Sequências de Protocolo para o Canal de Colisão sem Realimentação

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

***Resumo*— O Canal de Colisão sem Realimentação (CCsR) é um modelo de canal proposto 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. Códigos ciclicamente permutáveis (CP) constituem uma solução natural para a construção de sequências de protocolo para o CCsR quando apenas uma fração do total de usuários está ativa num dado intervalo de tempo. Neste artigo, é demonstrado um teorema que permite o uso de códigos CP como um conjunto de sequências de protocolo eficientes, quer os códigos sejam ou não de peso constante. Por fim, é feita uma comparação entre algumas famílias de sequências de protocolo construídas a partir de códigos CP.**

***Palavras-Chave*— Canal de colisão sem realimentação, códigos de peso constante, códigos ciclicamente permutáveis, sequências de protocolo.**

***Abstract*— The collision channel without feedback (CCWFB) is a proposed channel model for situations in which a given number of users share the same communication channel for sending bit packets. In the CCWFB each user has a protocol sequence that determines the time intervals in which the user can send his packets. Cyclically permutable (CP) codes provide a natural solution to the construction of protocol sequences for the CCWFB when a fraction of the total number of users are active in a given time interval. In this paper, a theorem is proved on how CP codes can be used as a set of efficient protocol sequences, whether the codes are constant-weight or not. Finally, a comparison is performed among some families of protocol sequences constructed by means of CP codes.**

***Keywords*— Collision channel without feedback, constant-weight codes, cyclically permutable codes, protocol sequences.**

I. INTRODUÇÃO

O Canal de Colisão sem Realimentação (CCsR) é um modelo de canal proposto [1], [2] 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. Códigos ciclicamente permutáveis (CP) [3] constituem uma solução natural para a construção de sequências de protocolo para o CCsR quando M usuários, num total de U usuários, estão ativos num dado intervalo de tempo. Algumas famílias de sequências de protocolo foram propostas na literatura [4]-[6], baseadas em códigos CP derivados de códigos cíclicos Reed-Solomon [4], BCH [5] e códigos constacíclicos [7]. Tais famílias de sequências de protocolo são aqui designadas como *Sequências-RS*, *Sequências-BCH* e *Sequências-Constacíclicas*, respectivamente. Um dos objetivos deste artigo é mostrar como códigos CP podem ser usados como sequências de protocolo para o CCsR, quer tais códigos sejam ou não de peso constante. Adicionalmente, são comparados os parâmetros das sequências de protocolo propostas em [4] e [5] com aquelas propostas em [6] e [7].

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. 304696/2010-2 e da Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), Proj. IBPG-0288-0.34/10.

O restante do artigo está organizado do seguinte modo. A Seção II contém alguns conceitos básicos e a Seção III aborda sucintamente as principais características do CCsR, incluindo um caso particular em que M usuários, de um total de U, $M < U$, estão ativos. Na Seção IV demonstra-se um teorema que permite o uso de códigos CP, de peso constante ou não, como um conjunto de sequências de protocolo. Além do mais, são apresentados os parâmetros das sequências de protocolo de interesse neste artigo e outros parâmetros são deduzidos para serem usados comparativamente. A Seção V apresenta uma comparação de famílias de sequências de protocolo derivadas de códigos CP, em função dos respectivos parâmetros, e na Seção VI são apresentadas as conclusões deste artigo.

II. CONCEITOS BÁSICOS

A seguir são apresentadas as definições de ordem cíclica, de código ciclicamente permutável e de representação-$\mathbf{V}$ [7].

A. Ordem cíclica: 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. A ordem cíclica de uma N-upla é igual a N ou igual a um dos seus divisores. O termo ordem cíclica plena refere-se ao caso em que $i = N$ é o menor número inteiro positivo tal que $\mathbf{S}^i(\mathbf{b}) = \mathbf{b}$.

B. Código Ciclicamente Permutável: É um código de bloco binário em que as palavras-código possuem ordem cíclica plena e são ciclicamente distintas [3]. 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. A distância mínima cíclica, d_c, de um código CP é definida como a menor distância de Hamming entre uma palavra-código $\mathbf{c}$ e os seus distintos deslocamentos cíclicos ou algum deslocamento cíclico de uma outra palavra-código $\mathbf{c}'$.

C. Representação-$\mathbf{V}$: Seja $\mathbf{v}$ uma $(p-1)$-upla binária cuja ordem cíclica é igual a $p-1$ e seja GF(p) um corpo finito, cujos elementos não-nulos são representados pelas potências a^i, $i = 0, 1, \ldots, p-2$, em que a denota um gerador do grupo multiplicativo de GF(p).

Definição 1: Define-se a *representação*-$\mathbf{V}$ para os elementos de $\mathrm{GF}(p)$ associando um-a-um seus elementos não-nulos a^i com as $(p-1)$-uplas binárias distintas $\mathbf{S}^i(\mathbf{v})$, $i = 0, 1, 2, \ldots, p-2$. O elemento 0 de $\mathrm{GF}(p)$ é representado por uma $(p-1)$-upla binária $\mathbf{v}'$ e seus deslocamentos cíclicos tais que $\mathbf{S}^j(\mathbf{v}') \neq \mathbf{S}^i(\mathbf{v})$, $0 \leq i, j \leq p-2$. Em particular, $\mathbf{v}'$ pode ser escolhida como a $(p-1)$-upla toda nula.

A distância mínima $d(\mathbf{v})$, da representação-$\mathbf{V}$, é a menor distância de Hamming entre as $(p-1)$-uplas binárias desta representação.

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

III. O CANAL DE COLISÃO SEM REALIMENTAÇÃO (CCSR)

No CCsR [1], [2], de forma compartilhada, os usuários emitem informação na forma de pacotes cujos valores são elementos de $\mathrm{GF}(Q)$, e geralmente um valor elevado de Q é usado. Cada pacote possui uma duração fixa de T segundos. Os usuários particionam o tempo dos seus respectivos relógios em intervalos de tempo com duração de T segundos e os seus pacotes devem ser transmitidos alinhados com estes intervalos.

No CCsR, devido à ausência de um elo de realimentação e da defasagem entre os relógios dos usuários, não é possível, por exemplo, compartilhar o canal em um modo de transmissão por divisão de tempo (TDMA)[8, p. 371]. Além do mais, a ausência de um elo de realimentação não permite que os usuários tenham alguma informação sobre as mensagens enviadas em intervalos de tempo anteriores. A saída do CCsR corresponde a uma das três situações possíveis: *silêncio*, *colisão* e *mensagem*. O "silêncio" indica que, num dado intervalo de tempo, não há emissão de pacotes por parte dos usuários, ou seja, não há nenhum usuário ativo. A "colisão" indica que mais de um usuário está ativo emitindo pacotes no mesmo intervalo de tempo. E, por último, a "mensagem" indica que, num dado intervalo de tempo, um único usuário está ativo emitindo pacotes.

No CCsR, cada usuário possui uma sequência de protocolo binária de comprimento N. Para o usuário i, a sequência de protocolo é denotada por $\mathbf{s}_i = \{s_{i_l}\}_{l=1}^{N}$. A sequência de protocolo determina quando o usuário i é permitido utilizar o canal e ela é independente dos pacotes enviados. A sequência de protocolo controla a emissão de pacotes do usuário i conforme explicado a seguir. No j-ésimo intervalo de tempo, se $s_{i_j} = 1$, $1 \leq j \leq N$, então é permitido que o usuário use o canal. Caso contrário, $s_{i_j} = 0$, o usuário não tem permissão para usar o canal e, desta forma, permanece em silêncio durante o j-ésimo intervalo de tempo. O usuário i continua a usar periodicamente sua sequência de protocolo, $\mathbf{s}_i$, até que não tenha mais pacotes para emitir. Após esse tempo de atividade, o usuário i deve permanecer inativo por, no mínimo, $N-1$ intervalos de tempo para poder voltar a emitir pacotes. Para o CCsR, um *quadro* corresponde ao período de uma sequência de protocolo que é igual a N intervalos de tempo. Assim, se $\mathbf{s}_i$ tem peso de Hamming w, então o usuário i é capaz de enviar w pacotes por quadro. Sob certas restrições de uso do canal, o usuário i codifica os seus próprios pacotes, assim transmitindo pacotes redundantes, de tal forma que alguns dos seus pacotes perdidos em colisões possam, em condições específicas, ser recuperados no receptor.

A. Um caso particular

Em [4] 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 do 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 total de informação máxima obtida nesta situação é dada por [4]

$$R_{\mathrm{sum}} = \frac{M\sigma}{N} \quad \text{(pacotes/intervalo de tempo).} \tag{1}$$

IV. SEQUÊNCIAS DE PROTOCOLO

Em [4] as sequências de protocolo propostas são obtidas, exclusivamente, por meio de códigos CP de peso constante, ou seja, todas a palavras do código CP possuem o mesmo peso de Hamming. Uma abordagem complementar ao trabalho apresentado em [4] utiliza códigos ciclicamente permutáveis de peso não-constante [6], [7] para obter sequências de protocolo. Códigos CP de peso não-constante permitem que usuários distintos usem sequências de protocolo com diferentes *fatores de trabalho*. O fator de trabalho λ_i do usuário i, $1 \leq i \leq U$, é definido como a fração de tempo em que a sua sequência de protocolo assume o valor 1 [2]. Então, para sequências de protocolo provenientes das palavras de um código CP de comprimento N, pode-se, alternativamente, definir o fator de trabalho λ_i, para o usuário i, como a razão entre o peso w_i da palavra-código, correspondente à sequência de protocolo, e o comprimento N das palavras-código, logo $\lambda_i = w_i/N$. Se o código CP for de peso constante, então todos os usuários possuem o mesmo fator de trabalho dado por $\lambda = w/N$.

O Teorema 4 em [4] estabelece condições para códigos CP de peso constante serem usados como sequências de protocolo para o CCsR. Além do mais, permite calcular os valores de M e σ neste caso. Entretanto, para o caso de códigos CP de peso não-constante, que não é abordada em [4], é necessário estabelecer um novo resultado. Com esse intuito, o Teorema 1, enunciado na sequência, estabelece um resultado para o cálculo de M e σ quando as palavras de um código CP, de peso constante ou não, são usadas como sequências de protocolo. Se o código CP for de peso constante, então o Teorema 1 resulta equivalente ao Teorema 4 em [4].

Definição 2: A **correlação** entre duas N-uplas binárias é definida como o número de coordenadas em que ambas possuem o valor 1.

Lema 1: Em um código ciclicamente permutável de peso não-constante, CCP(N, M_c, d_c), a *correlação*, denotada por ρ, entre qualquer palavra-código e seus deslocamentos cíclicos ou entre quaisquer deslocamentos cíclicos de duas palavras-código distintas satisfaz $\rho \leq w_{\max} - d_c/2$, em que $w_{\max}$ denota o maior peso de Hamming dentre as palavra do código.

Demonstração: Para duas N-uplas binárias quaisquer, cuja distância de Hamming seja d, e que possuam pesos de Hamming w_i e w_j, respectivamente, o número de 1's em que elas coincidem é exatamente $(w_i + w_j)/2 - d/2$. Sendo as N-uplas binárias palavras de um código CP, sendo $w_{\max}$ o maior peso de Hamming dentre as palavras-código e sendo d_c a distância mínima cíclica, então o valor máximo para a correlação entre duas palavras do código é obtido quando ambas possuem peso $w_{\max}$. Assim, $\rho = w_{\max} - d_c/2$. Portanto, a correlação entre quaisquer deslocamentos cíclicos de duas palavras-código distintas satisfaz $\rho \leq w_{\max} - d_c/2$. ■

Teorema 1: 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

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

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

Demonstração: Inicialmente, considere a estratégia pela qual o receptor é capaz de identificar os usuários cujos pacotes foram recebidos com sucesso. Para isto, considere o conjunto $\mathcal{W}$ cujos elementos são os pesos de Hamming das sequências de protocolo dos U usuários do canal e considere um quadro arbitrário de comprimento N que é processado pelo receptor em um instante de tempo também arbitrário. Seja $\tau = [\tau_1, \tau_2, \ldots, \tau_N]$ a N-upla binária que representa o *vetor atividade de transmissão*, em que τ_j, $1 \leq j \leq N$, assume valores 0 ou 1 e é recebido no j-ésimo intervalo de tempo desse quadro. Se $\tau_j = 0$, houve "silêncio" no j-ésimo intervalo de tempo, caso contrário, se $\tau_j = 1$, houve uma "mensagem" ou uma "colisão". O receptor decide se o usuário i está ativo no quadro recebido se e somente se os valores de j para os quais $\tau_j = 1$ coincidem com os valores de l para os quais $s_{i_l} = 1$, $1 \leq l \leq N$, em que $\mathbf{s}_i = \{s_{i_l}\}_{l=1}^{N}$, $1 \leq i \leq U$, denota a sequência de protocolo do usuário i. Se o usuário i, de fato, estiver ativo no quadro, então a regra de decisão descrita estará sempre correta. No entanto, se o usuário i não estiver ativo no quadro, então a regra de decisão utilizada falhará. Para deduzir uma condição suficiente assegurando que o usuário i não está ativo em um quadro arbitrário, considere um número M de usuários ativos cujas sequências de protocolo possuem peso arbitrário, não necessariamente iguais, mas que pertencem a $\mathcal{W}$, e considere, ainda, que a sequência de protocolo do usuário i tem peso igual a $w_i \in \mathcal{W}$. Portanto, se o usuário i não estiver ativo no quadro, quando no máximo M usuários estão ativos, e ρ denota o número máximo de 1's em que as sequências de protocolo dos M usuários coincidem, uma por vez, com os 1's em $\mathbf{s}_i$, então $M\rho < w_{\min}$ é uma condição suficiente para identificar corretamente que o usuário i não está ativo, qualquer que seja o $w_i \in \mathcal{W}$. Porém, do Lema 1 tem-se $\rho \leq w_{\max} - d_c/2$, porque a sequência de protocolo de cada usuário pode estar deslocada ciclicamente. Assim resulta que $M(w_{\max} - d_c/2) < w_{\min}$ ou, equivalentemente, $M(w_{\max} - d_c/2) \leq w_{\min} - 1$ é uma condição suficiente para identificar corretamente os usuários ativos por quadro. Nessa condição, o número de usuários ativos M é dado por

$$M = \left\lfloor \frac{w_{\min} - 1}{w_{\max} - d_c/2} \right\rfloor. \quad (3)$$

No próximo passo é estabelecida uma condição suficiente para que cada um dos M usuários ativos, por quadro, possa enviar no mínimo σ pacotes, que são recebidos livres de colisão. Para isto, suponha que o usuário i está ativo. Como os pacotes dos demais $M-1$ usuários ativos podem colidir com, no máximo, $w_{\max} - d_c/2$ pacotes enviados pelo usuário i, o usuário i tem a garantia de que $w_{\min} - (M-1)(w_{\max} - d_c/2)$ dos seus pacotes chegam ao receptor sem sofrer colisão, qualquer que seja o peso $w_i \in \mathcal{W}$ da sequência de protocolo do usuário i. Logo, $\sigma \geq w_{\min} - (M-1)(w_{\max} - d_c/2)$ ou, equivalentemente,

$$M = \left\lfloor \frac{w_{\min} - \sigma}{w_{\max} - d_c/2} \right\rfloor + 1. \quad (4)$$

Por fim, é trivial que a condição $M \leq U$ seja satisfeita e, portanto, se o valor de M é o mínimo entre U e os valores inteiros dados em (3) e (4), então o receptor é capaz de identificar corretamente os usuários ativos por quadro e cada um deles tem a garantia de poder enviar σ pacotes que são recebidos livres de colisão. Porém, as expressões (3) e (4) são deduzidas considerando o pior caso, pois é possível situações em que só há usuários ativos que possuem sequências de protocolo com peso $w_{\min}$ e, então, o número de usuários ativos é maior que o valor calculado em (3) e (4). Logo, justifica-se a desigualdade em (2) e a condição de igualdade ocorre quando o código CP é de peso constante. ■

A. Sequências-BCH e Sequências-RS

Segundo [5], os parâmetros (U, M, N, σ) das sequências-BCH são $U = p^{(k-2)r}, N = p(p^r - 1)$ e M em função de σ é dado por

$$M = \min\left\{U, \left\lfloor \frac{w - 1}{w - d_c/2} \right\rfloor, \left\lfloor \frac{w - \sigma}{w - d_c/2} \right\rfloor + 1\right\}, \quad (5)$$

em que p é um número primo tal que $p \geq 5$, e r e k são números inteiros tais que $r \geq 1$ e $3 \leq k \leq p-1$. As sequências de protocolo são palavras de um código CP de peso constante com $w = p^r - 1$ e $d_c \geq 2(p^r - 1 - (k-1)p^{r-1})$. É demonstrado em [5] que, para $r = 1$, as Sequências-BCH equivalem às Sequências-RS [4], considerando os códigos Reed-Solomon com comprimento do bloco máximo igual a $p - 1$.

Segundo [9], o limitante superior para o valor de M é deduzido considerando o número máximo de usuários ativos que podem transmitir, no mínimo, um pacote que seja recebido livre de colisão em um quadro de comprimento N. Assim, para $\sigma = 1$, o segundo termo do lado direito em (5) é o menor. Logo, substituindo w por $p^r - 1$ e d_c por $2(p^r - 1 - (k-1)p^{r-1})$

resulta $M \geq \left\lfloor \frac{(p^r-1)-1}{(p^r-1)-[p^r-1-(k-1)p^{r-1}]} \right\rfloor = \left\lfloor \frac{p^r-2}{(k-1)p^{r-1}} \right\rfloor$. Para valores elevados de p, o valor de M é aproximadamente igual a $\lfloor p/(k-1) \rfloor$, em que $\lfloor x \rfloor$ é o maior número inteiro positivo tal que $\lfloor x \rfloor \leq x$. Se este resultado for utilizado para avaliar o número de usuários ativos, então, no máximo, $\lfloor p/2 \rfloor = (p-1)/2$ podem estar ativos, uma vez que $3 \leq k \leq p-1$.

Em [5], para deduzir o limitante inferior para o valor de R_{sum}, o primeiro passo é avaliar para quais valores de σ, no lado direito de (5), o terceiro termo é o menor. Para isto, o segundo e o terceiro termos do lado direito de (5) podem ser reescritos, respectivamente, como $m_1 \leq \frac{w-1}{w-d_c/2}$ e $m_2 \leq \frac{w-\sigma}{w-d_c/2} + 1 = \frac{2w-\sigma-d_c/2}{w-d_c/2}$. Para que ocorra $m_2 \leq m_1$, é suficiente que $(2w-\sigma-d_c/2) \leq (w-1)$, o que implica em $\sigma \geq w+1-d_c/2$. Logo, para $\sigma \geq (k-1)p^{r-1}+1$, o terceiro termo é o menor. Portanto, $M \geq \left\lfloor \frac{w-\sigma}{(k-1)p^{r-1}} \right\rfloor + 1 > \frac{w-\sigma}{(k-1)p^{r-1}}$, e quando substituído em (1) resulta em $R_{\text{sum}} \geq \frac{\sigma(w-\sigma)}{N(k-1)p^{r-1}}$, cujo valor é máximo para $\sigma = w/2$, desde que $(w/2) \geq (k-1)p^{r-1}+1$. Logo, sendo $N = p(p^r-1) = pw$, resulta $R_{\text{sum}} \geq \frac{(w/2)(w-w/2)}{pw(k-1)p^{r-1}} = \frac{p^r-1}{4(k-1)p^r}$, que para valores elevados de p pode ser aproximada para $\frac{1}{4(k-1)}$.

B. Sequências-Constacíclicas

As Sequências-Constacíclicas podem ser obtidas por meio de códigos CP de peso constante ou não. A seguir, códigos CP de peso não-constante são usados para gerar as Sequências-Constacíclicas tipo-I e códigos CP de peso constante são usados para gerar as Sequências-Constacíclicas tipo-II.

1) Sequências-Constacíclicas tipo-I: Segundo [6], [7], os parâmetros (U, M, N, σ) das sequências baseadas em códigos CP de peso não-constante são $U = p^{k-2}, N = p^2-1$ e M em função de σ é dado por

$$M \geq \min\left\{U, \left\lfloor \frac{w_{\min}-1}{w_{\max}-d_c/2} \right\rfloor, \left\lfloor \frac{w_{\min}-\sigma}{w_{\max}-d_c/2} \right\rfloor + 1\right\}, \quad (6)$$

em que p é um número primo tal que $p \geq 5$ e k é um número inteiro par tal que $4 \leq k \leq q-1$. 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-**V** e $d(\mathbf{v})$ denota sua distância mínima.

Para obter-se o limitante superior para M, segue-se o mesmo procedimento aplicado às Sequências-BCH com a hipótese adicional de que todos os usuários ativos, num determinado quadro, possuam sequências de protocolo que correspondem a palavras do código CP com peso igual a $w_{\min}$. Tal hipótese corresponde a substituir $w_{\max}$ por $w_{\min}$ em (6) que, nesse caso, é satisfeita com igualdade. Além do mais, para palavras do código CP com peso igual a $w_{\min}$, $d(\mathbf{v}) = 2$. Assim, para $\sigma = 1$, $w_{\max} = w_{\min}$ e $d(\mathbf{v}) = 2$, obtém-se $M \geq \left\lfloor \frac{(p+1)-1}{(p+1)-(p-k+2)} \right\rfloor = \left\lfloor \frac{p}{(k-1)} \right\rfloor$. Logo, se este resultado for utilizado para avaliar o número de usuários ativos, então, no máximo, $\lfloor p/3 \rfloor$ podem estar ativos, uma vez que $4 \leq k \leq p-1$.

Na dedução do limitante inferior para R_{sum}, o primeiro passo é avaliar para quais valores de σ, no lado direito em (6), o terceiro termo é o menor. Seguindo o mesmo procedimento utilizado para as Sequências-BCH, obtém-se $\sigma \geq w_{\max}+1-d_c/2$. Como $d(\mathbf{v}) \geq 2$ para $w(\mathbf{v}') \geq 3$, resulta $\sigma \geq (k-1)w(\mathbf{v}')+1$ e o terceiro termo é o menor. Assim $M \geq \left\lfloor \frac{w_{\min}-\sigma}{(k-1)w(\mathbf{v}')} \right\rfloor + 1 > \frac{w_{\min}-\sigma}{(k-1)w(\mathbf{v}')}$, que quando substituído em (1) resulta em $R_{\text{sum}} \geq \frac{\sigma(w_{\min}-\sigma)}{N(k-1)w(\mathbf{v}')}$, cujo valor é máximo para $\sigma = w_{\min}/2$, desde que $(w_{\min}/2) \geq (k-1)w(\mathbf{v}')+1$. Logo, sendo $N = p^2-1 = (p+1)(p-1) = w_{\min}(p-1)$, resulta $R_{\text{sum}} \geq \frac{(w_{\min}/2)(w_{\min}-w_{\min}/2)}{w_{\min}(p-1)(k-1)w(\mathbf{v}')} = \frac{(p+1)}{4(p-1)(k-1)w(\mathbf{v}')}$, que para valores elevados de p pode ser aproximada para $\frac{1}{4(k-1)w(\mathbf{v}')}$.

2) Sequências-Constacíclicas tipo-II: Em [6], [7], os parâmetros (U, M, N, σ) das sequências baseadas em códigos CP de peso constante são $U = A_{p+1}/N, N = p^2-1$ e M em função de σ é dado por

$$M = \min\left\{U, \left\lfloor \frac{w-1}{w-d_c/2} \right\rfloor, \left\lfloor \frac{w-\sigma}{w-d_c/2} \right\rfloor + 1\right\}, \quad (7)$$

em que p é um número primo tal que $p \geq 5$, k é um número inteiro par tal que $4 \leq k \leq p-1$ e o valor de A_{p+1} é dado em [10, pág. 189]. As sequências de protocolo são palavras de um código CP de peso constante com $w = p+1$ e $d_c = 2(p-k+2)$. O limitante superior para o valor de M é o mesmo deduzido para as Sequências-Constacíclicas tipo-I, pois a hipótese assumida, naquele ponto, de que todos os usuários ativos possuem sequências de protocolo que são as palavras do código CP com peso igual a $w_{\min}$, corresponde às Sequências-Constacíclicas tipo-II. Logo, $M \leq \lfloor p/3 \rfloor$.

A dedução do limitante inferior para o valor de R_{sum} segue o procedimento já apresentado anteriormente para as outras sequências. Dessa forma, $\sigma \geq w+1-d_c/2$. Logo, para $\sigma \geq k$, o terceiro termo, do lado direito de (7) é o menor. Assim resulta $M \geq \left\lfloor \frac{w-\sigma}{(k-1)} \right\rfloor + 1 > \frac{w-\sigma}{k-1}$, que quando substituído em (1), resulta em $R_{\text{sum}} \geq \frac{\sigma(w-\sigma)}{N(k-1)}$, cujo valor é máximo para $\sigma = w/2$, desde que $(w/2) \geq k$. Logo, sendo $N = p^2-1 = (p+1)(p-1) = w(p-1)$, resulta $R_{\text{sum}} \geq \frac{(w/2)(w-w/2)}{w(p-1)(k-1)} = \frac{(p+1)}{4(p-1)(k-1)}$, que para valores elevados de p pode ser aproximada para $\frac{1}{4(k-1)}$.

V. Comparação das Sequências de Protocolo

De acordo com [9], 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.

A. Análise dos Parâmetros das Sequências

A Tabela I resume os parâmetros para comparação das sequências apresentadas e que são discutidos a seguir. Como todas as sequências de protocolo analisadas neste artigo são

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 $r > 1$.

Critérios	**Sequências**			
	Constacíclica tipo-I	Constacíclica tipo-II	RS	BCH
Limitante inferior para R_{sum}	$\frac{1}{4(k-1)w(\mathbf{v}')}$	$\frac{1}{4(k-1)}$	$\frac{1}{4(k-1)}$	$\frac{1}{4(k-1)}$
Limitante superior para M	$\lfloor p/3 \rfloor$	$\lfloor p/3 \rfloor$	$\lfloor p/2 \rfloor$	$\lfloor p/2 \rfloor$
Nº de sequências geradas (U)	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-p	$p(p^r-1)$
Diferentes fatores de trabalho	*sim*	*não*	*não*	*não*

obtidas por meio códigos CP, isto implica que quando os pacotes chegam ao receptor num dado quadro de transmissão, é possível distinguir os usuários ativos sem a necessidade de cabeçalhos de identificação [9]. A sequência de protocolo de cada usuário pode ser identificada, mesmo que seja recebida com algum deslocamento cíclico, uma vez que a sequência resultante de um deslocamento cíclico é diferente dela mesma e da sequência de protocolo de cada um dos outros usuários. É também desejável que as sequências de protocolo deem suporte a usuários com diferentes fatores de trabalho [9], pois diferentes sensores ou estações de trabalho, podem necessitar de usuários com diferentes taxas de transmissão. Dentre as sequências apresentadas, só as Sequências-Constacíclicas tipo-I possuem tal característica, pois o código CP utilizado não é de peso constante.

O comprimento N do quadro utilizado nas transmissões também é um parâmetro importante porque quanto maior o comprimento do quadro, maior a complexidade de decodificação por intervalo de tempo [5]. As Sequências-Constacíclicas possuem comprimento $N = p^2-1$ que é aproximadamente o mesmo valor do comprimento das Sequências-RS, $N = p^2 - p$. Comparando com as Sequencias-BCH, cujo comprimento é $N = p(p^r - 1)$, as Sequências-Constacíclicas possuem comprimento bem inferior, principalmente, à medida que o valor de r aumenta. Por exemplo, para $p = 13$, $k = 4$ e $r = 2$, as Sequências-BCH têm $N = 2184$, enquanto que as Sequências-Constacíclicas e as Sequências-RS, para os mesmos valores de p e k, possuem $N = 168$ e $N = 156$, respectivamente.

Sequências-Constacíclicas tipo-I geram $U = p^{k-2}$ sequências distintas, enquanto que as Sequências-Constacíclicas tipo-II geram $U = A_{p+1}/N$ sequências distintas. Comparando o valor de U das Sequências-Constacíclicas tipo-I com o valor de U das Sequências-RS e Sequências-BCH, conclui-se que ele é igual ao valor da primeira e inferior ao valor da segunda, $U = p^{(k-2)r}$, principalmente para valores elevados de r. Já o valor de U das Sequências-Constacíclicas tipo-II, comparado com os valores de U das Sequências-Constacíclicas tipo-I, Sequências-RS e Sequências-BCH, é sempre inferior.

Sequências-Constacíclicas tipo-I e tipo-II 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 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 no caso das Sequências-Constacíclicas tipo-I 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, como mencionado anteriormente, as Sequências-Constacíclicas tipo-I são as únicas na literatura, obtidas por meio de códigos CP, que comportam usuários com diferentes fatores de trabalho.

VI. Conclusões

Por meio do Teorema 1, neste artigo são estabelecidas condições para códigos CP, sejam eles de peso constante ou não, serem usados como um conjunto de sequências de protocolo para o CCsR. O resultado das comparações feitas na Seção V mostra que as Sequências-Constacíclicas têm parâmetros similares às Sequências-RS e às Sequências-BCH, tendo como diferencial possibilitar que os usuários trasmitam dados com diferentes taxas entre si.

Referências

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

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

[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] 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.

[6] J. S. 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.

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

[8] Andreas F. Molisch, *Wireless Communications*, 2nd ed., John Wiley & Sons Ltd., 2011.

[9] W. S. Wong, "New protocol sequences for random-access channels without feedback", *IEEE Trans. Inform. Theory*, vol.53, no.6, pp. 2060–2071, June 2007.

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