Proposta de Construção de Polinômios Absolutamente Irredutíveis Geradores de Curvas Algébricas com muitos Pontos Racionais

Givaldo Oliveira dos Santos, e Reginaldo Palazzo Jr.

***Resumo*— Este trabalho tem por objetivo apresentar uma nova proposta, até onde é de nosso conhecimento, de construção de polinômios absolutamente irredutíveis sobre $GF(q)$. Tais polinômios conduzem à geração de curvas algébricas com muitos pontos racionais que, na grande maioria dos casos de interesse, são caracterizadas como curvas algébricas maximais.**

***Palavras-Chave*— Polinômios absolutamente irredutíveis, curvas algébricas maximais, pontos racionais, algoritmo de Berlekamp-Massey**

***Abstract*— The aim of this paper is to present a new method of constructing absolutely irreducible polynomials over $GF(q)$. These polynomials have the property of generating algebraic curves with many rational points which, in the majority of the cases of interest, are characterized as maximal algebraic curves.**

***Keywords*— Absolutely irreducible polynomials, maximal algebraic curves, rational points, Berlekamp-Massey Algorithm**

I. INTRODUÇÃO

Dentro do programa de pesquisa sobre modelagem de sistemas de comunicações digitais em espaços homogêneos, [1], entendido espaços com curvatura constante, e em particular considerando variedades Riemannianas bi-dimensionais, nos deparamos com o problema da caracterização geométrica do processo de decodificação dos códigos cíclicos sobre $GF(q)$ através do uso do algoritmo de Berlekamp-Massey (BM).

O polinômio localizador de erros do algoritmo BM apresenta a propriedade de ser irredutível sobre $GF(q)$. Como conseqüência deste fato, a motivação para a presente proposta decorre do fato de que se o polinômio $f(x, y)$ é absolutamente irredutível sobre o fecho algébrico de $GF(q)$, então o "lugar geométrico"das raízes da correspondente curva $\mathcal{X}_f : f(x, y) = 0$ é conexo, portanto um espaço topológico completo (compacto). Como o subconjunto fechado irredutível do espaço afim $\mathcal{A}^n$ é uma variedade algébrica afim, então o conjunto de zeros, $\mathcal{X}_F$, associado ao polinômio homogeneizado F de f (irredutível), é, portanto, uma variedade afim V(F). Para $n = 3$, V(F) é uma superfície. Por outro lado, no caso em que o corpo é o dos números complexos $\mathbb{C}$, uma curva $\mathcal{X}$ é simplesmente uma superfície de Riemann. Além do gênero, parâmetro caracterizador da superfície, o grau do polinômio em y corresponde à quantidade de folhas que cobre esta superfície. Fica claro, dessa forma, que a caracterização geométrica decorrente do polinômio localizador de erros do algoritmo BM é uma superfície.

Somente estes fatos seriam suficientes para justificar tal proposta. Além disso, tais polinômios implicam na geração de curvas algébricas maximais, condição necessária para a construção de bons códigos algébrico-geométricos (AG).

Portanto, o objetivo deste trabalho é de estabelecer uma nova proposta, até onde é de nosso conhecimento, de construção de polinômios absolutamente irredutíveis conduzindo a curvas algébricas com muitos pontos racionais.

Este trabalho está organizado da seguinte forma. Na Seção II, apresentamos os conceitos e definições básicas sobre curvas algébricas, pontos racionais, plano projetivo, ponto singular, gênero de uma curva plana projetiva, e quantidade de pontos racionais associada a uma curva plana projetiva não-singular. Na Seção III, apresentamos os elementos necessários que culminarão na proposta de construção de polinômios absolutamente irredutíveis segundo o critério de Einsenstein. Na Seção IV, são apresentados vários exemplos de geração de curvas algébricas sobre $GF(q)$ decorrentes da construção proposta na seção anterior. Finalmente, na Seção V, apresentamos as conclusões.

II. PRELIMINARES

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

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

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

$$f(x, y) = 0, \tag{1}$$

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

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 $f(x, y) \equiv 0$, são chamados **pontos racionais**.

Consideraremos o corpo $\mathbb{K}$ como sendo o corpo $GF(q)$ consistindo de $q = p^r$ elementos (p um número primo) e

O autor está no CEFET-Alagoas, Brasil. email: givaldodt@ig.com.br
O autor está no Departamento de Telemática, FEEC-UNICAMP, Brasil. email: palazzo@dt.fee.unicamp.br

$\overline{\mathbb{K}} = \overline{GF(q)}$ o seu fecho algébrico. Neste caso, o conjunto de pontos $GF(q)$-racionais da curva (1), definida sobre $GF(q)$, coincidem com o conjunto de soluções da equação (1) nos elementos x, y do corpo $GF(q)$. Em particular, para $GF(p)$, p primo, então a questão relativa aos pontos $GF(p)$-racionais da curva (1) é equivalente às soluções da congruência $f(x,y) \equiv 0 \, mod \, p$.

Definição 2.3: O conjunto de todas as razões $(a_0 : a_1 : a_2)$ é chamado **plano projetivo** e será denotado por $\mathbb{P}^2(\mathbb{K})$. Cada $(a_0 : a_1 : a_2)$ é chamado um ponto de $\mathbb{P}^2(\mathbb{K})$.

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

Definição 2.4: Seja $\mathbb{K}$ um corpo e $f(x,y) \in \mathbb{K}[x,y]$, o anel de polinômios sobre $\mathbb{K}$. Um **ponto singular** da curva $\mathcal{X}_f$ é um ponto $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$ tal que $f(x_0, y_0) = 0$, $f_x(x_0, y_0) = 0$ e $f_y(x_0, y_0) = 0$, onde $\frac{\partial f}{\partial x} = f_x$ e $\frac{\partial f}{\partial y} = f_y$. Se $F(X,Y,Z)$ é a homogeneização de $f(x,y)$, então $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{K})$ é um **ponto singular** de $\widehat{\mathcal{X}}_f$ (fecho projetivo de $\mathcal{X}_f$).

Definição 2.5: Seja $\mathcal{X}$ uma curva projetiva sobre um corpo $\mathbb{K}$, representada por $F(X,Y,Z) = 0$. Um ponto $P = (x_0, y_0, z_0) \in \overline{\mathbb{K}}$, é um **ponto singular** se, e somente se,

$$F(P) = \frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

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

Definição 2.6: O polinômio F com coeficientes no corpo $\mathbb{K}$ é **absolutamente irredutível** se F é irredutível em qualquer extensão algébrica $\overline{\mathbb{K}}$ do corpo $\mathbb{K}$.

Proposição 2.1: [4], [2] Seja $F(X,Y,Z) = 0$ a equação de uma curva plana projetiva singular $\mathcal{X}$, onde $F(X,Y,Z)$ é um polinômio homogêneo de grau m. Se $P_1, P_2, \ldots, P_n$ são os pontos singulares de $\mathcal{X}$ cujas multiplicidades para os correspondentes pontos P_i são $r_1, r_2, \ldots, r_n$, então o gênero da curva plana é

$$g(\mathcal{X}) = \frac{(n-1)(n-2)}{2} - \sum_{i=1}^{n} \delta(P_i),$$

onde $\delta(P_i) = r_i(r_i - 1)/2$.

Definição 2.7: [7] Dada uma curva plana projetiva não-singular $\mathcal{X}$, definida sobre um corpo finito $\mathbb{K}$, então um ponto $(x,y,z) \in \mathcal{X}$ é um ponto racional sobre $\mathbb{K}$ se $(x,y,z) \in \mathbb{K}^3$.

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

Lema 2.1 (Fórmula de Plücker): [5] Seja $f(x,y) \in \mathbb{K}[x,y]$ um polinômio de grau n tal que $\widehat{\mathcal{X}}_f$ é não-singular, então o gênero da curva $\mathcal{X}_f$ (ou de $\widehat{\mathcal{X}}_f$) é dado por

$$g(\mathcal{X}_f) = \frac{(n-1)(n-2)}{2}.$$

Teorema 1: [7], [2] Seja $\mathcal{X}$ uma curva projetiva não-singular de gênero g definida sobre $GF(q)$. Se $N_q(\mathcal{X}(g))$ denota o número de pontos racionais de $\mathcal{X}$ de gênero g sobre $GF(q)$, então

$$|N_q(\mathcal{X}(g)) - q - 1| \leq g\lfloor 2q^{1/2} \rfloor,$$

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

Definição 2.8: Uma curva projetiva $\mathcal{X}$ é maximal quando $N_q(\mathcal{X}(g)) = q + 1 + g[2\sqrt{q}]$.

III. Construção de Polinômios Absolutamente Irredutíveis

Nesta seção apresentamos a proposta de construção de polinômios absolutamente irredutíveis sobre corpos finitos os quais satisfazem o critério de Eisenstein.

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

Os únicos polinômios $f(x)$ absolutamente irredutíveis têm a forma $f(x) = ax + b$ isto porque todo polinômio $f(x)$ se decompõe em fatores lineares em alguma extensão finita de corpos.

A proposição a seguir e seu corolário mostram que polinômios absolutamente irredutíveis se comportam mais como polinômios lineares com uma única indeterminada.

Proposição 3.1: [5] Seja $f(x,y)$ um polinômio não-constante sobre um corpo $\mathbb{K}$. Então existe uma extensão finita de corpos $\mathbb{L}$ tal que $f(x,y)$ tem um fator absolutamente irredutível em $\mathbb{L}[x,y]$.

Demonstração: A prova é por indução no grau de $f(x,y)$. Se o grau é 1, então $f(x,y)$ é absolutamente irredutível. Suponha que a proposição foi provada para todos os graus menores que n e que $f(x,y)$ tem grau n.

Se $f(x,y)$ é absolutamente irredutível não há nada o que provar. Caso contrário, existe uma extensão finita de corpos $\mathbb{J}$ tal que $f(x,y)$ não é irredutível em $\mathbb{J}[x,y]$ (obviamente que $\mathbb{J}$ pode ser $\mathbb{K}$). Então, em $\mathbb{J}[x,y]$,

$$f(x,y) = g(x,y)h(x,y),$$

onde g e h têm grau menor que n e nenhum deles é uma constante. Pela hipótese de indução segue que, para alguma extensão finita de corpos $\mathbb{L}$ de $\mathbb{J}$, $g(x,y)$ tem um fator absolutamente irredutível $p(x,y)$ em $\mathbb{L}[x,y]$. Agora, $p(x,y)$ é também um fator de $f(x,y)$ em $\mathbb{L}[x,y]$ e $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$. Assim, a proposição é verificada para $f(x,y)$ com grau n. ■

Corolário 3.1: [5] Seja $f(x,y)$ um polinômio não-constante sobre um corpo $\mathbb{K}$. Então existe uma extensão finita de corpos $\mathbb{L}$ tal que $f(x,y)$ se decompõe em um produto de fatores absolutamente irredutíveis em $\mathbb{L}[x,y]$.

Demonstração: A prova é por indução no grau de $f(x,y)$. Se $f(x,y)$ é absolutamente irredutível não há nada que provar. Este é sempre o caso se $n = 1$. Caso contrário, pela Proposição 3.1, existe uma extensão finita de corpos $\mathbb{J}$ de $\mathbb{K}$ tal que

$$f(x,y) = p(x,y)q(x,y), \quad (2)$$

em $\mathbb{J}[x,y]$ e $p(x,y)$ é absolutamente irredutível. Então, o grau de $q(x,y)$ é menor que n e, assim, pela hipótese de indução, existe uma extensão finita de corpos $\mathbb{L}$ de $\mathbb{J}$ tal que $q(x,y)$ se divide em fatores absolutamente irredutíveis sobre $\mathbb{L}$. Então, pela equação (2), o mesmo acontece com $f(x,y)$. ■

A proposição a seguir, caso especial do critério de Eisenstein, fornece um modo fácil de construção de polinômios absolutamente irredutíveis. O critério não é um meio necessário, porém existem muitos polinômios que o satisfaz.

Proposição 3.2 (Critério de Eisenstein): [5] Seja $f(x,y) \in \mathbb{K}[x,y]$ escrito como

$$f(x,y) = \sum_{i=0}^{n} f_{n-i}(x)y^i$$

$$= f_0(x)y^n + f_1(x)y^{n-1} + \cdots + f_{n-1}(x)y + f_n(x).$$

Suponha que $mdc(f_0(x), f_1(x), \ldots, f_n(x)) = 1$ e que exista um elemento $\zeta \in \mathbb{L}$ para alguma extensão de $\mathbb{K}$ tal que

(i) ζ não é raiz de $f_0(x)$;
(ii) ζ é uma raiz de $f_{n-i}(x)$ para todo $1 \leq i < n$;
(iii) ζ não é uma raiz dupla de $f_n(x)$.

Então $f(x,y)$ é absolutamente irredutível.

Corolário 3.2: [5]Existe um número infinito de polinômios absolutamente irredutíveis sobre qualquer corpo.

Apresentamos agora, a proposta de construção de polinômios absolutamente irredutíveis sobre corpos finitos.

Sejam $a_1, a_2, \ldots, a_n$, onde $a_i \in GF(q)$ e $n \leq q$, definidos através da equação

$$(Y-Y_1)(Y-Y_2)\ldots(Y-Y_n) = Y^n + a_1Y^{n-1} + \cdots + a_{n-1}Y + a_n$$

sobre $GF(q)$, onde

$$\begin{aligned} a_1 &= \sum_{i=1}^{n} Y_i \\ a_2 &= \sum_{i<j} Y_iY_j \\ a_3 &= \sum_{i<j<k} Y_iY_jY_k \\ &\vdots \\ a_n &= Y_1Y_2\ldots Y_n = \prod_{i=1}^{n} Y_i. \end{aligned} \tag{3}$$

Esses valores são conhecidos como as **funções simétricas elementares** de Y_i. Observamos que, se nem todos os Y_i's são nulos, então existe pelo menos um $a_i \neq 0$. Suponha que $a_i = 0$ para todo i, então os Y_i's são todos nulos. Para mostrar que essa afirmação é verdadeira, considere $a_n = 0$, isto é, $Y_1Y_2\ldots Y_n = 0$, sem perda de generalidade, podemos assumir que $Y_n = 0$. Suponha, agora, que é sempre verdade que em decorrência dos a_i's serem zero que os Y_i's são também zeros. Assim, para $a_1 = Y_1 + Y_2 + \ldots + Y_n = 0$, temos que $Y_1 = 0$. Portanto, se $a_i = 0$ para todo i, então os Y_i's são todos nulos.

Definição 3.1: Seja $f(x,y)$ um polinômio a duas variáveis (x,y) sobre o corpo $GF(q)$ definido por

$$f(x,y) = y^n + f_{j,b}(x)\sum_{i=j}^{n} g_i(x)y^{n-i}$$

$$= p_0(x)y^n + p_1(x)y^{n-1} + \cdots + p_{n-1}(x)y + p_n(x), \tag{P1}$$

onde

- $j = \min\{k \in \{1,2,\ldots,n\} \mid a_k \neq 0\}$;
- $f_{j,b}(x) = x - b + a_j, \quad b \in GF(q)$;
- $h_i(x) = (x-b)\rho + \frac{a_i}{a_j} - b^{i-1}$;
- $g_i(x) = x^{i-1} + h_i(x), \quad i = j, \ldots, n$;
- $p_i(x) = f_{j,b}(x)g_i(x), \quad i = j, \ldots, n.$

com

$$\rho = \begin{cases} 0, & \text{se } \begin{cases} i < n \ \text{ ou } i = n \text{ e} \\ \frac{a_n}{a_j} - b^{n-1} \neq -(b-a_j)^{n-1} \end{cases} \\ 1, & \text{se } i = n \ \text{ e } \frac{a_n}{a_j} - b^{n-1} = -(b-a_j)^{n-1} \end{cases}$$

Teorema 2: O polinômio da Definição 3.1, para $n > 0$ e $n \neq 2$, é absolutamente irredutível.

Demonstração: Seja $\zeta = (b - a_j)$. Observe que ζ não é raiz de $p_0(x) = 1$, mas é raiz de $p_i(x) = f_{j,b}(x)g_i(x)$ para $j \leq i < n$, logo satisfaz (i) e (ii) da Proposição 3.2. Vamos provar agora que ζ não é raiz dupla de $p_n(x)$, isto é, não é raiz de $g_n(x)$. A prova será dividida em duas partes:

(i) Suponha que $a_n/a_j - b^{n-1} \neq -(b-a_j)^{n-1}$, $\rho = 0$ e que ζ é raiz de $g_n(x)$. Desta forma, calculando $g(\zeta) = g(b-a_j) = (b-a_j)^{n-1} + a_n/a_j - b^{n-1} = 0$, temos que $a_n/a_j - b^{n-1} = -(b-a_j)^{n-1}$, contradição. Logo, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein.

(ii) De modo análogo, supondo que $a_n/a_j - b^{n-1} = -(b-a_j)^{n-1}$ e $\rho = 1$, devemos ter que ζ não é raiz de $g_n(x)$. Vamos supor que ζ é raiz de $g_n(x)$, consequentemente $g(\zeta) = g(b-a_j) = (b-a_j)^{n-1} + (b-a_j-b) + a_n/a_j - b^{n-1} = 0$, logo $a_j = 0$. Absurdo, pois $a_j \neq 0$ para algum j. Assim, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein

Portanto, $f(x,y)$ é absolutamente irredutível pelo critério de Eisenstein. ■

Como exemplos de polinômios absolutamente irredutíveis construídos a partir da Definição 3.1, citamos os seguintes:

1) Considere $\mathbb{K} = GF(9)$ 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 (P1), $f_1(x) = x + a_1 - b = x + 1 - 0 = x + 1$, $g_1(x) = 1 + 0 = 1$, $g_2(x) = x + a_2/a_1 - b = x + 2$, $g_3(x) = x^2 + a_3/a_1 - b^2 = x^2 + 1$ e $g_4(x) = x^3 + a_4/a_1 - b^3 = x^3 + 2$. Assim,

$$\begin{aligned} f(x,y) = \; & y^4 + (x+1)y^3 + (x+1)(x+2)y^2 + \\ & + (x+1)(x^2+1)y + (x+1)(x^3+2) \end{aligned}$$

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

2) Considere $\mathbb{K} = GF(16)$ 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 (P1), $f(x,y) = y^3 + (x+1)y^2 + (x+1)(x-1)y + (x+1)x^2$. Portanto, $f(x,y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 1$.

3) Sejam $a_1 = 1, a_2 = 0, a_3 = 0$ e $b = 1$, isto é, $a_i, b \in GF(16)$, $i = 1,2,3$, assim, pelo polinômio (P1), $f(x,y) = y^3 + xy^2 + x(x-1)y + x^3 - x$. Portanto, $f(x,y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

4) Sejam $a_1 = 0, a_2 = 0, a_3 = 1$ e $b = 1$, isto é, $a_i, b \in GF(16)$, $i = 1,2,3$, logo, pelo polinômio

(P1), $f(x,y) = y^3 + x^3 + x^2 - x$. Portanto, $f(x,y)$ é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

Teorema 3: O polinômio $f(x,y) = y^2 + f_1(x)y + g(x)$, com $f_1(x) = x + c_1 - b$, é absolutamente irredutível se uma das condições abaixo for satisfeita:

(i) $g(x) = (x+c_1-b)(x+c_2/c_1-b)$, se $c_1 \neq 0$ e $c_2 \neq c_1^2$;
(ii) $g(x) = (x + c_1 - b)c_1$, se $c_1 \neq 0$ e $c_2 = c_1^2$;
(iii) $g(x) = (x + c_2 - b)$, se $c_1 = 0$.

Demonstração: Usando o fato de que $c_1 \neq 0$, então temos duas situações a considerar: $i)$ $c_2 \neq c_1^2$; e $ii)$ $c_2 = c_1^2$. Para ambas as situações, a Proposição 3.2 mostra que $f(x,y)$ é absolutamente irredutível.

Considerando agora $c_1 = 0$, temos duas situações a considerar: $i)$ $c_2 \neq 0$; e $ii)$ $c_2 = 0$. Para $i)$ temos que $f(x,y) = y^2 + (x - b)y + (x + c_2 - b)$ é absolutamente irredutível, visto que, não existe dois polinômios $h_1 = d_1x+e_1$ e $h_2 = d_2x+e_2$, tais que $h_1+h_2 = x-b$ e $h_1h_2 = x+c_2-b$. Agora, para $ii)$, temos que $f(x,y) = y^2+(x-b)y+(x-b)$. Logo, $f(x,y)$ é absolutamente irredutível pela Proposição 3.2. Portanto, $f(x,y)$ é absolutamente irredutível sobre qualquer corpo $GF(q)$, se uma das três condições for satisfeita. ■

Proposição 3.3: O polinômio

$$f(x,y) = y^2 + f_1(x)y + g(x), \tag{P2}$$

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 $g(x) = (x+a_1-b)(x+a_2/a_1-b)$, 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 $a_1 = 0$.

Demonstração: Pelo Teorema 3, temos que as condições (i) e (ii) mostram que $f(x,y)$ é absolutamente irredutível. Considerando agora, $a_1 = 0$ e $a_2 \neq 0$, temos que $f(x,y) = y^2+(x+a_2-b)$, é absolutamente irredutível, pela Proposição 3.2. Portanto, $f(x,y)$ é absolutamente irredutível sobre qualquer corpo $GF(q)$, se uma das três condições é satisfeita. ■

Por exemplo, considerando o corpo de Galois $GF(16)$ e $a_1 = \alpha$, $a_2 = \alpha^4$, $b = \alpha$. Como $a_2 \neq a_1^2$ e $a_1 \neq 0$, temos pela Proposição 3.3, que $f_1(x) = x+a_1-b = x+\alpha-\alpha = x$ e $g(x) = (x+a_2/a_1-b)(x+a_1-b) = (x+\alpha^3-\alpha)(x+\alpha-\alpha) = (x+\alpha^9)x$. Portanto, $f(x,y)$ é dado por $f(x,y) = y^2 + xy + (x+\alpha^9)x$. Dessa forma, pela Proposição 3.2, este polinômio é absolutamente irredutível sobre $GF(16)$, com $\zeta = 0$.

Considere agora, o corpo de Galois $GF(9)$ e $a_1 = 1$, $a_2 = \alpha^4$, $b = \alpha$. Como $a_2 \neq a_1^2$ e $a_1 \neq 0$, temos pela Proposição 3.3, 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, pela Proposição 3.2, este polinômio é absolutamente irredutível sobre $GF(9)$, com $\zeta = \alpha^3$.

Observação 3.1: Os polinômios (P1) e (P2), podem ser colocados 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.

IV. Curvas Algébricas sobre Corpos Finitos Associadas aos Polinômios (P1) e (P2)

Nesta seção utilizamos os resultados da seção anterior. A condição do polinômio ser absolutamente irredutível garante que a curva $\mathcal{X} : f(x,y) = 0$ é conexa. Na realidade, se $\mathcal{X}$ é estabelecida como na Definição 3.1 por 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. Com isto, faz sentido falarmos agora em construção de curvas algébricas sobre corpos finitos associadas aos polinômios (P1) e (P2) apresentados na Seção III.

Observação 4.1: Observe que a curva algébrica associada ao polinômio absolutamente irredutível (P2) sobre $GF(q)$ é não-singular.

A seguir, apresentamos vários exemplos de curvas algébricas (maximais e não-singulares) com muitos pontos racionais advindas dos polinômios (P1) e (P2). Calcularemos todos os pontos com coordenadas nos corpos finitos $GF(4)$, $GF(5)$, $GF(8)$, $GF(9)$ e $GF(16)$, para as curvas aqui mencionadas.

Exemplo 4.1: 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 $\mathcal{X}_f$ a curva definida pela equação $y^2+xy+\alpha^5y+x^2+\alpha^4x+\alpha^5 = 0$ sobre $GF(8)$, onde $f(x,y) = y^2 + xy + \alpha^5y + x^2 + \alpha^4x + \alpha^5$. Esta curva é não-singular de gênero 0. O polinômio homogêneo de f é dado por

$$F(X,Y,Z) = Y^2 + XY + \alpha^5YZ + X^2 + \alpha^4XZ + \alpha^5Z^2.$$

Esta curva tem nove pontos racionais, como mostra a tabela seguinte:

	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

Pela Definição 2.8 esta curva é maximal.

Exemplo 4.2: Seja $GF(4) = \{0, 1, \alpha, \overline{\alpha}\}$, onde $\alpha^2 = \alpha + 1 = \overline{\alpha}$. Considere a curva $\mathcal{X}$ sobre $GF(4)$ dada pela equação $y^2+xy+x^2+\alpha xz = 0$. Esta curva é não-singular com g = 0. Seus cinco pontos racionais são dados pela seguinte tabela:

	P_1	P_2	P_3	P_4	P_5
x	α	α	1	1	0
y	α	0	α	$\overline{\alpha}$	0
z	1	1	0	0	1

Como esta curva possui 5 pontos racionais, pela Definição 2.8, é uma curva maximal.

Exemplo 4.3: Encontramos dois exemplos de curvas de g $=$ 0 com 17 pontos racionais em seus modelos projetivos suaves (não-singulares) sobre $GF(16)$. Estas curvas são, portanto, definidas pelos seguintes polinômios:

$$f_1(x,y) = y^2 + xy + x^2 + \alpha^9 x,$$

e

$$f_2(x,y) = y^2 + xy + x^2 + x.$$

Os correspondentes polinômios homogêneos são:

$$F_1(X,Y,Z) = Y^2 + XY + X^2 + \alpha^9 XZ,$$

e

$$F_2(X,Y,Z) = Y^2 + XY + X^2 + XZ.$$

Os conjuntos dos pontos racionais de cada curva são dados, respectivamente, por

$$\left\{\begin{array}{llll} (\alpha^8,\alpha^{14},1); & (\alpha^4,\alpha^{12},1); & (\alpha^{14},\alpha^3,1); & (\alpha,1,1); \\ (\alpha^5,\alpha^{12},1); & (\alpha^8,\alpha^6,1); & (\alpha^7,\alpha^3,1); & (\alpha^5,\alpha^{14},1); \\ (\alpha^4,\alpha^6,1); & (\alpha,\alpha^4,1); & (\alpha^{14},1,1); & (\alpha^7,\alpha^4,1); \\ (\alpha^9,\alpha^9,1); & (\alpha^9,0,1); & (\alpha^{10},1,0); & (\alpha^5,1,0); \\ (0,0,1) & & & \end{array}\right.$$

e

$$\left\{\begin{array}{llll} (\alpha^5,\alpha^6,1); & (\alpha^5,\alpha^9,1); & (\alpha^7,\alpha^6,1); & (\alpha^7,\alpha^{10},1); \\ (\alpha^{10},\alpha^3,1); & (\alpha^{10},\alpha^{12},1); & (\alpha^{11},\alpha^3,1); & (\alpha^{11},\alpha^5,1); \\ (\alpha^{13},\alpha^9,1); & (\alpha^{13},\alpha^{10},1); & (\alpha^{14},\alpha^5,1); & (\alpha^{14},\alpha^{12},1); \\ (1,1,1); & (1,0,1); & (\alpha^{10},1,0); & (\alpha^5,1,0); \\ (0,0,1) & & & \end{array}\right.$$

Como estas curvas possuem 17 pontos racionais e g $= 0$, então pela Definição 2.8, são curvas maximais.

Exemplo 4.4: Encontramos quatro exemplos de curvas de g $= 1$ com nove pontos racionais em seus modelos projetivos não-singulares sobre $GF(4)$. Estas curvas são definidas pelos seguintes polinômios:

$$\begin{aligned} f_1(x,y) &= y^3 + x^3 + 1 \\ f_2(x,y) &= y^3 + x(x^2 + x - 1) \\ f_3(x,y) &= y^3 + xy^2 + x^2y + x(x^2 + x + 1) \\ f_4(x,y) &= y^3 + (x+1)y^2 + (x+1)^2y + x^3 + 1). \end{aligned}$$

Os correspondentes polinômios homogêneos são:

$$\begin{aligned} &F_1(X,Y,Z) = Y^3 + X^3 + Z^3 \\ &F_2(X,Y,Z) = Y^3 + X^3 + X^2Z - XZ^2 \\ &F_3(X,Y,Z) = Y^3 + XY^2 + X^2Y + X^3 + X^2Z + XZ^2 \\ &F_4(X,Y,Z) = Y^3 + XY^2 + ZY^2 + X^2Y + Z^2Y + X^3 + Z^3 \end{aligned}$$

Os pontos racionais de cada curva são dados, respectivamente, por

$$\left\{\begin{array}{lll} (1,0,1); & (\alpha,1,0); & (1,0,\alpha); \\ (\alpha^2,1,0); & (1,0,\alpha^2); & (1,1,0); \\ (0,\alpha,1); & (0,\alpha^2,1); & (0,1,1) \end{array}\right.$$

$$\left\{\begin{array}{lll} (0,0,1); & (1,\alpha,1); & (1,0,\alpha); \\ (1,\alpha^2,1); & (1,0,\alpha^2); & (1,1,0); \\ (\alpha^2,1,0); & (\alpha,1,0); & (1,1,1) \end{array}\right.$$

$$\left\{\begin{array}{lll} (0,0,1); & (\alpha,1,1); & (1,0,\alpha) \\ (\alpha^2,1,1); & (1,0,\alpha^2); & (1,1,0); \\ (\alpha^2,\alpha,1); & (\alpha,\alpha^2,1); & (1,1,1) \end{array}\right.$$

$$\left\{\begin{array}{lll} (0,1,1); & (\alpha,\alpha,1); & (1,0,\alpha); \\ (\alpha^2,1,1); & (1,0,\alpha^2); & (1,1,0); \\ (\alpha,1,1); & (\alpha^2,\alpha^2,1); & (1,0,1) \end{array}\right.$$

Pela Definição 2.8, estas curvas são maximais.

Exemplo 4.5: Seja $GF(5) = \{0,1,2,3,4\}$. Para $a_1 = 3$, $a_2 = 2$ e $a_3 = 0$, temos, pela Definição 3.1, que a curva $\mathcal{X}_f$ sobre $GF(5)$ é definida pelo polinômio $f(x,y) = y^3 + xy^2 + 3y^2 + x^2y + 2xy + 2y + x^3 + 3x^2$. O polinômio homogêneo de f é dado por $F(X,Y,Z) = Y^3 + XY^2 + 3Y^2Z + X^2Y + 2XYZ + 2YZ^2 + X^3 + 3X^2Z$. Esta curva é não-singular de gênero g $= 1$. Os dez pontos racionais desta curva são dados pela seguinte tabela:

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
x	2	0	0	0	3	4	4	1	1	4
y	0	0	3	4	2	2	3	2	3	1
z	1	1	1	1	1	1	1	0	0	0

Pela Definição 2.8, esta curva é maximal.

Exemplo 4.6: Encontramos dois exemplos de curvas de g $=$ 1 com 16 pontos racionais em seus modelos projetivos suaves (não-singulares) sobre $GF(9)$. Estas curvas são definidas pelos seguintes polinômios:

$$\begin{aligned} f_1(x,y) &= y^3 + (x+1)(x+1)y + (x+1)(x^2+1) \\ f_2(x,y) &= y^3 + x^2y + x(x^2 + x - 1). \end{aligned}$$

Os correspondentes polinômios homogêneos são:

$$\begin{aligned} F_1(X,Y,Z) = {} & XZ^2 + X^2Z + X^3 + YZ^2 + YX^2 \\ & + Z^3 + 2XYZ + Y^3 \\ F_2(X,Y,Z) = {} & Y^3 + X^2Y + X^3 + X^2Z - XZ^2. \end{aligned}$$

Os pontos racionais de cada curva são dados, respectivamente, por

$$\left\{\begin{array}{llll} (\alpha^7,1,0); & (\alpha^6,\alpha^7,1); & (1,1,1); & (\alpha^2,\alpha^5,1); \\ (\alpha^6,\alpha^3,1); & (\alpha^2,\alpha,1); & (1,\alpha,1); & (0,\alpha^3,1); \\ (0,1,1); & (0,\alpha,1); & (\alpha^6,0,1); & (\alpha^2,0,1); \\ (\alpha^4,0,1); & (\alpha^9,0,1); & (\alpha^5,1,0); & (1,1,0) \end{array}\right.$$

e

$$\left\{\begin{array}{llll} (\alpha,\alpha^3,1); & (\alpha,\alpha^7,1); & (\alpha^3,\alpha^5,1); & (\alpha^4,\alpha,1); \\ (\alpha^4,\alpha^3,1); & (\alpha^4,1,1); & (1,\alpha,1); & (1,\alpha^3,1); \\ (1,1,1); & (\alpha^3,\alpha,1); & (\alpha^5,1,0); & (1,0,\alpha^5); \\ (\alpha^7,1,0); & (1,0,\alpha^7); & (0,0,1); & (1,1,0) \end{array}\right.$$

Pela Definição 2.8, estas curvas são maximais.

O objetivo de apresentarmos estes exemplos de curvas algébricas maximais dadas pela Definição 3.1 e pela Proposição 3.3 é mostrar que existe a possibilidade de se utilizar tais curvas na construção de bons códigos lineares binários através de curvas algébricas-geométricas, usando métodos conhecidos de concatenação. Esses códigos são chamados de códigos algébricos-geométricos (códigos AG) e foram introduzidos por Goppa, [3].

V. CONCLUSÕES

Neste trabalho apresentamos uma nova proposta, até onde é de nosso conhecimento, de construção de polinômios absolutamente irredutíveis sobre $GF(q)$. Tais polinômios conduzem a geração de curvas algébricas com muitos pontos racionais que na grande maioria dos casos de interesse são caracterizadas como curvas algébricas maximais.

AGRADECIMENTOS

Os autores gostariam de agradecer à FAPESP, CNPq, CAPES e FAPEAL pelo suporte financeiro durante o período desta pesquisa.

REFERÊNCIAS

[1] Projeto Temático FAPESP, *Códigos Geometricamente Uniformes em Espaços Homogêneos*, Processo No. 02/07473-7.
[2] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, Benjamin, New York, 1969.
[3] V.D. Goppa, "Codes on algebraic curves,"*Sov. Math. Dokl*, vol. 24, pp.75-91, 1981.
[4] C.J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Mathematics, Vol. 97, USA, 1991.
[5] O. Pretzel, *Codes and Algebraic Curves*, Oxford Lecture Series in Mathematics and its Applications, No. 8, Oxford, 1998.
[6] G.O. dos Santos, *Caracterização Geométrica do Processo de Decodificação da Classe dos Códigos Alternantes Cíclicos através de Polinõmios Absolutamente Irredutíveis*, Tese de Doutorado, FEEC - UNICAMP, Abril 2003.
[7] J.H. van Lint, e G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar, vol. 12, Birkhãuser Verlag, Basel, 1988.