CÓDIGOS CORRETORES DE ERROS E A NÃO EXISTÊNCIA DE CÓDIGOS PERFEITOS DESCONHECIDOS SOBRE CORPOS FINITOS

Maycon Gonçalves Carneiro[1], Santos Richard Bejarano Correio[2]

1-Acadêmico do curso de Licenciatura em Matemática da UTFPR; 2-Professor do curso de Licenciatura em Matemática da UTFPR.

Resumo - Códigos corretores de erros estão presentes sempre que fazemos uso de CDs, informações digitais e até mesmo em nossos documentos. Tais códigos são responsáveis por adicionar dados à uma mensagem que se queira transmitir ou armazenar, possibilitando-nos ao receber uma mensagem sabermos se a mesma está correta ou não. Assim, diversos estudos são realizados, principalmente por Matemáticos e Engenheiros Elétricos, os quais buscam códigos que corrijam o maior número de erros com o menor custo computacional. De grande importância é o teorema que mostra a não existência de códigos perfeitos desconhecidos sobre corpos finitos. Este trabalho visa mostrar-nos esse resultado. Assim, poupamos tempo em procurar códigos perfeitos somente em corpos infinitos.

Palavras-Chave: códigos perfeitos, não existência, desconhecidos, corpos finitos.

ERROR CORRECTING CODES AND THE NONEXISTENCE OF UNKNOWN PERFECT CODES OVER FINITE FIELDS

Abstract- Error correcting codes are always present when we use CDs, digital data and even our documents. Such codes are responsible for adding data to a message which should be transferred or saved, making it possible to know whether the message is correct or not when we receive it. Thus, several studies are carried out, mainly by mathematicians and electric engineers, which seek codes that correct the biggest numbers of errors with the smallest computational cost. The theorem that shows the non-existence of unknown perfect codes over finite fields has considerable importance. This paper aims to demonstrate this result. Hence, we save time searching perfect codes in infinite fields only.

KeyWord: perfects codes, nonexistence, unknown, finite fields.

1. INTRODUÇÃO

Segundo Hefez (2002), um código corretor de erros é um modo organizado de adicionar-se algum dado à uma mensagem que se queira transmitir, que possibilite, ao recuperar a informação, detectar e corrigir erros ou seja, diferente de criptografia, onde se introduz o erro, para que não se consiga decifrar a mensagem. O exemplo mais comum de código corretor de erros é um idioma. Por exemplo, uma palavra da língua portuguesa pode ser considerada como um elemento de A^27 , onde A é o alfabeto, já com as vogais acentuadas e cedilha e 27 é o comprimento da palavra mais longa da língua portuguesa. Vemos que esse é um código corretor de erros, pois se escrevermos "cathorro", sabemos que a palavra não existe, logo, foi cometido algum erro, mas não é um bom código pois se transmitirmos a palavra "rato" e cometermos um erro de tal forma que a mensagem seja recebida como "gato", não poderemos identificar o erro pois esta palavra também é uma palavra em nosso código, então, como as palavras estão muito próximas umas das outras temos pouca eficiência em nosso código.

Um bom código é aquele que corrige o maior número de erros, te tal forma que, sendo d a distância entre as palavras do código, e a pertencendo a A, considerando D o disco com centro em a e raio e, ao recebermos uma palavra c, esta encontra-se num disco de raio r <= e em torno

de uma palavra a do código. Já um código perfeito é aquele onde sendo C contido em A^n um código com distância mínima d e D o disco com centro em c e raio e, temos que:

$$U(c \text{ pertencente } C)\ D(c,e) = A^n ,$$

ou seja, qualquer palavra c que recebamos certamente estará em algum disco.

Este trabalho apresenta alguns parâmetros para códigos perfeitos, e apresenta resultados que mostram a não existência de códigos perfeitos desconhecidos para os demais parâmetros sobre corpos finitos.

2. MATERIAL E MÉTODOS

Estudando álgebra, geometria, e alguns conceitos de cálculo, podemos observar o comportamento de certos corpos ou seja, anéis munidos das operações de soma e multiplicação, onde todo elemento não nulo possui um inverso, bem como o comportamento dos códigos corretores sobre esses corpos, logo, de uso dessas ferramentas matemáticas podemos encontrar códigos perfeitos sobre alguns corpos.

Para chegarmos ao resultado do teorema que nos diz que não existem códigos perfeitos desconhecidos sobre corpos finitos, fazemos uso de alguns lemas que impõem condições e restrições sobre os parâmetros do código, para então provar o teorema para dois casos:

$$\text{(i) } n >= \text{œ } e^2 + e;$$
$$\text{(ii) } n < \text{œ } e^2 + e.$$

3. RESULTADOS E DISCUSSÃO

Alguns códigos perfeitos são conhecidos, como os códigos de Golay para os casos e = 2, q = 3, n = 11, e e = 3, q = 2, n = 23 (e=número de erros que o código corrige, n=comprimento, q=número de símbolos de A); os códigos perfeitos triviais nos casos n = e, e q =2, n = 2e+1; e os códigos perfeitos de erros singulares (códigos de Hamming). Então, alguns parâmetros nos permitem criar códigos perfeitos:

Com o resultado dos lemas que restringem os parâmetros do código, como por exemplo, o lema que nos diz que se existe um código corretor de e erros com comprimento n sobre um corpo GF(q) com (e < n) então

$$q <= (n-1)/e,$$

e o teorema provado para os dois casos de n, obtemos o resultado que não existem códigos perfeitos desconhecidos sobre corpos finitos logo, na procura pelos mesmos, descartamos tais corpos.

4. CONCLUSÕES

Visto que na Teoria da Informação os códigos corretores de erros ocupam um lugar significativo e muitas ferramentas matemáticas são usadas para o desenvolvimento dos mesmos, uma atenção maior deve ser dada ao estudo de procura códigos cada vez melhores, ou de códigos perfeitos. Visto as vantagens que os mesmos oferecem, bem como sua aplicação em diversas áreas, de grande importância são os resultados acima apresentados, pois poupam-nos tempo, logo, dinheiro.

REFERÊNCIAS

HEFEZ, A. **Curso de Álgebra**: Coleção Matemática Universitária. Volume 1. 2. ed. IMPA: Rio de Janeiro. 1993.

HEFEZ, A.; VILLELA, M. L. T. **Códigos Corretores de Erros**: Serie de Computação e Matemática. IMPA: Rio de Janeiro. 2002;

SILVA, J. G. Filho. **Informação, codificação e segurança de dados.** Universidade de Brasília. Disponível em:http://www.ene.unb.br/~juliana/cursos/teoriainf/codsec07.pdf Acesso em: 02 mai. 2008.

SOUZA, A. O.; CÂMARA, M. A. da. **Códigos Corretores de Erros Lineares**. Monografia. Uberlândia, 2006. 36p. Especialização (Matemática) - Faculdade de Matemática, UFU.

TIETÄVÄINEN, A. On the Nonexistence of Perfect Codes Over Finite Fields. SIAM: **Journal of Apllied Mathematics**, v.24, p.88 - 96, January 1963.