EXPANSÕES POLINOMIAIS DE EXPONENCIAIS EM CORPOS FINITOS GF(p)

M. M. Campello de Souza, H. M. de Oliveira, e R. M. Campello de Souza[*]

OBJETIVOS - Uma das mais poderosas teorias em Matemática é a Análise Real. Este trabalho introduz novas ferramentas para corpos finitos, similares àquelas da Análise clássica, visando a concepção de uma Análise para corpos finitos. Esta teoria vem sendo usada em Engenharia Elétrica [1], é a base de códigos algébricos, e está relacionada, de várias formas, a campos de investigação tais como criptografia, espalhamento espectral e análise de sinais através das transformadas de corpo finito.

PRINCIPAIS RESULTADOS - Uma trigonometria em corpos finitos foi recentemente introduzida [2]. Qualquer função de GF(p) para GF(p), definida por N pontos, pode ser escrita como um polinômio de grau N-1; por exemplo, $2^i \equiv i^3+1 \pmod 5$. Em geral existem N coeficientes e esta decomposição corresponde à série de MacLaurin finita com a vantagem de que não existem erros. Por exemplo, a função 1-cos sobre GF(5) fornece (pela fórmula de interpolação de Lagrange) $\cos_1(i) \equiv 1 - 2i - i^2 + 2i^3 \pmod 5$ e a função 1-seno expandida: $\text{sen}_1(i) \equiv j(i^3 - i^2 - 2i) \pmod 5$. A fórmula de Euler sobre um corpo de Galois é verificada em termos de séries, e.g. $\cos(i)+j\text{sen}(i) \equiv i^3+1 \equiv 2^i \pmod 5$. A unicidade da decomposição em série pode ser estabelecida por: *Proposição1:* Dada uma função definida por seus valores f(x), $\forall x \in$ GF(p), existe somente uma série de Maclaurin para f.■ Em corpos finitos, há essencialmente interesse em derivadas de polinômios, uma vez que outras funções podem ser expandidas em série. A derivada clássica sobre corpos finitos apresenta problemas, uma vez que as derivadas de ordem maior ou igual a característica do corpo se anulam. Tendo por base a derivada de Hasse [3], um novo conceito de derivada em um corpo finto é introduzido para explorar a estrutura cíclica. Diferentemente da derivada de Hasse, $a^{[r]}(x)$, a qual sempre decrementa o grau do polinômio, a derivada negacíclica de Hasse introduzida aqui, considera o anel polinomial GF(p)[x] módulo $x^{p-1}+1$. A derivada de uma constante não mais se anula e o grau da função polinomial é preservado. Em um corpo finito, a série de Taylor pode ser expandida em torno de um ponto arbitrário $\beta \in$ GF(p). É interessante observar que, trabalhando com $x^p - 1 \equiv 0$, tem-se um resto de Lagrange $R_p(\zeta)$ nulo, embora ζ não tenha sentido. Seja a expansão β-ádica de a(x): $a(x) \equiv b_0 + b_1(x-b) + b_2(x-b)^2 + ... + b_{N-1}(x-b)^{N-1}$, com b_0=a(β). Tem-se que $a^{[r]}(\beta) \equiv C_N^r\, b_r$. A unicidade da série de Taylor de corpo finito segue de [4]. Expansões β-ádicas módulo p=3, para 2^x em GF(3) são: $2^x \equiv 2 + 2(x-1)^2$ 1-ádica; $2^x \equiv 1 + (x-2) + 2(x-2)^2$ 2-ádica. Considerando-se o anel GF(p)[x], com $x^{p-1}+1 \equiv 0$, então as derivadas negacíclicas de Hasse podem ser usadas. Desde que grau(a(x))=p-2, séries clássicas podem ser truncadas, e.g., $(e^x)_7 \equiv 1 + x + 4x^2 + 6x^3 + 5x^4 + x^5 \pmod 7$. Para se introduzir funções trigonométricas, é possível considerar o complexo $j = \sqrt{-1}$, desde que -1 é um resíduo não quadrático para p≡3 (mod 4) e escolher exp(j i) tal que: cos(i)=$\mathfrak{Re}$ exp(j i)$\equiv 1 + 4i^2 + 5i^4 \pmod 7$, sen(i)=$\mathfrak{Im}$ exp(j i) $\equiv i + 6i^3 + i^5 \pmod 7$. É fácil verificar que cos(i) é uma função par e sen(i) é ímpar. A derivada negacíclica de Hasse resulta em: $\text{sen}^{[1]}\, i = \cos(i)$ and $\cos^{[1]} i = -\text{sen}(i)$. Resultados podem ser generalizados para definir funções *hiperbólicas* sobre corpos finitos, p ímpar, de acordo com o desenvolvimento em série. Usando a convenção $\alpha^{-\infty}=0$ $(\forall\alpha) \in$ GF(p), outras funções tais como a hipérbole 1/x podem ser definidas. i = 0 1 2 3 4 1/i = -∞ 1 3 2 4. Finalmente, é interessante considerar a função logaritmica sobre um corpo finito como o inverso da função exponencial. Assim, em GF(5), tem-se i = 0 1 2 3 4 $\log_2$ i = -∞ 0 1 3 2. Algumas propriedades interessantes são satisfeitas por tais logaritmos. Sejam A, B ∈ GF(p) e α um elemento de ordem ord(α). Então $\log_\alpha A.B \equiv \log_\alpha A + \log_\alpha B \pmod{\text{ord}(\alpha)}$. A mudança da base de um logaritmo também é possível. Seja β um elemento primitivo de GF(p). Então $\log_\alpha x \equiv \log_\beta x.(\log_\beta \alpha)^{-1} \pmod{\text{ord}(\alpha)}$. Um outro resultado estabelece uma ligação entre a derivada de Hasse e a Transformada de Fourier de Corpo Finito [5]. A função de corpo finito f obtida pela permutação dos elementos da imagem de f é referida como sendo uma permutação-f. *Proposição 2:* Os coeficientes da expansão em série de McLaurin de um dado sinal f correspondem a transformada de Fourier de corpo finito inversa de uma permutação-f. ■

CONCLUSÕES - O objetivo principal deste trabalho é introduzir novas ferramentas úteis para aplicações em Engenharia envolvendo corpos finitos. Neste contexto, funções discretas são consideradas e séries de MacLaurin são derivadas por interpolação de Lagrange. Uma nova derivada sobre corpos finitos é definida, a qual é baseada na derivada de Hasse e é referida como a derivada negacíclica de Hasse. Séries de Taylor sobre corpos finitos e expansões α-ádicas sobre GF(p) são então consideradas. Funções trigonométricas e exponenciais sobbre corpos finitos são apresentadas. Estas ferramentas são úteis em teoria da codificação, criptografia e processamento digital de sinais.

REFERÊNCIAS - [1] R.J. McEliece, "Finite Fields for Computer Scientists and Engineers", Kluwer, 1987. [2] R.M. Campello de Souza, H.M. de Oliveira, A.N. Kauffman and A.J.A. Paschoal, "Trigonometry in Finite Fields and a New Hartley Transform", Proceedings of the 1998 IEEE *Int. Symp. on Infor. Theory*, ISIT98, MIT, Cambridge, MA, p.293, 1998. [3] J.L. Massey, N. von Seemann and P.A. Schoeller,"Hasse Derivatives and Repeated-root Cyclic Codes", IEEE *Int. Symp. on Infor. Theory*, ISIT, Ann Arbor, USA, 1986. [4] S. Lang, Linear Algebra, Addison-Wesley Pub. Co., 1966. [5] R. E. Blahut, "Transform Techniques for Error-Control Codes", *IBM J. Res. Develop.*, 23, No.3, pp. 299-314, May, 1979.

[*] CODEC - Grupo de Pesquisas em Comunicações. Departamento de Eletrônica e Sistemas - CTG–UFPE C.P. 7800, 50711-970, Recife-PE , Brasil. E-mail: Ricardo@npd.ufpe.br , hmo@npd.ufpe.br, marciam@npd.ufpe.br