Construção de Geradores de Sequências utilizando os Códigos Alternantes sobre Anéis Locais

Ingrid Araújo Sampaio* **Yuzo Iano**
Departamento de Comunicação, DECOM, UNICAMP,
13083-970, Campinas, SP
E-mail: ingrid@decom.fee.unicamp.br, yuzo@decom.fee.unicamp.br,

Reginaldo Palazzo Junior
Universidade Estadual de Campinas- Departamento de Telemática
13083-970, Campinas, SP
E-mail: palazzo@dt.fee.unicamp.br.

RESUMO

Neste trabalho apresentamos uma alternativa de utilização da estrutura algébrica para encontrarmos o grupo das unidades. Como a cardinalidade do grupo das unidades de $\mathbb{Z}_m$, até onde é de nosso conhecimento, não guarda uma relação monotonicamente crescente com m e como em certas aplicações práticas necessita-se de valores grandes da cardinalidade consideramos a utilização de extensões Galoisianas de anéis locais para se atingir este objetivo. Contudo, diante da dificuldade, desenvolvemos algoritmos para a determinação do mesmo. Observando que, conhecida a cardinalidade de um determinado anel $\mathbb{Z}_{p^m}$, consequentemente a base p será conhecida, logo, podemos determinar a cardinalidade dos correspondentes anéis para subsequentes valores de m. Através do polinômio gerador obtido no grupo das unidades, notaremos que a sua cardinalidade está associada com o comprimento da palavra-código e que a realização da transformada discreta de Fourier está relacionada com a geração e codificação dos códigos cíclicos sobre anéis locais portanto, tem um dispositivo, registro de deslocamento com realimentação linear, ou seja, um gerador de sequências que vai realizar a transformada discreta de Fourier sobre anéis locais.

Com a utilização dos códigos alternantes, faremos a decodificação do mesmo onde precisaremos da síndrome para fazermos uso do algoritmo de Berlekamp-Massey modificado. Identificaremos o polinômio gerador para geração da seqüência e por meio dos registros de deslocamento com realimentação linear ou LFSR, obtermos os códigos cíclicos. Com isso, realizamos a transformada discreta de Fourier através do polinômio gerador dos códigos cíclicos sobre anéis locais, polinômio este que indica quantos módulos terão no circuito.

Palavras-chave: *Códigos Alternantes, Transformada Discreta de Fourier, Algoritmo de Berlekamp-Massey Modificado, Anéis Locais.*

Referências

[1] A. A. Andrade, R. Palazzo Jr., "Decoding of BCH and alternant codes by using Fourier transform in a Galois ring", *Int. J. Applied Mathematics,* Vol. 16, N. 1, pp.69-83, 2004.

[2] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, Owego, NY, 1984.

*bolsista de Doutorado / Fapesb

[3] J. C. Interlando, *Uma Contribuição a Construção e Decodificação de Códigos Lineares sobre Grupos Abelianos via Concatenação de Códigos sobre Anéis Inteiros Residuais*, Tese de Doutorado, FEEC-UNICAMP, 1994.

[4] R. Palazzo Jr., J. C. Interlando, J. R. Gerônimo, A. A. Andrade, O. M. Favareto, T. P. Nóbrega Neto, M. C. Araújo e G. O. Santos, *Fundamentos Algébricos e Geométricos dos Códigos Corretores de Erros*, DT-FEEC-UNICAMP, 2003.