{b}_1$ e $\mathbf{b}_2$, correspondendo a $\mathbf{c}_1$ e $\mathbf{c}_2$ respectivamente, diferem em $dd(\mathbf{v})$ coordenadas no mínimo, em que $d(\mathbf{v})$ é a distância mínima da representação-$\mathbf{V}$. Uma vez que $d(\mathbf{c}_1, \mathbf{c}_2) \geq d$ é satisfeita com igualdade para algumas escolhas de $\mathbf{c}_1$ e $\mathbf{c}_2$, conclui-se que $d_{\min} \geq dd(\mathbf{v})$, a qual é satisfeita com igualdade caso a representação-$\mathbf{V}$ seja equidistante. ■

VI. Códigos ciclicamente permutáveis

Um *código ciclicamente permutável* (código CP) é um código de bloco binário em que as palavras-código possuem ordem cíclica plena e são ciclicamente distintas [3]. A, Györfi, e Massey [4] foram os primeiros a propor uma maneira geral de construir códigos CP por meio de códigos Reed-Solomon (RS) p-ários ou por meio de códigos Berlekamp-Justesen (BJ) [12]. Neste artigo, propõe-se a construção de códigos CP por meio de códigos constacíclicos ao invés de códigos RS ou BJ. Enquanto os códigos CP propostos em [4] são necessariamente de peso constante, os códigos CP propostos neste artigo podem ser de peso constante ou não. Seguindo a notação usada em [4], $CCP(N, M_c, d_c)$ denota um código ciclicamente permutável de comprimento N, com M_c palavras-código e distância mínima cíclica d_c.

O conceito de classe de equivalência constacíclica definido para as palavras de um código constacíclico, Seção II, pode ser aplicado de maneira semelhante às palavras de um código cíclico ou para uma N-upla, em geral. Desta forma, sendo $\mathbf{b}$ uma N-upla p-ária, pode-se definir *classe de equivalência cíclica* como sendo o conjunto de N-uplas cujos elementos correspondem a todos os deslocamentos cíclicos de $\mathbf{b}$. Em termos do operador $\mathbf{S}^i$, duas N-uplas, $\mathbf{b}$ e $\mathbf{b}'$, pertencem à mesma classe de equivalência cíclica se $\mathbf{S}^i(\mathbf{b}) = \mathbf{b}'$ para algum valor de i, $1 \leq i \leq N-1$. Se $\mathbf{b}$ tem ordem cíclica j, então a classe de equivalência a qual $\mathbf{b}$ pertence tem j N-uplas e, portanto, esta classe tem ordem cíclica j. Alternativamente, um código CP pode ser definido como um código de bloco binário tal que suas palavras-código pertencem a diferentes classes de equivalência cíclica cada uma com ordem cíclica igual ao comprimento das palavras-código.

Segundo A, Györfi e Massey [4], para o procedimento de seleção das palavras de um código CP a partir das palavras de um código cíclico binário ser qualificado como *construção*, tal processo deve ser facilmente implementável. Ainda, segundo [4], para as construções serem consideradas *boas*, o número de palavras do código CP, dado por M_c, deve ser o mais próximo possível de M/N, em que M e N denotam, respectivamente, o número de palavras do código cíclico binário e o comprimento do código. Além do mais, a distância mínima $d_{\min}$ do código cíclico binário deve ser a maior possível para os valores de M e N definidos.

O teorema a seguir estabelece um meio eficiente de selecionar as palavras de um código constacíclico p-ário que são constaciclicamente distintas, possuem ordem constacíclica plena e que o total de palavras selecionadas aproxima-se do limitante superior M/N, quando esse código constacíclico gera um código cíclico binário de acordo com o Teorema 2.

Teorema 3: Seja $\mathcal{C}$ um código constacíclico linear p-ário $(p+1, k, d)$ com polinômio gerador $g(x)$ e seja $s(x)$ um polinômio de grau 2 que pertence ao expoente p^2-1 e é fator do polinômio de paridade $h(x)$. Além do mais, considere $m(x)$ um polinômio-mensagem cujo grau é menor ou igual a $k-3$. Então, as palavras-código $c(x)$ selecionadas tal que $c(x) = g(x)[1 + s(x)m(x)]$ têm ordem constacíclica plena e são constaciclicamente distintas.

Demonstração: Se $c(x) \in \mathcal{C}$ tem ordem constacíclica plena, então o menor valor para o qual i satisfaz

$$\begin{aligned} x^i c(x) &= c(x) \bmod x^{p+1} - a, \text{ ou,} \\ (x^i - 1)c(x) &= 0 \bmod x^{p+1} - a, \end{aligned} \tag{9}$$

é $i = p^2 - 1$. Visto que $s(x)$ é um fator de $h(x)$, pode-se escrever $h(x) = a(x)s(x)$, em que $a(x)$ é fator de $h(x)$. Substituindo $c(x)$ por $g(x)[1 + s(x)m(x)]$ em (9) obtém-se

$$\begin{aligned} (x^i - 1)g(x)[1 + s(x)m(x)] &= 0 \bmod g(x)h(x), \\ (x^i - 1)[1 + s(x)m(x)] &= 0 \bmod h(x), \\ &= 0 \bmod a(x)s(x). \end{aligned} \tag{10}$$

Como $\text{mdc}[1 + s(x)m(x), s(x)] = 1$, a Equação (10) é satisfeita se e somente se $s(x)$ tem fator comum com $x^i - 1$. Porém, por definição, $s(x)$ pertence ao expoente p^2-1. Assim, o menor valor de i para o qual a Equação (10) é satisfeita é $i = p^2 - 1$. Portanto, as palavras-código $c(x)$ selecionadas, $c(x) = g(x)[1 + s(x)m(x)]$, têm ordem constacíclica plena.

Para provar que as palavras-código são constaciclicamente distintas, considere duas palavras-código, distintas, $c_1(x) = g(x)[1+s(x)m_1(x)]$ e $c_2(x) = g(x)[1+s(x)m_2(x)]$. Suponha que $c_1(x)$ e $c_2(x)$ pertençam à mesma classe de equivalência constacíclica. Ou seja,

$$x^i c_2(x) = c_1(x) \bmod x^{p+1} - a, \tag{11}$$

para algum valor de i tal que $0 < i < p^2 - 1$. Manipulando algebricamente a Equação (11) obtém-se

$$x^i - 1 + s(x)[x^i m_2(x) - m_1(x)] = 0 \bmod a(x)s(x). \tag{12}$$

Para que a Equação (12) seja satisfeita, $s(x)$ deve ser fator de $x^i - 1$. Entretanto, esta condição é impossível, pois $s(x)$ pertence ao expoente $p^2 - 1$ e $0 < i < p^2 - 1$. Assim, a hipótese de que as palavras-código $c_1(x)$ e $c_2(x)$ pertencem à mesma classe de equivalência constacíclica é falsa e, portanto, elas são constaciclicamente distintas. ■

Construção: Seja p um número primo, $p > 3$, $n = p + 1$ e k um número par tal que $2 \leq k \leq p - 1$. Escolha uma representação-$\mathbf{V}$ e um código $\mathcal{C}$ constacíclico linear p-ário $(p+$

$1, k, p-k+2)$ (MDS). Aplicando o Teorema 2 a cada palavra-código $c(x)$ selecionada de acordo com o Teorema 3, obtém-se um $CCP(N, M_c, d_c)$ com $N = p^2 - 1$, $M_c = p^{k-2}$ e com distância mínima cíclica $d_c \geq (p - k + 2)d(\mathbf{v})$.

Dependendo da escolha das $(p-1)$-uplas binárias $\mathbf{v}$ e $\mathbf{v}'$, na representação-$\mathbf{V}$, os códigos CP da *Construção* podem ser de peso constante ou não. Se $\mathbf{v}$ e $\mathbf{v}'$ são escolhidas tal que $w(\mathbf{v}) = w(\mathbf{v}')$, então os códigos CP são de peso constante, caso contrário, i.e., $w(\mathbf{v}) \neq w(\mathbf{v}')$, os códigos CP não são de peso constante.

De maneira análoga ao que é feito em [4], a eficiência do procedimento utilizado para gerar os códigos CP da *Construção* é analisada. As palavras do código CP da *Construção* pertencem a um código cíclico binário de comprimento $N = p^2 - 1$ e com $M = p^k$ palavras-código. Desta forma, a razão $M/N = p^k/(p^2 - 1)$ é o limitante superior para o número de palavras que podem ser selecionadas para o código CP. O procedimento utilizado na *Construção* seleciona $M_c = p^{k-2}$ e este valor é menor que o limitante superior por um fator de $(p^2 - 1)/p^2$ que tende ao valor 1 à medida que o valor de p aumenta. Uma das construções de códigos CP proposta em [4] utiliza códigos Reed-Solomon. As palavras do código CP pertencem a um código binário cíclico de comprimento $N = p(p - 1)$ com $M = p^k$ palavras-código. O procedimento utilizado seleciona $M_c = p^{k-2}$ palavras para o código CP. Logo, o limitante superior é dado por $M/N = p^{k-1}/(p-1)$ e o total de palavras $M_c = p^{k-2}$ difere desse limitante por um fator de $(p-1)/p$. Comparando-se este fator com o fator $(p^2 - 1)/p^2$, percebe-se que para qualquer valor de p, $(p^2-1)/p^2 > (p-1)/p$. Portanto, a *Construção* é mais eficiente do que aquela baseada em códigos RS, proposta em [4], e também facilmente demonstrável ser mais eficiente do que a outra construção, baseada em códigos BJ, também proposta em [4].

VII. Aplicação em sistemas de marca d'água

De acordo com [9], *marca d'água digital* é uma mensagem, também digital, incorporada aos dados hospedeiros, que, tipicamente, contém informações sobre origem, estado e destino dos dados. Existe uma variedade de situações em que *sistemas de marca d'água digital* são usados [7], [9]. Por exemplo, autenticação de dados, transmissão de informação em segundo plano (e.g., legendas em filmes) e, principalmente, proteção de direitos autorais. Em geral, a marca d'água deve carregar a maior quantidade possível de informação, deve ser irremovível dos dados hospedeiros, imperceptível para usuários não autorizados e resistente contra ataques, em que o termo *ataque* refere-se a qualquer tentativa de manipular os dados hospedeiros com o intuito de comprometer, destruir ou remover a marca d'água. Códigos corretores de erro podem ser usados em sistemas de marca d'água para aumentar a resistência a ataques [6], [7]. Nesses casos, a marca d'água é codificada e a palavra-código resultante é incorporada aos dados hospedeiros. Se a marca d'água ao ser recuperada contiver erros devido, principalmente, aos ataques, ainda é possível recuperar a marca d'água desde que a quantidade de erros seja menor ou igual a t, em que t denota a capacidade de correção do código corretor de erro utilizado.

Códigos ciclicamente permutáveis além de aumentarem a resistência contra ataques, como citado anteriormente, são úteis devido a propriedade de autosincronismo [13, Cap. 12], sendo esta uma característica interessante em aplicações de marca d'água que envolvem dados hospedeiros de áudio e/ou de video. Nessas situações, a marca d'água é espalhada pelos quadros dos dados hospedeiros como uma maneira simples de aumentar a resistência contra os ataques de corte [7]. Ao utilizar uma marca d'água codificada por meio de um código CP de comprimento N, a eficiência contra esse tipo de ataque pode ser melhorada, pois a marca d'água pode ser recuperada diretamente de qualquer sequência de N quadros consecutivos, sem a necessidade de recuperar o sincronismo, pois o resultado obtido ou é a própria palavra-código ou um de seus $N - 1$ deslocamentos cíclicos.

VIII. Conclusões

Este artigo mostrou um meio de construir códigos ciclicamente permutáveis por meio de códigos constacíclicos p-ários. Comparando com a construção proposta em [4], que utiliza códigos Reed-Solomon p-ários, a construção proposta neste artigo é mais eficiente. Outra vantagem é que os códigos CP propostos não são necessariamente de peso constante como ocorre em [4]. Além do mais, a construção de códigos CP apresentada oferece um maior leque de opções para aplicações em sistemas de marca d'água digital.

Referências

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

[2] J. S. de Lemos Neto, *Construção de sequências de protocolo para o canal de colisão sem realimentação*, Recife, 2011. Dissertação (Mestrado em Engenharia Elétrica) - Depto. de Eletrônica e Sistemas, UFPE.

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

[4] 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.

[5] V. C. da Rocha Jr. and J. S. de Lemos Neto, "Nonlinear binary codes derived from constacyclic Codes", *SBrT International Telecommunications Symposium*, Manaus, AM, págs. 1-4, Sept. 2010.

[6] J. R. Hernández, F. Pérez-González and J. M. Rodríguez, "The impact of channel coding on the performance of spatial watermarking for copyright protection", *in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1998 (ICASSP 98)*, Seattle, WA, vol. 5, pp. 2973-2976, May 1998.

[7] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Norwood, MA: Artech House, January 2000.

[8] M. Kuribayashi and H. Tanaka, "How to generate cyclically permutable codes from cyclic codes", *IEEE Trans, Inform. Theory*, vol. IT-52, no. 10, pp. 4660-4663, October 2006.

[9] F. Hartung and M. Kutter, "Multimedia watermarking techniques", *Proceedings of the IEEE*, vol. 87, no.7, pp.1079-1107, July 1999.

[10] V. C. da Rocha, Jr., "Maximum distance separable multilevel codes", *IEEE Trans. Inform. Theory*, vol.30, no.3, pp. 547-548, May 1984.

[11] 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.

[12] E. R. Berlekamp and J. Justesen, "Some long cyclic linear binary codes are not so bad", *IEEE Trans, Inform. Theory*, vol. IT-20, pp. 351-356, May 1974.

[13] W. W. Peterson and E. J. Weldon Jr., *Error-Correcting Codes*, MIT Press, 2nd Edition, 1972.