Decodificação de lista para códigos de F. K. Schmidt usando Bases de Gröbner

Taciana A. Souza, Francisco M. Assis, Leocarlos B. S. Lima

***Resumo*— Códigos de F. K. Schmidt são códigos algébrico-geométricos que consistem numa generalização dos códigos de Hermite. Neste artigo é apresentado um algoritmo de decodificação de lista para códigos F. K. Schmidt, que exibem melhor desempenho em comparação com algoritmos de decodificação única, que são menos flexíveis. O algoritmo apresentado emprega bases de Gröbner sobre módulos e consiste numa generalização do algoritmo proposto por Lee e O'Sullivan, em 2009, para códigos de Hermite.**

***Palavras-Chave*— Códigos algébrico geométricos, decodificação de lista, curva de F. K. Schmidt, Bases de Gröbner.**

***Abstract*— F. K. Schmidt codes are algebraic geometric codes that consist on a generalization of Hermitian codes. In this paper, a list decoding algorithm for F. K. Schmidt codes is presented, which yields better performance than single decoding algorithms, that are less flexible. The presented algorithm employs Gröbner basis on modules and is a generalization of an algorithm proposed by Lee and O'Sullivan, in 2009, for Hermitian codes.**

***Keywords*— Algebraic geometric codes, List decoding, F. K. Schmidt curve, Gröbner basis.**

I. INTRODUÇÃO

Neste artigo é apresentado um algoritmo de decodificação de lista para códigos algébrico-geométricos (AG) definidos sobres curvas, introduzidos por F. K. Schmidt (FKS). Este algoritmo é uma generalização do algoritmo introduzido por Lee e O'Sullivan [1] para a classe de códigos de um ponto definidos sobre a curva de Hermite.

O problema da decodificação de lista consiste em obter uma lista com L palavras-código que estão dentro de uma esfera de Hamming centrada do vetor recebido v. Desse modo, dada a distância de Hamming do código, a decodificação de lista permite a recuperação de erros além do limite $\lfloor \frac{d-1}{2} \rfloor$ erros de uma palavra recebida.

As vantagens da decodificação da lista foram consideradas pela primeira vez em 1957, por Peter Elias [2], explorando o comportamento assintótico da probabilidade de erro em canais discretos sem memória. Em 1997, Sudan [3] introduziu o problema de recuperar polinômios de um dado conjunto de pontos, que é um problema de grande interesse teoria de codificação e aprendizagem [2], [6], [4], [12].

Em 1999, Shokrollahi e Wasserman [12] apresentaram um esquema de decodificação de lista para códigos algébrico-geométricos. Em 2001, em sua tese, Guruswami [19] apresentou uma investigação detalhada da decodificação da lista, e demonstrou seu potencial, sua viabilidade e sua importância como um conceito combinatório e algorítmico. Além disso, em 2006, Guruswami [4] apresentou alguns resultados algorítmicos centrais da decodificação de lista, que culminaram com a dedução da capacidade de decodificação da lista.

Taciana A. Souza, Francisco M. Assis e Leocarlos B. S. Lima¸ Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande (UFCG), Campina Grande-PB, Brasil, E-mails: tacian.souza@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br, leocarlos@dee.ufcg.edu.br. Este trabalho foi parcialmente financiado pelo CNPq (141756/2015-2).

Algoritmos de decodificação de lista consistem em duas etapas básicas: interpolação, que consiste em encontrar polinômio interpolador a partir da mensagem recebida, e a fatoração, na qual são encontradas as raízes do polinômio interpolador, formando uma lista que contém L palavras-código, incluindo a palavra-código que foi enviada.

Na decodificação de lista para códigos AG, a interpolação obtém um polinômio em uma variável sobre um corpo de funções em várias variáveis, cuja fatoração é um problema que envolve um grande número de operações algébricas. Nesse sentido, na busca por algoritmos eficientes para executar a fatoração, em 2000, Roth e Ruckenstein [10] apresentaram um procedimento eficiente para decodificação de lista de códigos de Reed-Solomon, no qual a etapa de fatoração utiliza um algoritmo de reconstrução para determinar as raízes de polinômios em uma variável sobre anéis polinomiais. A fim de generalizar este algoritmo para códigos AG, Wu e Siegel [16] estenderam o algoritmo rápido de Roth e Ruckenstein para encontrar raízes de polinômios em uma variável sobre um corpo de funções. No presente trabalho, os algoritmos de interpolação e fatoração citados foram implementados utilizando o software Macaulay2.

A. Códigos Algébrico-Geométricos

Os códigos algébrico-geométricos (AG) foram introduzidos por Goppa [20], e são baseados na teoria das curvas algébrico-geométricas. Em 1982, Tsfasman et al. [7] apresentaram estudo sobre códigos AG, mostrando que estes ultrapassam o limite de Gilbert-Varshamov, o que tem um significado importante no desenvolvimento na teoria de códigos corretores de erros.

Definição 1: Seja $\mathcal{X}$ uma curva projetiva suave de gênero g.

- Um divisor D é uma soma formal $D = \sum_{P \in \mathcal{X}} n_P P$, com $n_P \in \mathbb{Z}$ e $n_P = 0$, $\forall\ P \in \mathcal{X}$;
- Um divisor é chamado efetivo se todos os valores de n_P forem não-negativos ($D \succ 0$);
- O grau do divisor D é $deg(D) = \sum n_P$.

Definição 2: Seja $\mathbb{F}$ um corpo finito com q^2 elementos. Seja D um divisor sobre uma curva $\mathcal{X}$. Definimos o espaço vetorial $L(D)$ sobre $\mathbb{F}$ por

$$L(D) := \{f \in \mathbb{F}(\mathcal{X})^* : (f) + D \succ 0\} \cup \{0\} \qquad (1)$$

Observe que se $D = \sum n_i P_i - \sum m_j Q_j$, com $n_i, m_j > 0$, então $L(D)$ consiste da função nula e das funções f no corpo

de funções que têm zeros de multiplicidade pelo menos m_j em Q_j e não têm polos, exceto possivelmente nos pontos P_i, com ordem no máximo n_i.

Definição 3: Um código algébrico-geométrico $C(D,G)$ de comprimento n sobre $\mathbb{F}$ é a imagem do mapeamento linear $ev : L(G) \longrightarrow \mathbb{F}^n$ definido por

$$ev(f) := (f(P_1), f(P_2), \cdots, f(P_n)), \tag{2}$$

em que $P_1, P_2, \cdots, P_n$ são pontos racionais de uma curva $\mathcal{X}$.

B. Códigos de F. K. Schmidt

Seja $\mathcal{X}$ uma curva FKS definida pela equação [14]

$$\mathcal{X} : y^q + y = x^s, \tag{3}$$

em que $s|(q+1)$ e o gênero g de $\mathcal{X}$ é $\frac{1}{2}(q-1)(s-1)$.

Se $s = q+1$, então $\mathcal{X}$ é uma curva de Hermite. Seja $\mathbb{F}(\mathcal{X})/\mathbb{F}$ o *corpo de funções de Hermite* sobre $\mathbb{F}$. Se $s < q+1$, então $\mathbb{F}(\mathcal{X})/\mathbb{F}$ é isomorfo a um subcorpo do corpo de funções de Hermite.

O número de pontos racionais na curva FKS é $N = q(1 + (q-1)s) + 1$ e o ponto no infinito é denotado por Q. Seja $G = uQ$ um divisor de $\mathbb{F}(\mathcal{X})/\mathbb{F}$, então a base de $L(uQ)$ é dada por [14]

$$\{x^i y^j | 0 \leq j \leq q-1,\, 0 \leq i,\, iq + js \leq u\}.$$

O código FKS é definido por

$$FKS_u = C(D,G),$$

em que $D = P_1 + P_2 + \cdots + P_n$, P_i é um ponto racional e $n = N - 1$.

Observe que se $u < n$, então ev é um mapeamento injetor em $L(uQ)$ e, pelo teorema de Riemann-Roch, a dimensão de FKS_u é igual a $\dim L(uQ) = u + 1 - g$ para $m \geq 2g - 1$. Além disso, a distância mínima de FKS_u é $n - m$ [1].

Exemplo 1: Sejam $q = 3$ e $s = 2$. Considere o corpo finito $\mathbb{F} = GF(9) = \{0, 1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$. A curva FKS será

$$\mathcal{X} : y^3 + y = x^2.$$

Esta curva FKS tem $n = 15$ pontos racionais e um ponto no infinito Q, e gênero $g = 1$.

Considere $m = 7$, então o código de FKS é definido pelo mapeamento

$$ev : L(7Q) \longrightarrow \mathbb{F}^n$$
$$ev(f) := (f(P_1), f(P_2), \cdots, f(P_{15}))$$

em que $P_1, P_2, \cdots, P_{15}$ são pontos racionais da curva $\mathcal{X}$.

II. Decodificação de Lista

A ideia da decodificação única impõe restrições ao decodificador para que seja considerada apenas a palavra que for mais próxima da mensagem original. Contudo, na década de 1950, de modo independente, Elias [2] e Wozencraft [15] propuseram que, ao invés de uma única palavra na saída do decodificador, poderia se obter uma lista com L palavras código que estão a uma distância menor ou igual a d do vetor recebido. Mesmo quando o decodificador é limitado a produzir um número relativamente pequeno de respostas, a decodificação da lista permite a recuperação de erros além do limite de $(d-1)/2$.

Um código corretor de erros é considerado um bom código quando possibilita praticamente atingir a capacidade do canal com probabilidade de erro arbitrariamente pequena. Nesse sentido, Elias [2] mostrou que, para um código C de comprimento n e taxa R, é possível escolher um tamanho da lista L grande o suficiente, de modo que a probabilidade de erro média sobre todos os códigos é quase tão pequena quanto aquela do melhor código considerado. Neste caso, demonstrou que quase todos os códigos são aproximadamente tão bons ou comparáveis aos melhores códigos.

Definição 4: Um código linear C de comprimento n sobre um corpo finito $\mathbb{F}$ é chamado (e,b)-decodificável se toda esfera de Hamming de raio e contida em $\mathbb{F}^n$ contém no máximo b palavras código.

Observe que um código $[n,k,d]$ sobre $\mathbb{F}$, com bloco de comprimento n, dimensão k e distância mínima d é $(\lfloor (d-1)/2 \rfloor, 1)$-decodificável.

Sudan [3] mostrou que um código Reed-Solomon de comprimento n e dimensão k é (e,b)-decodificável, em que e é aproximadamente $n - \sqrt{2kn}$ e b é aproximadamente $\sqrt{2n/k}$. Shokrollahi e Wasserman [12] generalizaram este resultado para a classe dos códigos AG e demonstraram o teorema seguinte.

Teorema 1: Seja C um código AG de comprimento n e dimensão k sobre uma curva algébrica de gênero g. Seja $\gamma := k + g - 1$ e $\beta := \lceil \sqrt{2\alpha n} + g - 1 \rceil$. Então, C é $(n - \beta - 1, \lceil \sqrt{2n/\gamma} \rceil)$-decodificável [12].

O passo da interpolação na decodificação de lista de códigos AG pode ser visto como o problema de encontrar o polinômio minimal de um ideal com relação a uma certa ordenação monomial. Para resolver esse problema, Lee e O'Sullivan [1] apresentaram um algoritmo baseado na teoria das bases de Gröbner sobre módulos (uma generalização da noção de espaço vetorial, em que o conjunto de escalares é um anel). Nesse algoritmo, inicialmente, é obtido um ideal a partir da palavra recebida e dos pontos racionais da curva que definem o divisor D, ou seja, $P_1, P_2, \cdots, P_n$. Em seguida, os geradores do ideal são convertidos em uma base de Gröbner de um módulo, e o polinômio minimal dessa base é encontrado, ou seja, o polinômio interpolador.

Considerando que as curvas FKS são um caso geral de curvas hermitianas [14], observe que a curva de Hermite corresponde ao caso particular da curva FKS, no qual $s = q+1$. Nossa contribuição, neste trabalho, é adaptar o algoritmo apresentado por Lee e O'Sullivan [1] ao caso da curva FKS, em que $s < q+1$. Desse modo, são enunciadas a seguir algumas notações e definições necessárias.

Seja $\mathcal{X}$ uma curva FKS definida pelo polinômio absolutamente irredutível $X^s - Y^q - Y$ sobre $\mathbb{F}$. O anel de coordenadas de $\mathcal{X}$ é o domínio de integridade

$$R = \mathbb{F}[X,Y]\langle X^s - Y^q - Y \rangle. \tag{4}$$

O corpo de funções de $\mathcal{X}$ é o corpo de frações K de R. Sejam x e y as classes residuais de X e Y em R, respectivamente. Assim, $x^s - y^q - y = 0$ e $R = \mathbb{F}[x,y]$.

Sejam $\{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ uma base de $L(uQ)$. Seja $P_i = (\alpha_i, \beta_i)$ um ponto racional $\mathcal{X}$, com $\alpha_i, \beta_i \in \mathbb{F}$. Definimos H_i para $1 \leq j \leq n$ por:

$$H_i = -\frac{(X^{q^2} - X)(Y^q + Y - {\beta_i}^q - \beta_i)}{(X - \alpha_i)(Y - \beta_i)} \in \mathbb{F}[X, Y]$$

Seja h_i a classe residual de H_i em R, e para uma palavra recebida $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}^n$. De modo análogo ao que foi apresentado para curvas de Hermite por Lee e O'Sullivan [1], definimos h_v para a curva FKS por:

$$h_v = \sum_{i=1}^{n} = v_i h_i$$

de modo que $h_i(P_i) = 1$ e 0 caso contrário, isto é, h_i se anula nos pontos P_j em que $j \neq i$. Isto implica que $ev(h_v) = v$ for $v \in \mathbb{F}^n$.

Sejam $S = \mathcal{X} \times \mathbb{A}^1_{\mathbb{F}}$ uma superfíce e o anel de coordenadas

$$R[z] = \mathbb{F}[X, Y, Z]/\langle X^s - Y^q - Y \rangle,$$

em que z denota a classe residual de Z no anel quociente.

Fixando um inteiro positivo m, chamado de multiplicidade, definimos um ideal de $R[z]$,

$$I_{v,m} = \langle z - h_v, \eta \rangle^m,$$

em que $\eta = x^{q^2} - x$.

A fim de adaptar os resultados dos teoremas e lemas apresentados por Lee e O'Sullivan [1] para a curva FKS foi observado que na demonstração do Lema 4 [1], é necessário considerar algumas mudanças, as quais são apresentadas a seguir.

Lema 1: Seja m um inteiro positivo. Seja v um vetor de $\mathbb{F}^n$. Então,

$$dim_{\mathbb{F}} R[z]/\langle z - h_v, \eta \rangle^m = n \begin{pmatrix} m+1 \\ 2 \end{pmatrix}$$

Seja $\mu \in R$ com $t = d(v, ev(\mu))$. Então,

$$dim_{\mathbb{F}} R[z]/(\langle z - h_v, \eta \rangle^m + \langle z - \mu \rangle) = m(n - t).$$

Demonstração: Considere o ideal

$$I = \langle X^s - Y^q - Y \rangle + \langle Z - H_v, X^{q^2} - X \rangle^m$$

O conjunto de zeros de I é denotado por $V(I) = \{(\alpha_i, \beta_i, v_i), 1 \leq i \leq n\}$. Essencialmente, o que foi mostrado em [1] é que, se $(a, b, c) \in V(I)$, então $(a, b, c) = (\alpha_i, \beta_i, v_i)$, para algum $1 \leq i \leq n$. Contudo, para a curva FKS é necessária uma verificação adicional para valores de a. Destacamos aqui essa verificação.

Observe que, se $(a, b, c) \in V(I)$, como $(X^{q^2} - X)^m \in I$ temos que $a^{q^2} - a = 0$. Assim, $a \in \mathbb{F}$. Contudo, ao contrário das curvas de Hermite, a curva FKS admite apenas $s(q+1)+1$ elementos possíveis na primeira coordenada de um ponto racional P_i. Então, é necessário verificar se (a, b, c) atinge esse requisito. Portanto, desde que $a \in \mathbb{F}$, temos

$$a^s - b^q - b = 0 \Rightarrow (a^s - b^q - b)^q = a^{sq} - b^{q^2} - b^q = 0 \quad (5)$$

Se $a^s \in GF(q)$ (que é a verificação necessária mencionada), então a última igualdade à direita pode ser reescrita como:

$$a^s - b^{q^2} - b^q = 0 \quad (6)$$

Subtraindo a equação à esquerda em (5) de (6), obtemos

$$a^s - b^{q^2} - b^q - (a^s - b^q - b) = 0 \Rightarrow b^{q^2} - b = 0 \Rightarrow b \in \mathbb{F}.$$

Então, $(a, b) \in \mathbb{F}^2$ é um ponto racional da curva FKS, para algum $1 \leq i \leq n$ e $(Z - H_v)^m \in I \Rightarrow c = v_i$.

Seja $\mathcal{O}_{(\alpha_i, \beta_i, v_i)}$ o anel local $K[X, Y, Z]_{\langle X - \alpha_i, Y - \beta_i, Z - v_i \rangle}$. Assim como foi apresentado no trabalho de Lee e O'Sullivan [1], o Teorema 2.2 no Capítulo 4 de Cox et al. [1] garante que, como $V(I)$ é finito, temos um isomorfismo natural

$$K[X, Y, Z]/I \cong \bigoplus_{i=1}^{n} \mathcal{O}_{(\alpha_i, \beta_i, v_i)}/I\mathcal{O}_{(\alpha_i, \beta_i, v_i)}.$$

Fixe o valor de i e o automorfismo

$$(X, Y, Z) \mapsto (X + \alpha_i, Y + \beta_i, Z + v_i)$$

induz o isomorfismo

$$\mathcal{O}_{(\alpha_i, \beta_i, v_i)}/I\mathcal{O}_{(\alpha_i, \beta_i, v_i)} \cong \mathcal{O}/I\mathcal{O},$$

em que $\mathcal{O} = K[X, Y, Z]_{\langle X, Y, Z \rangle}$.

Substituindo (X, Y, Z) por $(X+\alpha_i, Y+\beta_i, Z+v_i)$ na curva $\mathcal{X}$, obtem-se:

$$I' = \langle (X+\alpha_i)^s - Y^q - \beta_i^q - Y - \beta_i \rangle + \langle Z + AX + BY, X^{q^2} - X \rangle^m,$$

para algum $A, B \in K[X, Y]$. Pela Proposição 2.11 em Cox et al. [8], e como $V(I')$ é finito e contém a origem, tem-se:

$$dim_K \mathcal{O}/I\mathcal{O} = dim_K K[[X, Y, Z]]/I'K[[X, Y, Z]]$$

Observe que

$$(X + \alpha_i)^s - (Y + \beta_i)^q - (Y + \beta_i) = 0$$

Utilizando o binômio de Newton no termo $(X + \alpha_i)^s$ tem-se:

$$(X+\alpha_i)^s = \begin{pmatrix} s \\ 0 \end{pmatrix} X^s {\alpha_i}^0 + \begin{pmatrix} s \\ 1 \end{pmatrix} X^{s-1}\alpha_i + \cdots + \begin{pmatrix} s \\ s \end{pmatrix} X^0 {\alpha_i}^s$$

$$(X+\alpha_i)^s = X^s + \begin{pmatrix} s \\ 1 \end{pmatrix} X^{s-1}\alpha_i + \cdots + \begin{pmatrix} s \\ s-1 \end{pmatrix} X{\alpha_i}^{s-1} + {\alpha_i}^s$$

Pelo Teorema da Preparação de Weierstrass

$$Y^q + Y - (X + \alpha_i)^s + {\beta_i}^q + \beta_i = Y^q + Y - X^s -$$

$$\begin{pmatrix} s \\ 1 \end{pmatrix} X^{s-1}\alpha_i - \cdots - \begin{pmatrix} s \\ s-1 \end{pmatrix} X{\alpha_i}^{s-1} - {\alpha_i}^s + {\beta_i}^q + \beta_i$$

$$(Y - XP)U,$$

para algum $P \in K[[X]]$ e a unidade U de $K[[X, Y]]$.

Considere o ideal de $K[[X, Y, Z]]$,

$$I'K[[X, Y, Z]] = \langle Y - XP \rangle + \langle Z, X \rangle^m.$$

Assim $K[[X,Y,Z]]/I'K[[X,Y,Z]] \cong K[X,Z]\langle X,Z\rangle^m$, para todo i

$$dim_K K[X,Y,Z]/I = n\ dim_K[X,Z]/\langle X,Z\rangle^m =$$

$$dim_K K[X,Y,Z]/I = n \begin{pmatrix} m+1 \\ 2 \end{pmatrix}$$

■

Teorema 2: Suponha que $f \in I_{v,m}$ seja não nula. Seja $w = deg_u(f)$. Se $c = ev(\mu)$ é uma palavra código de C satisfazendo $d(v,c) < n - w/m$, então $f(\mu) = 0$ [1].

Considere a ordenação monomial necessária para adaptação do Algoritmo I [1] conforme definimos a seguir. Seja $\Omega = \{x^i y^j z^k | 0 \leq i, 0 \leq j \leq q-1, 0 \leq k\}$ o conjunto de monômios de $R[z]$. O grau do monômio $x^i y^j z^k$ é dado por

$$deg_u(x^i y^j z^k) = qi + sj + uk$$

Para dois monômios $x^{i_1} y^{j_1} z^{k_1},\ x^{i_2} y^{j_2} z^{k_2} \in \Omega$, definimos:

$$x^{i_1} y^{j_1} z^{k_1} >_u x^{i_2} y^{j_2} z^{k_2},$$

se $deg_u(x^{i_1} y^{j_1} z^{k_1}) >_u deg_u(x^{i_2} y^{j_2} z^{k_2})$ ou $k_1 > k_2$.

Analogamente ao algoritmo proposto por Lee e O'Sullivan [1], definimos o Q-polinômio do ideal I_M como o único elemento em $I_{v,m}$ com o menor termo líder com relação a ordenação monomial $>_u$.

Desse modo, pode-se observar que uma condição importante para a eficiência do Algoritmo I [1] é que a ordem total $>_u$ definida em $R = F[x,y]$, deve também determinar uma ordem monomial total no módulo livre (módulo que possui uma base) $R[z]_l$ sobre $F[x]$, para a curva de Hermite. Contudo, observou-se que ao aplicar o Algoritmo I para a curva FKS, se fixarmos $R[z]_l$ como um módulo em $F[x]$, a ordenação total de $R = F[x,y]$ não será mantida em $F[x]$.

Observe que o grau de y na curva FKS é igual a q, tal que $s < q+1 \Rightarrow s < q$, em que s é o grau de x. Desse modo, y tem um grau maior que x. Portanto, para preservar a ordem monomial $>_u$ devemos adaptar o Algoritmo I considerando $R[z]_l$ como um módulo livre em $F[y]$.

O anel $R = \mathbb{F}[x,y]$ pode ser considerado como um módulo livre sobre $F[y]$ com uma base $\{1, x, \cdots, x^{s-1}\}$. Assim, $R[z]_l$ é um módulo livre sobre $\mathbb{F}[y]$ com uma base $\{x^j z^i | 0 \leq i \leq l; 0 \leq j \leq s-1\}$.

Na construção do ideal $I_{v,m,l}$ definimos $\eta = y^{q^2} - y$, e o conjunto de geradores de $I_{v,m,l}$ como um módulo sobre $F[y]$ será:

$$\{x^j G_i | 0 \leq i \leq l; 0 \leq j \leq s-1\}.$$

Na próxima seção é apresentado o algoritmo de interpolação para códigos FKS como uma adaptação do Algoritmo I [1] para códigos de Hermite de um ponto. Desse modo, destacamos o Algoritmo II como nossa contribuição e, além disso, apresentamos um exemplo que foi implementado com o auxílio do software Macaulay2.

III. Resultados

Seja $T = \{(i,j) | 0 \leq i \leq l, 0 \leq j \leq q-1\}$, ordenado lexicograficamente. Então, $\{x^j z^i | (i,j) \in T\}$ é uma base para $R[z]_l$ como um $\mathbb{F}[y]$-módulo. O índice de $f \in R[z]_l$ é o maior valor de $(i,j) \in T$, tal que o coeficiente de $x^j z^i$ é não-nulo. Observe que $ind(x^j G_i) = (i,j)$. O peso de um elemento da base $x^j z^i$ é $ui + qj$. Assim, se o termo líder, com relação à $>_u$, de $f \in R[z]_l$ é $y^k x^j z^i$, então $ind(lt(f)) = (i,j)$.

Observe que o algoritmo atualiza o conjunto de geradores até $ind(lt(g_r)) = r$, para todo $r \in T$. No final do algoritmo, o conjunto atualizado de geradores é uma base de Gröbner de $I_{v,m,l}$.

A. Algoritmo II - FKS

O algoritmo encontra o elemento de $I_{v,m,l}$ com o menor termo líder.

Seja $g_{(i,j)} = \sum_{(i',j') \in T} a_{(i,j),(i',j')} x^{j'} z^{i'}$ para $(i,j) \in T$ durante a execução do algoritmo.

Inicialmente, configure $g_{(i,j)} \leftarrow x^j G_i$ para $(i,j) \in T$.

II1. Configure $r \leftarrow (0,0)$.

II2. Tome o sucessor de r. Se $r \in T$, então prossiga. Caso contrário, vá para o passo II6.

II3. Faça $p \leftarrow ind(lt(g_r))$. Se $p = r$, então volte ao passo II2.

II4. Tome $d \leftarrow deg(a_{r,p}) - deg(a_{p,p})$ e $c \leftarrow lc(a_{r,p}) lc(a_{p,p})^{-1}$.

II5. (a) Se $d \geq 0$, então faça

$$g_r \leftarrow g_r - c y^d g_p$$

(b) Se $d \leq 0$, então, armazene g_p em uma variável temporária,

$$g_p \leftarrow g_r$$

$$g_r \leftarrow y^{-d} g_r - c g_p$$

Volte para o passo II3.

II6. Saída $g_{(i,j)}$ com o menor termo líder, e termina o algoritmo.

Exemplo 2: : Seja $\mathbb{F}$ um corpo finito com q^2 elementos, em que $q = 3$ e considere a curva FKS sobre $\mathbb{F}$ com $s = 2$. Sejam os parâmetros $u = 7$, $l = 2$ e $m = 2$. A curva FKS sobre $\mathbb{F}_9$ é dada por

$$x^2 - y^3 - y = 0$$

Seja $\mathbb{F} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$. A base do espaço linear $L(uP_\infty)$ será $\{1, x, y, x^2, xy, y^2, xy^2\}$.

Seja w a mensagem enviada, ev a palavra código, e o vetor erro e v a mensagem recebida:

$\omega = [1, 0, \alpha, 0, 0, 0, 0]$.

$ev = [1, \alpha^6, \alpha, \alpha^7, 0, \alpha^3, \alpha^2, \alpha^5, \alpha^4, \alpha^7, 0, \alpha^3, \alpha^2, \alpha^5, \alpha^4]$.

$e = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$.

$v = [\alpha^4, \alpha^6, \alpha, \alpha^7, 0, \alpha^3, \alpha^2, \alpha^5, \alpha^4, \alpha^7, 0, \alpha^3, \alpha^2, \alpha^5, \alpha^4]$.

Usando o Algoritmo II construímos o seguinte ideal

$$I_{v,2,2} = \langle G_0, G_1, G_2 \rangle,$$

em que

$G_0 = y^{18} + y^{10} + y^2$

$$G_1 = y^{23} - \alpha y^{22} + y^{21} - \alpha y^{20} + y^{17} + y^{15} - \alpha y^{14} + y^{13}$$
$$+ z y^9 - \alpha y^{12} - \alpha y^{10} + y^7 - \alpha y^6 + y^5 - zy - \alpha y^4 + \alpha y^2 - y.$$

$$G_2 = y^{28} + \alpha y^{27} + \alpha y^{26} - \alpha y^{25} - \alpha y^{24} + \alpha y^{23} + \alpha y^{22} + \alpha y^{21}$$

$$-\alpha y^{19} + \alpha y^{18} - zy^{14} - \alpha y^{17} + \alpha zy^{13} + (-\alpha+1)y^{16} - zy^{12} - \alpha y^{15}$$

$$+\alpha zy^{11} + \alpha y^{13} - \alpha y^{12} - zy^8 + \alpha y^{11} + \alpha y^{10} + zy^6 - \alpha zy^5$$

$$+(-\alpha-1)y^8 + zy^4 + z^2 - \alpha zy^3 - \alpha y^6 + \alpha y^5 + \alpha zy + (\alpha-1)y^4 - z$$

$$-\alpha y^3 + \alpha^2 y^2 + \alpha y + 1.$$

Para o ideal $I_{v,2,2} = \langle G_0, yG_0, G_1, yG_1, G_2, yG_2 \rangle$, determina-se uma base de Gröbner e o polinômio minimal desta base, que será o polinômio interpolador.

Usando o Algoritmo II obtemos a base de Gröbner:

$g_0 = y^{16} - zy^8 + \alpha y^9 - y^8 + z^2 + \alpha zy - z + \alpha^2 y^2 + \alpha y + 1$

$g_1 = xy^{16} - zxy^8 + \alpha xy^9 - xy^8 + z^2 x + \alpha zxy - zx + \alpha^2 xy^2 + \alpha xy + x$

$g_2 = zy^9 - \alpha y^{10} - y^9 + z^2 y + \alpha zy^2 + \alpha^2 y^3 - y$

$g_3 = xy^9 z - \alpha xy^{10} - xy^9 + z^2 xy + \alpha zxy^2 + \alpha^2 xy^3 - xy$

$g_4 = z^2 y^2 + \alpha zy^3 + zy^2 + \alpha^2 y^4 - \alpha y^3 + y^2$

$g_5 = z^2 xy^2 + \alpha zxy^3 + zxy^2 + \alpha^2 xy^4 - \alpha xy^3 + xy^2$

O polinômio com menor termo líder é o g_4. Logo,

$Q = z^2 y^2 + \alpha zy^3 + zy^2 + \alpha^2 y^4 - \alpha y^3 + y^2$.

A fatoração do polinômio é $Q = [z - (\alpha y + 1)]^2$.

Portanto, $z = \alpha y + 1$ é uma raiz de multiplicidade igual a dois.

Observe que os coeficientes da raiz $z = \alpha y + 1$ escrita na base de $L(uP_\infty)$ dada correspondem à mensagem enviada $\omega = [1, 0, \alpha, 0, 0, 0, 0]$.

IV. Conclusões

Algoritmos de decodificação de lista têm melhor desempenho mesmo quando são necessárias listas "com apenas uma palavra código", ou seja, em comparação com algoritmos de decodificação única, que são menos flexíveis. Nesse sentido, a nossa contribuição nessa pesquisa foi a adaptação do algoritmo de decodificação de lista proposto por Lee e O'Sullivan [1] para utiliação em códigos obtidos sobre curvas FKS. Para isso, observou-se que, no caso da curva FKS, em que $s < q + 1$, é necessário alterar a ordem monomial dos polinômios.

O algoritmo apresentado foi desenvolvido para códigos de um ponto. Para trabalhos futuros, estamos interessados em adaptar o algoritmo de decodificação de lista para códigos AG multiponto obtidos a partir das curvas FKS, uma vez que tais códigos podem ter melhores parâmetros do que os códigos AG de um ponto [18].

Agradecimentos

Os autores agradecem ao CNPq, à Universidade Federal de Campina Grande (UFCG), ao Departamento de Engenharia Elétrica (DEE) e à Coordenação de Pós-Graduação em Engenharia Elétrica (COPELE).

Referências

[1] K. Lee and M. E. O Sullivan, List decoding of hermitian codes using Gröbner bases, *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1662-1675, 2009.

[2] P. Elias, List decoding for noisy channels, Research Laboratory of Electronics, Massachusetts Institute of Technology, 1957.

[3] M. Sudan, Decoding of Reed Solomon Codes beyond the Error-Correction Bound, *Journal of Complexity*, **13**, p. 180-193, 1997.

[4] V. Guruswami, Algorithmic Results in List Decoding, *Foundations and Trends in Theoretical Computer Science*, vol. 2, no 2, pp. 107-195, 2006.

[5] M. Barbier and P. S. L. M. Barreto, Key Reduction of McEliece's Cryptosystem using List Decoding, *Proceedings of the IEEE International Symposium on Information Theory*, 31 July - 05 August 2011, St. Petesburg, Russia.

[6] V. Guruswami and M. Sudan, Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes, *Foundations of Computer Science*, Proceedings. 39th Annual Symposium on. IEEE, 1998.

[7] M. A. Tsfasman, S. G. Vlădutx and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Mathematische Nachrichten*, Wiley Online Library, vol. 109, no 1, pp. 21-28, 1982.

[8] D. Cox, J.Little and D.O'Shea, Ideals, varieties, and algorithms, *Undergraduate Texts in Mathematics*, Springer, New York, 2007.

[9] L. B. S. Lima and F. M. Assis, Automorphisms of FK Schmidt codes and a new method to derive cyclic sub-codes from algebraic geometric codes, *In PIMRC*, pp. 1690-1693, 2002.

[10] R. M. Roth and G. Ruckenstein, Efficient decoding of Reed-Solomon codes beyond half the minimum distance, *IEEE Transactions on Information Theory*, vol. 46, no 1, pp. 246-257, 2000.

[11] C. E. Shannon, A mathematical Theory of Communication, *Bell System Technical Journal*, vol.27, pp. 379-423, 1948.

[12] M. A. Shokrollahi and H. Wasserman, "List decoding of algebraic-geometric codes", *IEEE Transactions on Information Theory*, vol. 45, no 2, pp. 432-437, 1999.

[13] A. N. Skorobogatov and S. G. Vladut, "On the decoding of algebraic-geometric codes", *IEEE Transactions on Information Theory*,vol. 36, no 5, pp. 1051-1060, 1990.

[14] H. Stichtenoth, "Algebraic function fields and codes", *Springer Science & Business Media*, vol. 254, 2009.

[15] J. M. Wozencraft, List decoding, *Quarterly Progress Report*, vol. 48, pp. 90-95, 1958.

[16] Wu, Xin-Wen and P. H. Siegel, Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes, *IEEE Transactions on Information Theory*, vol. 47, no 6, pp. 2579-2587, 2001.

[17] V. D. Goppa, Algebraic-geometric codes, *Math. USSR Izvestiya 3*, vol. 21, pp. 75-91, 1983.

[18] G. L. Matthews, Weierstrass Semigroups and Codes from a Quotient of the Hermitian Curve, *Designs, Codes and Cryptography 37*, no. 3, pp. 473-492, 2005.

[19] V. Guruswami, List Decoding of Error-Correcting Codes, PhD Thesis, Massachusetts Institute of Technology, 2001.

[20] V. D. Goppa, Codes on Algebraic Curves. Soviet Math. Dokl. vol 24, No.1, pp. 170-172, 1981.