CONSTRUÇÃO DE CURVAS ALGÉBRICAS MAXIMAIS UTILIZANDO POLINÔMIOS ABSOLUTAMENTE IRREDUTÍVEIS

Givaldo Oliveira dos SANTOS (1); Thiago Jhonatha Fernandes SILVA (2)
(1) CEFET-AL/UNED-MD, Rua Lourival Alfredo, nº. 176, Marechal Deodoro – AL, CEP – 57160-000.
Tel.: (0xx) 82 3263-1122, e-mail: givaldodt@oi.com.br / givaldodt@ig.com.br
(2) CEFET – AL / UNED - MD, e-mail: thiagojhonatha@bol.com.br / thiagodga@oi.com.br.

RESUMO

Neste artigo apresentaremos resultados de implementação de algoritmos com base na pesquisa de **Santos (2003)** intitulada "Caracterização geométrica do processo de decodificação da classe dos códigos alternantes cíclicos através de polinômios absolutamente irredutíveis", na qual foi estabelecida uma relação de polinômios absolutamente irredutíveis e curvas, sobre corpos finitos. Nessa mesma pesquisa foram apresentadas as principais curvas algébricas utilizadas para construir códigos algébricos geométricos, isto é, curvas maximais. Salientamos, que a existência de curvas sobre corpos finitos com muitos pontos racionais (isto é, curvas maximais) possibilitam a construção de códigos ótimos. Portanto, os melhores códigos são aqueles construídos através de curvas com muitos pontos racionais, uma vez que o comprimento das palavras-código está diretamente relacionado a esse número. O problema principal de construir códigos algébrico-geométricos (AG) é encontrar uma maneira de executar as computações exigidas de uma forma mais rápida e eficiente no processo de transmissão de dados e de sinais, utilizando curvas maximais, proporcionando assim, uma ferramenta útil para a teoria de codificação (por exemplo, códigos algébrico-geométricos, códigos traço, empacotamento de esfera e códigos esféricos), como também, para outros ramos da teoria de informação. Fundamentados nessa pesquisa, propomos no nosso trabalho, estudar, montar, estabelecer e implementar algoritmos no software computacional Maple, utilizando curvas algébricas que determinem o número de pontos racionais e o número de pontos singulares através de polinômios absolutamente irredutíveis apresentados por **Santos** (2004). A partir destes resultados, iremos buscar implementações de algoritmos que determinem condições necessárias nos polinômios para que as curvas geradas sejam maximais. Esperamos que, o presente trabalho, possa contribuir para a construção de códigos que facilitem na correção de eventuais erros da transmissão de dados.

Palavras-chave: algoritmo, curvas algébricas maximais, polinômios absolutamente irredutíveis, pontos racionais, pontos singulares.

INTRODUÇÃO

Desde a sua introdução por Claude Shannon, a teoria de códigos corretores de erros tem tido inúmeras aplicações. Ela intervém todas as vezes que queremos transmitir ou estocar mensagens ou dados que estão sujeitos as interferências que causem erros na mensagem a ser lida posteriormente

Um dos fatos mais importantes na Teoria de Códigos Corretores de Erros nos últimos anos foi à introdução de métodos baseados em curvas algébrico-geométricas para a construção de códigos lineares. Esses códigos, denominados algébrico-geométricos (códigos AG), foram introduzidos pelo matemático russo Goppa (1981, pp.75-91), que ao invés de avaliar polinômios em pontos simples, poderiam ser avaliados em funções algébricas em pontos de curvas definidas sobre corpos finitos. Alem disso mostrou também como substituir a condição sobre graus dos polinômios pelas condições de funções algébricas. Salientamos ainda que a existência de curvas sobre corpos finitos com muitos pontos racionais (isto é, curvas maximais) possibilitando a construção de códigos ótimos. Desta forma, os melhores códigos são aqueles construídos através de curvas com muitos pontos racionais, uma vez que o comprimento das palavras-código está diretamente atribuído a esse numero. O problema principal em se construir códigos algébrico-geométricos é praticamente encontrar uma forma de executar as computações exigidas de uma forma mais rápida e eficiente no processo de transmissão de dados e de sinais.

A figura 1, ilustra o modelo tradicional de um sistema de comunicações digital. Este sistema de comunicações conecta uma fonte a um destinatário através de um canal o qual poderá ser um cabo coaxial, uma fibra óptica, uma fita ou disco magnético, o espaço, etc.

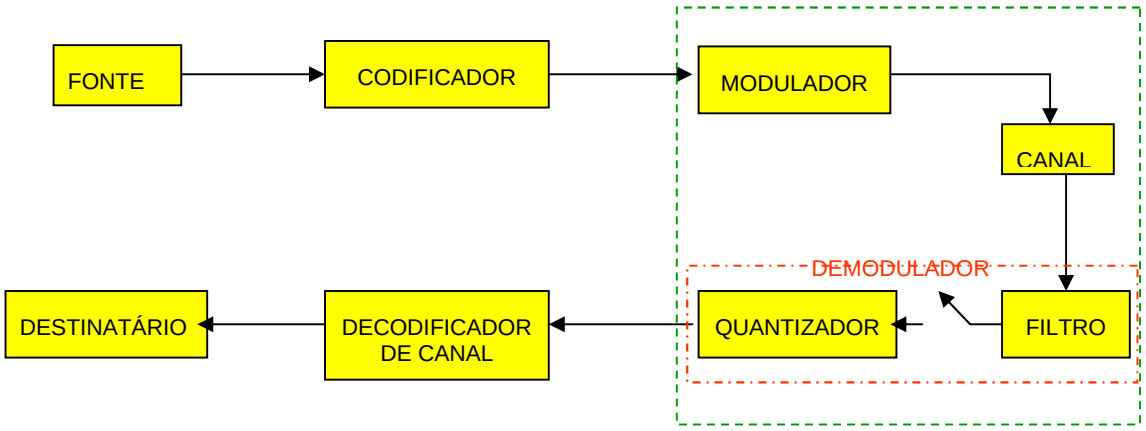

Figura 1 – Modelo de um sistema de comunicação digital

O **decodificador de canal** transforma a seqüência recebida em uma seqüência binária chamada **seqüência estimada**. O ideal seria que fosse uma replica fiel da seqüência de informação, mesmo que o ruído do canal tivesse introduzido erros. A outra componente do decodificador é o **decodificador de fonte** que transforma a seqüência estimada em uma seqüência estimada do mesmo tipo da saída da fonte e a envia ao destinatário.

A teoria dos códigos é um dos ramos da matemática em franca atividade, neste projeto de pesquisa estabelecemos uma adaptação de algoritmos para determinar pontos racionais e pontos singulares de uma curva algébrica e apresentaremos exemplos de curvas algébricas geradas por polinômios que sejam maximais. Trabalhamos também para obtermos implementações de algoritmos com o software Maple® para gerarmos pontos singulares e pontos racionais através dos polinômios construídos por SANTOS (2003).

PRELIMINARES

A – Curvas Algébricas

A descoberta da conexão entre a teoria da equação e os outros campos da matemática, como álgebra, geometria e analise, teve início no século XIX. Isso foi comprovado pelas investigações executadas por Lagrange, Gauss e Hermite nas teorias de formas quadráticas, investigações essas que culminaram na

criação da aritmética de corpos quadráticos e serviram como base para aproximar grupos matemáticos. Exemplos disso são os trabalhos de Kummer, que estudou a equação de Fermat $x^n+y^n=z^n$ e teve como resultado a criação da aritmética de corpos ciclotomicos (e assim foi desenvolvida a teoria de idéias para os corpos de números algébricos) e, finalmente, pelos resultados de Jacobi, relativos à aplicação dos teoremas de Euler e Abel na composição de integrais elípticas e abelianas para a adição de pontos racionais em curvas algébricas que estenderam os fundamentos para a aritmética de variedades Abelianas. Ao mesmo tempo, uma analogia próxima foi descoberta entre os corpos de números algébricos e as de funções analogia próxima foi descoberta entre os corpos de números algébricos e esses de funções algébricas, que conduziu, por um lado, à criação da teoria aritmética de corpos funções e por outro, à introdução em aritmética de corpos *p*-ádicos , que representa a parte da expansão de Puiseus para as funções algébricas em corpos de números. Assim, os fundamentos foram estendidos para a álgebra comutativa em termos da geometria algébrica moderna (PRETZEL, 1998).

Temos como principal característica encontrar soluções geométricas através das equações módulo p. Se $f(x,y) = 0$ for um polinômio em duas variáveis então a equação $f(x,y) = 0$ define uma curva X_f no plano. Por exemplo, as únicas soluções racionais para a curva elíptica $y^2 = x^3 - x$ são $(x,y) = (0,0)$ e $(\pm1,0)$, Isso nos faz considerar neste trabalho curvas algébricas sobre corpos finitos.

Um corpo $\overline{K}$ é **algebricamente fechado** se todo polinômio em $\overline{K}[X]$ tem raiz em K.

Sejam $\overline{K}$ um corpo algebricamente fechado e K um subcorpo de $\overline{K}$. Denotaremos por A^2 o plano afim sobre o corpo $\overline{K}$ consistindo do conjunto de todos os pares (a, b) de elementos, a, b de $\overline{K}$. Chamamos o par $P = (a, b)$ de um ponto do plano A^2 e os elementos a, b as coordenadas do ponto P.

Definição 2.1: Uma curva algébrica plana é o conjunto de todos os pontos $P = (x, y) \in A^2$ cujas coordenadas satisfazem a equação:

$$f(x, y) = 0, \qquad \text{[Eq. 01]}$$

onde $f(x, y)$ é um polinômio com coeficientes no corpo $\overline{K}$. Se os coeficientes do polinômio $f(x, y)$ pertencem ao subcorpo K, então dizemos que a curva (1) é definida sobre o subcorpo K.

Definição 2.2: Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{K}$. Então, os pontos em $\mathcal{X}$ com todas as suas coordenadas em $\mathbb{K}$, tais que $f(x, y)=0$, são chamados **pontos racionais**.

Quando uma curva $\mathcal{X}$ tem ao menos um ponto singular, dizemos que é uma **curva singular**. Caso contrário, **não-singular.**

Definição 2.3: O polinômio F de grau d é chamado à **homogeneização** de f, quando F é obtido de f, através da computação de Z's nos monômios de graus inferiores de f visando um polinômio F cujos monômios possuem o mesmo grau, determinado por $F(X,Y,Z) = Z^d f(X/Z, Y/Z)$

Definição 2.4 : Sejam K um corpo e $f(x, y) \in K[x, y]$. Um ponto singular da curva X_f é o ponto $(x_0, y_0) \in K \times K$ tal que $f(x_0, y_0) = 0$ e $f_x(x_0, y_0) = 0$ e $f_y(x_0, y_0) = 0$. Se $F(X, Y, Z)$ é a homogeneização de $f(x, y)$, então $(X_0 : Y_0 : Z_0) \in P^2(K)$ é um ponto singular de X_f se o ponto está na curva e se todas as derivadas parciais forem nulas, isto é:

$$\begin{aligned} F(X_0, Y_0, Z_0) &= F_x(X_0, Y_0, Z_0) \\ &= F_y(X_0, Y_0, Z_0) \\ &= F_z(X_0, Y_0, Z_0) \\ &= 0. \end{aligned} \qquad \text{[Eq. 02]}$$

Um polinômio F é **homogêneo** se todos os seus monômios têm o mesmo grau; este grau é o grau do polinômio homogêneo.

Em geral, mostra-se que se $f(x, y)$ é um polinômio de grau d tal que a curva $\hat{X}_f$ é não-singular, então o gênero topológico de X_f é determinado pela fórmula de Plúcker.

Lema 2.1 (Fórmula de Plücker) (Fulton, 1969): Seja $f(x,y) \in K[x,y]$ $f(x,\ y)$ um polinômio de grau n tal que $\hat{X}_f$ é não-singular, então o gênero da curva X_f (ou de $\hat{X}_f$) e´ dado por

$$g(X_f) = \frac{(n-1)(n-2)}{2} \qquad \text{[Eq. 03]}$$

Teorema 1 *(*Pretzel, 1991*):* Seja X uma curva projetiva não-singular de gênero g definida sobre $GF(q)$. Se $Nq(\mathcal{X}(g))$ denota o número de pontos racionais de X de gênero g sobre $GF(q)$, então

$$\left|N_q(X(g)) - q - 1\right| \le g\left\lfloor 2q^{1/2} \right\rfloor, \qquad \text{[Eq. 04]}$$

onde $\lfloor a \rfloor$ denota a parte inteira de a.

Definição 2.5: Uma curva projetiva X é maximal quando

$$N_q(X(g)) = q + 1 + g\left\lfloor 2q^{1/2} \right\rfloor \qquad \text{[Eq. 05]}$$

B – Irredutibilidade de Polinômios

Um polinômio não-constante $f(x,y) = p_0(x)y^n + p_1(x)y^{n-1} + \cdots + p_{n-1}(x)y + p_n(x)$, em K[x, y], é chamado redutível se existem polinômios *g* e *h* tal que

$$f(x,y) = g(x,y)h(x,y), \qquad \text{[Eq. 06]}$$

com $1 \le \deg(g(x,y)),\ \deg(h(x,y)) < \deg(f(x,y))$. Caso contrario, **irredutível**.

Definição 2.5: O polinômio *f* com coeficientes no corpo $\mathbb{K}$ é **absolutamente irredutível** se *f(x, y) é* irredutível sobre qualquer extensão algébrica $\overline{K}$ do corpo $\mathbb{K}$, isto é, *f(x, y)* é irredutível em $\overline{K}$.

A condição de polinômio absolutamente irredutível garante que a curva está “conectada” em um certo sentido, isto é, a curva *X* : *f (x, y)* = 0 é conexa. Na realidade se *X* está definida como acima por forma homogênea *F* em *GF(q) [,X Y Z]* irredutibilidade significa simplesmente que *F* não é o produto de duas formas homogêneas não-constantes em *GF(q)[X, Y, Z]* de grau menor. Absolutamente irredutível é uma propriedade geométrica que significa dizer que *F* é irredutível sobre qualquer extensão finita de *GF(q)*, isto é a curva *X* quando vista sobre o fecho algébrico de *GF(q)* não é união disjunta de outras curvas. Em termos práticos, quando *X* está definida por um modelo afim *f (x, y)*, absolutamente irredutível implica que o anel de coordenadas *GF(q) [x, y]* / *(f)* é um domínio integral e permanece assim quando o corpo *GF(q)* é substituído pó qualquer extensão finita. Isso garante, em outras palavras, que o corpo quociente é um corpo de função de grau de transcendência 1 (MORENO, 1991).

Apresentamos agora, polinômios absolutamente irredutíveis sobre corpos finitos construídos por Santos e Palazzo(2004) que satisfazem o critério de Eisenstein.

Sejam $a_1, a_2, \ldots, a_n$, onde $a_i \in GF(q)$ e $n \le q$, definidos através da equação $(Y - Y_1)(Y - Y_2)\ldots(Y - Y_n) = Y^n + a_1 Y^{n-1} + a_2 Y^{n-2} + \cdots + a_{n-1}Y + a_n$

sobre GF(q), onde

$$\begin{aligned} a_1 &= \sum_{i=1}^{n} Y_i \\ a_2 &= \sum_{i<j} Y_i Y_j \\ &\vdots \\ a_n &= Y_1 Y_2 \ldots Y_n = \prod_{i=1}^{n} Y_i \end{aligned} \qquad \text{[Eq. 07]}$$

Esses valores são conhecidos como funções simétricas elementares de Y_i.

Definição 2.6 (Santos, 2003, 2004**):** Seja *f(x, y)* um polinômio a duas variáveis (*x, y)* sobre o corpo *GF(q)* definido por

$$f(x,y) = y^n + f_{j,b}(x)\sum_{i=j}^{n} g_i(x)y^{n-1} \quad = p_0(x)y^n + p_1(x)y^{n-1} + \cdots + p_{n-1}(x)y + p_n(x), \qquad \text{[Eq. 08]}$$

onde • $j = \min\{k \in \{1,2,\ldots,n\}; a_k \neq 0\}$; • $f_{j,b}(x) = x - b + a_j$, $b \in GF(q)$;

• $h_i(x) = \rho \cdot (x-b) + \dfrac{a_i}{a_j} - b^{i-1}$; • $g_i(x) = x^{i-1} + h_i(x)$, $i = j,\ldots,n$;

• $p_i(x) = f_{j,b}(x)g_i(x)$, $i = j,\ldots,n$.

Teorema 2.1 (Santos, 2003): O polinômio [Eq. 08], para $n > 0$ *e* $n \neq 2$, é absolutamente irredutível.

Como exemplos de polinômios absolutamente irredutíveis construídos a partir da **Definição 2.6**, citamos os seguintes:

1) Considere $K = GF(9)$ como sendo o corpo de Galois gerado por α, raiz de $x^2 + 2x + 2 = 0$. Sejam $a_1 = 1, a_2 = 2, a_3 = 1, a_4 = 2$ e $b = 0$. *Como* $j = \min\{k \in \{1,2,3,4\}; a_k \neq 0\} = 1$ e $a_4 / a_1 - b^3 = 2 \neq -(b - a_1)^3 = 1$, então pelo polinômio [Eq.08] $f_1(x) = x + a_1 - b = x + 1 - 0$, $g_1(x) = 1 + 0 = 1$, $g_2(x) = x + a_2 / a_1 - b = x + 2$, $g_3(x) = x^2 + a_3 / a_1 - b^2 = x^2 + 1$ e $g_4(x) = x^3 + a_4 / a_1 - b^3 = x^3 + 2$. Assim,

$f(x,y) = y^4 + (x+1)y^3 + (x+1)(x+2)y^2 + (x+1)(x^2+1)y + (x+1)(x^3+2)$

é absolutamente irredutível sobre $GF(9)$, com $\varsigma = 1$.

2) Considere $K = GF(16)$ como sendo o corpo de Galois gerado por α, raiz de $x^4 + x + 1 = 0$.

Sejam $a_1 = 1, a_2 = 1, a_3 = 0$ e $b = 0$, isto é, $a_i, b \in GF(16), i = 1,2,3$. Assim, pelo polinômio [*Eq.* 08],

$f(x,y) = y^3 + (x+1)y^2 + (x+1)(x-1)y \ + (x+1)x^2$.

Portanto, $f(x,y)$ é absolutamente irredutível sobre $GF(16)$, com $\varsigma = 1$.

Teorema 2.2 (Santos, 2003): O polinômio

$$f(x,y) = y^2 + f_1(x)y + g(x), \qquad \text{[Eq. 09]}$$

tal que um dos $a_i's$ é diferente de zero, é absolutamente irredutível se uma das condições abaixo for satisfeita: *(i)* $f_1(x) = x + a_1 - b)$ e $g(x) = (x + a_1 - b)(x + \dfrac{a_2}{a_1} - b)$, se $a_1 \neq 0$ e $a_2 \neq a_1^{\,2}$;

(ii) $f_1(x) = x + a_1 - b)$ e $g(x) = (x + a_1 - b)a_1$, se $a_1 \neq 0$ e $a_2 = a_1^{\,2}$;

(iii) $f_1(x) = 0$ e $g(x) = (x + a_2 - b)$, se $a_1 = 0$.

Como exemplo de polinômio absolutamente irredutível construído a partir do **Teorema 2.2**, citamos o seguinte:

Considere $K = GF(9)$ como sendo o corpo de Galois gerado por α, raiz de $x^2 + 2x + 2 = 0$. Sejam $a_1 = 1$, $a_2 = \alpha^4$ e $b = \alpha$. Como $a_2 \neq a_1^{\,2}$ e $a_1 \neq 0$, então pelo Teorema 2.2, que $f_1(x) = x + a_1 - b = x + 1 - \alpha = x + 1 + 2\alpha = x + \alpha^3$ e $g(x) = (x + a_2 / a_1 - b)(x + a_1 - b) = (x + \alpha^4 - \alpha)(x + 1 - \alpha) = (x + \alpha^4 + 2\alpha)(x + 1 + 2\alpha) = (x + \alpha^6)(x + \alpha^3)$. Portanto, $f(x, y)$ é dado por

$$f(x, y) = y^2 + (x + \alpha^3)y + (x + \alpha^6)(x + \alpha^3).$$

Desse modo, este polinômio é absolutamente irredutível sobre $GF(9)$, com $\varsigma = \alpha^3$.

Observação 2.1: Os polinômios [Eq. 08] e [Eq. 09], podem ser representados sob a forma $f(x, y) = x^n + y^n + g(x, y)$, onde o grau de *g(x,y)* é menor ou igual a *n.*

RESULTADOS

Nesta seção apresentaremos os resultados advindos da nossa pesquisa. A condição de o polinômio ser absolutamente irredutível garante que a curva $\mathcal{X} : f(x, y) = 0$ é conexa. Na realidade, se $\mathcal{X}$ é uma forma homogênea F em $GF(q)[X, Y, Z]$, irredutibilidade significa simplesmente que F não é o produto de duas formas de grau menor que n, homogêneas não-constantes em $GF(q)[X, Y, Z]$. Absolutamente irredutível é uma propriedade geométrica que significa dizer que F é irredutível sobre qualquer extensão finita de $GF(q)$, isto é, a curva $\mathcal{X}$ quando vista sobre o fecho algébrico de $GF(q)$ não é a união disjunta de outras duas curvas. Em termos práticos, quando $\mathcal{X}$ está definida por um modelo afim $f(x, y)$, absolutamente irredutível implica que o anel de coordenadas $GF(q)[x, y]/(f)$ é um domínio de integridade e permanece assim se o corpo $GF(q)$ é substituído por qualquer extensão finita. Isso garante, em outras palavras, que o corpo quociente é um corpo de função de grau de transcendência 1. No que diz respeito ao gênero de $\mathcal{X}$, lembramos que o mesmo é uma medida da complexidade da curva $\mathcal{X}$ quando comparada com a reta projetiva. Salientamos ainda que a existência de curvas sobre corpos finitos com muitos pontos racionais (isto é, curvas maximais) possibilita a construção de códigos ótimos. Desta forma, os melhores códigos são aqueles construídos através de curvas com muitos pontos racionais, uma vez que os comprimentos das palavras código estão diretamente atribuídos a esse número. O problema principal em se construir códigos algébrico-geométricos é praticamente encontrar uma forma de executar as computações exigidas de uma forma mais rápida e eficiente no processo de transmissão de dados e de sinais. Com isto, faz sentido falarmos em construir algoritmos para determinar pontos racionais e pontos singulares de curvas algébricas sobre corpos finitos associadas aos polinômios das equações [Eq. 08] e [Eq. 09], apresentados na Seção II.

Apresentaremos agora os algoritmos para determinar os pontos racionais e pontos singulares de curvas algébricas, através dos polinômios absolutamente irredutíveis das equações [Eq. 08] e [Eq. 09], utilizando o software computacional Maple®, Salientamos que estes algoritmos são versões modificadas dos algoritmos de Gaétan (Nov. 1995, pp. 1615-1628) na linguagem computacional C.

Algoritmo para determinar pontos singulares

Seja *X* uma curva plana projetiva definida sobre *GF(q)* com equação *F(X;Y;Z) =0*

Sejam F_x ; F_y e F_z ; respectivamente, as derivadas de F com respeito às variáveis *X, Y, Z.*

Então

$$(a : b : c) \in X \text{ é singular} \iff \begin{cases} F(a, b, c) = 0 \\ F_X(a, b, c) = 0 \\ F_Y(a, b, c) = 0 \\ F_Z(a, b, c) = 0 \\ (a, b, c) \neq (0, 0, 0). \end{cases} \qquad \text{[Eq. 10]}$$

Para resolver o sistema [Eq. 10], adotaremos os seguintes passos, utilizando o pacote do Sistema Maple10:

Passo 1: Buscar o pacote que trabalha com curvas algébricas no Maple chamado **with(algcurves)**;

Passo 2: Definir os: números naturais m, n e o número primo p;

m:; n: (números naturais); p: (número primo);

Passo 3: Gerar o corpo de Galois GF(q), onde $q= p^m$, utilizando o polinômio gerador x^m+x+n-1 do corpo em questão, através da ferramenta alias:

alias(alpha=RootOf(x^m+x+n-1);

Passo 4: Obter o polinômio *f(x,y)* nas variáveis x e y, isto é, [Eq. 08] ou [Eq. 09];

Passo 5: Determinar o polinômio homogêneo de *f(x,y*), isto é, F(X,Y,Z):

F1:=homogeneous(f1,x,y,z) mod p;

Passo 6: Determinar as derivadas do polinômio homogêneo, seguindo os procedimentos abaixo**:**

F1x:=diff(F1,x)mod p; F1y:=diff(F1,y)mod p; F1z:=diff(F1,z)mod p;

Passo 7: Determinar os pontos singulares da curva gerada por [Eq. 08] ou por [Eq. 09]:

```
for i from 1 by 1 to m^n -1 do
for j from 1 by 1 to m^n -1 do
if (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1))mod p)=0 and
        (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1x))mod p)=0 and
        (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1y))mod p)=0
    then print(alpha^i,alpha^j,1) end if; od
if (simplify(subs({x=alpha^j,y=1,z=0},F1))mod p)=0 and
        (simplify(subs({x=alpha^j,y=1,z=0},F1x))mod p)=0 and
        (simplify(subs({x=alpha^j,y=1,z=0},F1z))mod p)=0
    then print(alpha^j,1,0) end if;
if (simplify(subs({x=alpha^j,y=0,z=1},F1))mod p)=0 and
        (simplify(subs({x=alpha^j,y=0,z=1},F1x))mod p)=0 and
        (simplify(subs({x=alpha^j,y=0,z=1},F1y))mod p)=0
    then print(alpha^j,0,1) end if;
if (simplify(subs({x=0,y=alpha^j,z=1},F1))mod p)=0 and
        (simplify(subs({x=0,y=alpha^j,z=1},F1x))mod p)=0 and
        (simplify(subs({x=0,y=alpha^j,z=1},F1y))mod p)=0
    then print(0,alpha^j,1) end if; od;
if (simplify(subs({x=1,y=0,z=0},F1))mod p)=0 and
        (simplify(subs({x=1,y=0,z=0},F1y))mod p)=0 and
        (simplify(subs({x=1,y=0,z=0},F1z))mod p)=0
    then print(1,0,0) end if;
if (simplify(subs({x=0,y=0,z=1},F1))mod p)=0 and
        (simplify(subs({x=0,y=0,z=1},F1x))mod p)=0 and
        (simplify(subs({x=0,y=0,z=1},F1y))mod p)=0
    then print(0,0,1) end if;
if (simplify(subs({x=0,y=1,z=0},F1))mod p)=0 and
        (simplify(subs({x=0,y=1,z=0},F1x))mod p)=0 and
        (simplify(subs({x=0,y=1,z=0},F1z))mod p)=0
    then print(0,1,0) end if;
```

Algoritmo para determinar pontos racionais

Agora apresentamos o que devemos fazer para encontrarmos os pontos racionais de uma curva algébrica sobre corpos finitos.

Seja *X* uma curva plana projetiva definida sobre *GF(q)* com equação *F(X;Y;Z) =0. Então,*

$$(a : b : c) \in X \text{ é racional sobre } GF(q) \iff \begin{cases} F(a, b, c) = 0 \\ a^q - a = 0 \\ b^q - b = 0 \\ c^q - c = 0 \\ (a, b, c) \neq (0, 0, 0). \end{cases} \quad \text{[Eq. 11]}$$

Para resolver o sistema [Eq. 11], adotaremos os seguintes passos utilizando o pacote do Sistema Maple10.

Passo 1: Buscar o pacote que trabalha com curvas algébricas no Maple chamado **with(algcurves)**;

Passo 2: Definir os: números naturais m, n e o número primo p;

Passo 3: Gerar o corpo de Galois GF(q), onde q= p^m , utilizando o polinômio gerador x^m+x+n-1 do corpo em questão, através da ferramenta alias:

alias(alpha=RootOf(x^m+x+n-1);

Passo 4: Obter o polinômio *f(x,y)* nas variáveis x e y, isto é, [Eq. 08] ou [Eq. 09];

Passo 5: Determinar o polinômio homogêneo de *f(x,y*), isto é, F(X,Y,Z):

F1:=homogeneous(f1,x,y,z) mod p;

Passo 7: Determinar os pontos racionais da curva gerada por [Eq. 08] ou por [Eq. 09].

Escreva:

```
soma:=0;
for i from 1 by 1 to m^n - 1 do
   for j from 1 by 1 to m^n - 1 do
       if (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1))mod p)=0
       then soma:=soma+1: print(alpha^i,alpha^j,1) end if;
       od;
       if (simplify(subs({x=alpha^j,y=1,z=0},F1))mod p)=0
       then soma:=soma+1:print(alpha^j,1,0) end if;
       if (simplify(subs({x=1,y=0,z=alpha^j},F1))mod p)=0
       then soma:=soma+1:print(1,0,alpha^j) end if;
       if (simplify(subs({x=0,y=alpha^j,z=1},F1))mod p)=0
       then soma:=soma+1:print(0,alpha^j,1) end if;
       od;
       if (simplify(subs({x=1,y=0,z=0},F1))mod p)=0
       then soma:=soma+1:print(1,0,0) end if;
       if (simplify(subs({y=1,x=0,z=0},F1))mod p)=0
       then soma:=soma+1:print(0,1,0) end if;
       if (simplify(subs({z=1,x=0,y=0},F1))mod p)=0
       then soma:=soma+1:print(0,0,1) end if;
       od;soma;
```

Exemplo 3.1: Seja $GF(8) = GF(2)/\langle x^3 + x + 1 \rangle$ o corpo de Galois gerado por α , raiz de $x^3 + x + 1$. Seja X_f a curva definida pela equação $y^2 + xy + \alpha^5 y + x^2 + \alpha^4 x + \alpha^5 = 0$ sobre *GF(8)*, onde $f(x, y) = y^2 + xy + \alpha^5 y + x^2 + \alpha^4 x + \alpha^5$. Esta curva é não-singular de gênero 0. O polinômio homogêneo de *f* é dado por $F(X, Y, Z) = Y^2 + XY + \alpha^5 YZ + X^2 + \alpha^4 XZ + \alpha^5 Z^2$

Esta curva tem nove pontos racionais, isto é,

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
x	1	0	α^5	0	1	α	α	α^6	α^6
y	0	α^2	0	α^3	α^4	1	α^2	1	α^3
z	1	1	1	1	1	1	1	1	1

Pelo limitante da **Definição 2.5** esta curva é maximal.

Apresentamos abaixo o algoritmo que determinou os pontos racionais do Exemplo 3.1, utilizando o softwear Maple.

```
> restart:with(algcurves):alias(alpha=RootOf(x^3+x+1=0,x)):
> f1:=y^2+(x+alpha^5)*y+(x+alpha^5)*(x+1);
```

$$f1 := y^2 + (x+\alpha^5)y + (x+\alpha^5)(x+1)$$

```
> F1:=homogeneous(f1,x,y,z) mod 2;
```

$$F1 := y^2 + yx + \alpha^5 yz + \alpha^5 z^2 + (\alpha^5+1)xz$$

```
> soma:=0;
```

soma:=0

```
> for i from 1 by 1 to 7 do
> for j from 1 by 1 to 7 do
> if (simplify(subs({x=alpha^i,y=alpha^j,z=1},F1))mod 2)=0 then soma:=soma+1:
print(alpha^i,alpha^j,1) end if;
> od;od;soma;
```

$$\alpha, \alpha^2, 1$$
$$\alpha, \alpha^7, 1$$
$$\alpha^6, \alpha^3, 1$$
$$\alpha^6, \alpha^7, 1$$
$$\alpha^7, \alpha^4, 1$$

```
> for i from 1 by 1 to 7 do
> if (simplify(subs({x=alpha^i,y=1,z=0},F1))mod 2)=0 then
soma:=soma+1:print(alpha^i,1,0) end if;
> if (simplify(subs({x=1,y=0,z=alpha^i},F1))mod 2)=0 then
soma:=soma+1:print(1,0,alpha^i) end if;
> if (simplify(subs({x=0,y=alpha^i,z=1},F1))mod 2)=0 then
soma:=soma+1:print(0,alpha^i,1) end if;
> od;soma;
```

$$1, 0, \alpha^2$$
$$0, \alpha^2, 1$$
$$0, \alpha^3, 1$$
$$1, 0, \alpha^7$$

```
> if (simplify(subs({x=1,y=0,z=0},F1))mod 2)=0 then print(1,0,0) end if;
> if (simplify(subs({y=1,x=0,z=0},F1))mod 2)=0 then print(0,1,0) end if;
> if (simplify(subs({z=1,x=0,y=0},F1))mod 2)=0 then print(0,0,1) end if;
```

METODOLOGIA

A pesquisa que está sendo desenvolvida consiste no estudo, analise e implementação de dados estudados a cerca das situações problema. Para tanto, foram realizadas pesquisas bibliográfica e documental sobre as temáticas abordadas contando com o estudo sobre curvas algébricas, pontos racionais e pontos singulares. Em seguida, foram feitos estudos e pesquisas sobre a temática do software Maple e suas aplicações práticas, como funciona e como se executa determinadas tarefas e programas para, em seguida, elaborar e implementar algoritmos para gerar curvas e determinar pontos racionais e pontos singulares.

1. CONCLUSÕES

O desenvolvimento de uma ferramenta para determinar pontos racionais e pontos singulares de uma curva algébrica vem preencher uma lacuna existente e pode ser de grande valia na determinação de códigos algébrico-geométricos. Neste trabalho apresentamos uma construção de algoritmos através de curvas algébricas e polinômios absolutamente irredutíveis para determinar os pontos racionais e os pontos singulares de curvas algébricas sobre corpos finitos. Em seguida, iremos caminhar no sentido de podermos concluir a sua implementação no que diz respeito à curva ser ou não maximal. Espera-se concluir essa

implementação concomitantemente até o final do presente semestre. Os pontos racionais desse polinômio são os elementos chaves no processo, pois apresentam as propriedades de construir novos códigos ótimos.

REFERÊNCIAS

ANDRADE, JOSÉ APARECIDO. **Introdução aos códigos corretores de erros.** XIV Semana da Matemática – Reunião regional da Sociedade Brasileira de Matemática, Instituto de Biociências, Letras e Ciências Exatas (IBILCE), Universidade Estadual Paulista (UNESP), São José do Rio Preto, 06-08 de maio de 2000.

FULTON, W. **Algebraic Curves: An Introduction to Algebraic Geometry**, Benjamin, New York, 1969.
GOPPA, V.D. **Codes on algebraic curves**,.Sov. Math. Dokl, vol. 24, pp.75-91, 1981.

GÁETAN HACHÉ AND D. LE BRIGAND, ”**Effective construction of algebraic geometry codes**,” IEEE Trans. Inform. Theory, vol. 41, pp. 1615-1628, Nov. 1995.

MORENO, C.J. **Algebraic Curves over Finite Fields**. Cambridge Tracts in Mathematics, Vol. 97, USA, 1991.

PRETZEL, OLIVER. **Codes and Algebraic Curves**. Oxford Lecture Series in Mathematics and its Applications, No. 8, Oxford, 1998.

SANTOS, GIVALDO OLIVEIRA DOS .**Caracterização Geométrica do Processo de Decodificação da Classe dos Códigos Alternantes Cíclicos através de Polinômios Absolutamente Irredutíveis**, Tese de Doutorado, FEEC - UNICAMP, Abril 2003.

SANTOS, GIVALDO OLIVEIRA DOS & PALAZZO, REGINALDO. ”**Proposta de construção de polinômios absolutamente irredutíveis geradores de curvas algébricas com muitos pontos racionais**,”XXI Simpósio Brasileiro de Telecomunicações, Belém-PA, pp. 1-6, Setembro 2004.