

TRANSFORMAÇÕES LINEARES PARA CORREÇÃO DE SURTOS BIDIMENSIONAIS

R. M. Campello de Souza, A. N. Kauffman, M. A. C. Moraes e R. C. C. Lima

Grupo de Pesquisa em Comunicações - CODEC

Departamento de Eletrônica e Sistemas - UFPE

C.P. 7800, 50970-730, Recife PE

ricardo@npd.ufpe.br

Resumo - Neste trabalho, uma técnica para correção de erros em surtos bidimensionais é apresentada. O procedimento faz uso de transformações lineares que mapeiam tais surtos em uma série de configurações de erros aleatórios corrigíveis.

Abstract - In this paper, a new scheme for correcting two-dimensional bursts is introduced. The technique is based on the use of a family of linear transformations that implement a two-dimensional interleaving to transform the error patches into correctable random error patterns.

Palavras Chaves : Códigos restritos, capacidade de Shannon, métodos combinados, série geradora, surtos de erros.

1. INTRODUÇÃO

A técnica de entrelaçamento representa um procedimento comum no combate aos surtos de erros em sistemas digitais de transmissão e/ou armazenamento de informação. O problema de se projetar esquemas de entrelaçamento bidimensionais (2-D) eficientes foi considerado em [1] e [2], onde resultados interessantes foram obtidos através de buscas computacionais. Especificamente, arranjos de $Q \times Q$ bits foram considerados, onde cada linha é uma palavra de um código linear binário com capacidade de correção de erros aleatórios $t = 1$. Para corrigir um surto 2-D de erros com peso de Hamming Q , uma transformação é aplicada ao arranjo, espalhando as posições corrompidas de maneira que, na nova configuração, cada uma delas pertence a uma linha diferente do arranjo, o que permite a correção do surto. Um exemplo da técnica com um código possuindo $t = 2$ foi apresentado. Embora o problema seja elegantemente descrito em termos de particionamento de conjuntos e reticulados, nenhuma teoria foi formulada para explicar por que algumas transformações espalham adequadamente os surtos, enquanto outras não o fazem. Recentemente, Kauffman et alli [3] abordaram o problema e o formularam em termos de transformações lineares, com o objetivo de esboçar uma teoria geral que estabelecesse condições para a construção de mapeamentos capazes de espalhar surtos 2-D de peso Q . Apenas o caso particular de arranjos $Q \times Q$ e surtos isolados foi considerado.

Neste trabalho, a abordagem é revista e uma teoria geral é apresentada, considerando arranjos $M \times N$, bem como a ocorrência de surtos 2-D múltiplos. Neste contexto, os conceitos preliminares relacionados com o problema são descritos na seção 2, onde um surto 2-D é caracterizado geometricamente. Na seção 3, o problema da construção de transformações que

levam ao espalhamento correto do surto de erros é resolvido via aritmética modular, incluindo o caso do chamado entrelaçamento perfeito. A generalização do esquema para correção de surtos 2-D múltiplos através de códigos lineares com capacidade t de correção de erros aleatórios é apresentada na seção 4. As conclusões referentes à pesquisa relatada neste trabalho são apresentadas na seção 5.

2. PRELIMINARES

No que se segue $C(n, k, d)$, ou simplesmente C , denota um código de bloco linear binário de comprimento n , dimensão k , distância mínima de Hamming d e capacidade de correção de erros aleatórios t , onde $d = 2t + 1$. Com o objetivo de corrigir surtos, um subconjunto de M palavras-código de C é escrito como um arranjo A de $M \times N$ bits. Na maior parte deste trabalho, o caso $t = 1$ é considerado, de maneira que o esquema é projetado para corrigir surtos de erros de peso menor ou igual a M . Por um surto de erros de peso M , compreende-se aqui um surto 2-D que corrompe w elementos de A , onde $w \leq M$. Para descrever a característica de aglomeração dos erros, vamos adotar um modelo de surtos retangulares, o que significa que as posições em erro formam uma submatriz R , de A , de dimensões r e s , onde $rs = M$, ou eles podem ser cobertos minimalmente por R (Figura 1).

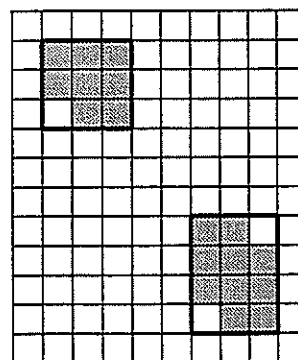


FIG. 1: Surtos de pesos $w = 8$ (quadrado : $r = s = 3$) e $w = 10$ (retângulo : $r = 4, s = 3$).

O formato 2-D de surto citado acima pode ser descrito em termos simples e ainda assim é genérico o suficiente para incluir as situações de interesse prático. É importante observar neste ponto, que as posições afetadas envolvem linhas cujos valores são elementos do conjunto de inteiros $\{0, 1, \dots, M -$

1}, de modo que quaisquer operações envolvendo estas quantidades podem ser executadas módulo M . Um outro ponto importante, como será mostrado mais adiante, é o fato de que a localização precisa do surto dentro do arranjo é irrelevante, desde que ele satisfaça às condições mencionadas acima.

3. TRANSFORMAÇÕES LINEARES

Para construir famílias de transformações cuja ação sobre o surto seja espalhá-lo de maneira que o mesmo se torne uma série de M padrões de erros simples, usamos aritmética modular. O entrelaçamento 2-D utilizado é obtido mapeando-se o elemento da linha a e coluna b (denotado por (a, b)) no elemento (c, d) , através de

$$Z_M \oplus Z_N \longrightarrow Z_M \oplus Z_N$$

$$(a, b) \longmapsto (c, d) = T((a, b))$$

onde $T(\cdot)$ é a transformação linear definida pelos parâmetros e, f, g, h :

$$T = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \quad (1)$$

ou seja,

$$c = ae + bf \pmod{M}$$

e

$$d = ag + bh \pmod{M}$$

Lema 1 - Uma condição necessária e suficiente para $T(\cdot)$ ser uma transformação inversível é que $MDC[(eh - fg), M] = 1$.

Prova - Em forma matricial

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \quad (2)$$

Para T^{-1} ser definida, precisa-se garantir a existência do inverso multiplicativo $\delta \pmod{M}$, onde $\delta = eh - fg$, isto é, a congruência

$$(eh - fg)\delta^{-1} \equiv 1 \pmod{M}$$

deve apresentar uma única solução. Uma condição necessária e suficiente para isto é que $MDC[(eh - fg), M] = 1$ [4].

Teorema 1 - A transformação $T_1(r, s)$ de parâmetros $e = h = 1, f = \pm r, g = 0$, define um mapeamento bijetivo dos elementos de qualquer submatriz R de A (como definida acima) para as linhas de A .

Prova - Considerando que $MDC[(eh - fg), M] = MDC[1, M] = 1$, T é inversível. A posição em que R se encontra é irrelevante, uma vez que qualquer conjunto de r inteiros consecutivos $i, i+1, \dots, i+r-1$ é um conjunto completo de resíduos módulo r . Se $(i+x) \equiv (i+y) \pmod{r}$, com $0 \leq x, y \leq r-1$, então $x \equiv y \pmod{r}$, o que implica $x = y$.

De (2), o elemento (a, b) de A , $0 \leq a \leq r-1, 0 \leq b \leq s-1$, é mapeado na linha c , onde $c = a \pm br \pmod{M}$. De modo semelhante, $c' = a' + b'r \pmod{M}$. Se $c \equiv c' \pmod{M}$, então

$$a \pm br \equiv a' \pm b'r \pmod{rs} \quad (3)$$

ou seja, $a \pm br \equiv a' \pm b'r \pmod{r}$ o que implica $a \equiv a'$. Então (3) pode ser reescrita na forma $br \equiv b'r \pmod{rs}$, e assim $b \equiv b' \pmod{s}$ ou $b = b'$. Portanto, se $c \equiv c' \pmod{M}$, os elementos (a, b) e (a', b') são os mesmos.

Uma situação interessante ocorre quando as posições corrompidas ocupam, após a transformação, não apenas linhas distintas, mas também colunas distintas. É o chamado entrelaçamento perfeito (EP). No caso examinado acima, o entrelaçamento não será necessariamente perfeito, pois podemos ter $w > N$. O teorema 2 a seguir mostra que, quando $M = N$, a condição EP pode ser obtida escolhendo-se os parâmetros de (1) adequadamente.

Teorema 2 - Seja A um arranjo bidimensional de dimensões Mn , onde $M = N = rs$. A transformação $T_2(r, s)$ de parâmetros $e = h = 1, f = \pm r, g = \pm s$, define um mapeamento bijetivo dos elementos de qualquer submatriz R de A para as linhas e colunas de A .

Prova - A prova para o mapeamento das linhas segue os mesmos passos utilizados no teorema 1. O elemento (a, b) de A é mapeado na coluna d , onde $d = ag + bh \pmod{M}$. De modo análogo, $d' = a'g + b'h \pmod{M}$, $0 \leq a, a' \leq r-1, 0 \leq b, b' \leq s-1$. Se $d \equiv d' \pmod{M}$, então

$$as + b \equiv a's + b' \pmod{rs} \quad (4)$$

o que implica $as + b \equiv a's + b' \pmod{s}$ e portanto $b \equiv b' \pmod{s}$ ou $b = b'$. De (4), $as \equiv a's \pmod{rs}$, de modo que $a \equiv a' \pmod{r}$ ou $a = a'$. Em resumo, $c \equiv c' \pmod{M}$ e $d \equiv d' \pmod{M}$, se e somente se $a \equiv a' \pmod{M}$ e $b = b' \pmod{M}$, o que significa um entrelaçamento perfeito dos M bits de R .

Entrelaçamento perfeito significa que se as colunas de A são palavras de um código corretor de erros, então elas poderão ser usadas no processo de correção. Desta forma, criam-se alternativas para o esquema, no sentido de que se pode considerar, por exemplo, o uso de códigos na forma de arranjos bi-dimensionais.

4. SURTOS MÚLTIPLOS E CÓDIGOS COM $t > 1$

Utilizando-se nas linhas um código com capacidade de correção de t erros aleatórios, é possível corrigir surtos de peso $\leq tM$. A idéia básica é considerar aritmética módulo tM como se trabalhássemos num arranjo estendido com tM linhas. Desse modo, a transformação $T(r, s)$ do teorema 1 pode ser aplicada para espalhar os erros ao longo das linhas do arranjo estendido. Depois disso, é necessário reduzir módulo M todos os valores de linhas maiores que $M - 1$. Isto resultará em, no máximo, M palavras-código corrompidas com

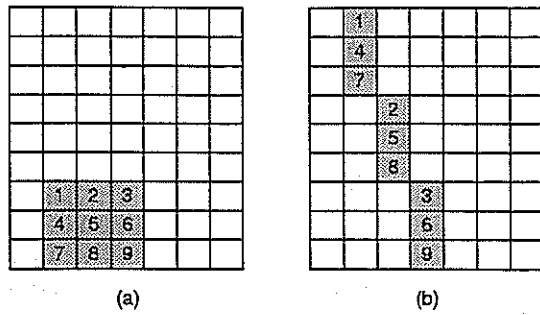


FIG. 2: (a) Surto 3x3 em um arranjo 9x7. (b) Surto espelhado. Cada uma das nove componentes ocupa uma linha diferente do arranjo.

padrões de erro de peso $\leq t$, os quais poderão então ser corrigidos. O mesmo procedimento pode ser considerado para arranjos quadráticos (isto é, $M = N$), quando então visualizamos o arranjo estendido tendo dimensões $tM \times tM$, resultando em não mais que t erros em cada linha e coluna do arranjo.

A correção de surtos múltiplos pode ser obtida como uma decorrência do teorema 1.

Colorário 1 - Seja A um arranjo com Mn bits, corrompido por p surtos retangulares, cada um com peso $\leq M$. Então as posições de A podem ser corrigidas através de $T_1(r, s)$ se o código C usado no esquema tem distância mínima $d = 2p+1$.

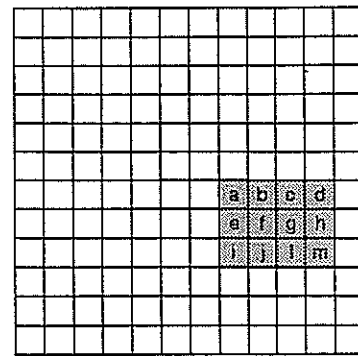
Prova - A aplicação de $T_1(r, s)$ espalhará todos os p surtos ao longo das M linhas de A , de modo que cada surto isolado afetará, no máximo, uma posição em cada linha do arranjo. Então cada linha irá conter não mais que p posições corrompidas, que podem ser corrigidas por C

5. EXEMPLOS

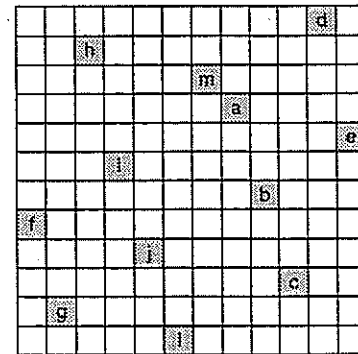
Nesta seção alguns exemplos são apresentados visando ilustrar os resultados obtidos anteriormente (teoremas 1 e 2, corolário 1).

Exemplo 1 - Um arranjo de dimensões $Mn = 9 \times 7$ é considerado, cujas linhas são palavras de um código corretor de erros com $t = 1$. A transformação $T = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ permite a correção de surtos bidimensionais $r \times s$ onde $r, s \leq 3$. Como $M > N$, os erros ocupam as mesmas colunas (Figura 2).

Exemplo 2 - Um arranjo de dimensões $Mn = 12 \times 12$ é considerado, cujas linhas são palavras de um código corretor de erros com $t = 1$. A transformação $T = \begin{bmatrix} 1 & 3 \\ 4 & 1 \end{bmatrix}$ permite a correção de surtos bidimensionais 3×4 (Figura 3). Como $M = N$, temos a condição de entrelaçamento perfeito (Figura 3)

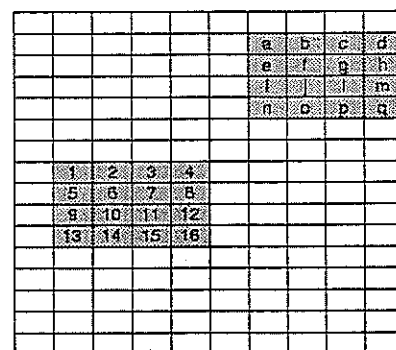


(a)

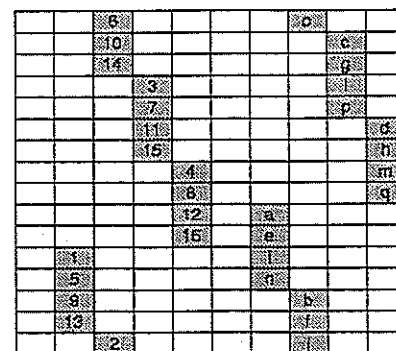


(b)

FIG. 3: (a) Surto 3x4 em um arranjo 12x12. (b) Surto espalhado. As doze componentes ocupam linhas e colunas diferentes do arranjo. É o chamado entrelaçamento perfeito.



(a)



(b)

FIG. 4: (a) Dois surtos 4x4 em um arranjo 16x10. (b) Surto espelhado. Cada uma das 16 linhas apresentam dois erros.

Exemplo 3 - Um arranjo de dimensões $Mn = 16 \times 10$ é

considerado, cujas linhas são palavras de um código corretor de erros com $t = 2$. A transformação $T = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$ permite a correção simultânea de dois surtos bidimensionais r e s , onde

$r, s \leq 4$. Como $M > N$, a transformação mantém as componentes do surto nas mesmas colunas (Figura 4).

6. CONCLUSÕES

Neste trabalho, a técnica de entrelaçamento bi-dimensional para controle de erros em surtos em arranjos Mn foi discutida. Um procedimento geral que descreve a construção de diferentes formas de surtos de interesse prático foi apresentada. O problema da construção de transformações lineares que conduzem ao espalhamento correto dos surtos foi abordado através de aritmética modular e condições necessárias e suficientes para a existência de tais transformações foram estabelecidas. Uma família geral de transformações foi introduzida, a qual permite a correção de surtos 2-D de peso $w \leq M$, e produz o chamado entrelaçamento perfeito nos casos em que $M = N$. A generalização do esquema usando-se um código linear com capacidade arbitrária de correção de erros aleatórios foi apresentada, bem como a correção de surtos múltiplos. Embora apenas códigos binários tenham sido considerados, a extensão do procedimento para códigos multítiplos, em qualquer das situações discutidas, pode ser feita de maneira direta.

REFERÊNCIAS

- [1] C. de Almeida, R. Palazzo Jr., Entrelaçamento Bi-dimensional Usando a Técnica do Particionamento de Conjuntos, Anais do XI Simpósio Brasileiro de Telecomunicações, vol. II, pp. 493-496, Natal, RN, Setembro 1993.
- [2] C. de Almeida, R. Palazzo Jr., Efficient Two-dimensional Interleaving Technique by Use of Set Partitioning Concept, Electronics Letters, vol. 32, no 6, pp. 538-540, march 1996.
- [3] A. N. Kauffman et alli, A Technique for Correcting Clusters of Errors, Proceedings of the International Telecommunications Symposium - ITS'96, pp. 64 - 66, Acapulco, México, october 1996.
- [4] D. M. Burton, Elementary Number Theory, Allyn and Bacon, 1976.

Ricardo Menezes Campello de Souza formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco em 1974, obteve o título de Mestre em Ciências pela mesma Universidade em 1979 e o título de PhD pela University of Manchester, Inglaterra, em 1983, ambos em Engenharia Elétrica. Desde 1979 é Professor do Departamento de Eletrônica e Sistemas da UFPE, onde foi coordenador do Programa de Pós-graduação em Engenharia Elétrica no período 1984-1987, Chefe do Departamento no período 1987-1992 e atualmente ocupa a posição de Professor Adjunto. Seus interesses

de pesquisa incluem matemática discreta, criptografia, teoria algébrica da codificação e processamento digital de sinais.

André Neumann Kauffman formou-se em Engenharia Elétrica, modalidade Eletrônica, pela Universidade Federal de Pernambuco em 1997, onde cursa atualmente o programa de Mestrado em Engenharia Elétrica. Seus interesses de pesquisa incluem matemática discreta, criptografia e processamento digital de sinais.

Maria Antonieta Carvalho de Moraes é concluinte do Curso de Graduação em Engenharia Elétrica, modalidade Eletrônica, da Universidade Federal de Pernambuco. Seus interesses de pesquisa incluem matemática discreta, criptografia e processamento digital de sinais.

Rossana Cláudia Cursino Lima é concluinte do Curso de Graduação em Engenharia Elétrica, modalidade Eletrônica, da Universidade Federal de Pernambuco. Seus interesses de pesquisa incluem matemática discreta, criptografia e processamento digital de sinais.