A Transformada Numérica de Pascal

A. J. A. Paschoal, H. M. de Oliveira e R. M. Campello de Souza

***Resumo* – Uma nova transformada linear sobre corpos finitos é introduzida, a transformada numérica de Pascal (TNP). A matriz de transformação da TNP é obtida do triângulo de Pascal, com elementos considerados sobre GF(p). Algumas propriedades da TNP são apresentadas e potenciais aplicações da mesma são sugeridas.**

Palavras-Chave— Transformada de Pascal, Triângulo de Pascal, Corpos Finitos.

***Abstract* – A new linear transform over finite fields is introduced, the number theoretic Pascal transform (NTPT). The NTPT transformation matrix is obtained from Pascal`s triangle, with elements taken modulo p. A few properties of the NTPT are presented and possible applications are suggested.**

Keywords – Pascal Transform, Pascal Triangle, Finite Fields.

I. INTRODUÇÃO

O triângulo de Pascal, conhecido desde o século XIV, tem sido utilizado em aplicações que envolvem as áreas de processamento de sinais [1,2], processamento de imagem [3], análise numérica [4], probabilidade [5], entre outras.

Existem diversas definições para a chamada matriz de Pascal [6]. Artigos vêm sendo publicados explorando propriedades destas matrizes. Neste artigo, é introduzida a Transformada de Pascal sobre o corpo finito GF(p).

Na seção II apresenta-se o triângulo de Pascal e sua versão sobre GF(3) e algumas matrizes de Pascal são apresentadas. Mostra-se como a matriz de Pascal pode ser decomposta em um produto de duas matrizes (uma triangular superior e outra triangular inferior). A partir desta decomposição, mostra-se como obter a matriz inversa de Pascal.

Na Seção III define-se a Transformada Numérica de Pascal - TNP. Na Seção IV são apresentadas algumas propriedades da TNP. Na Seção V são enumeradas possíveis áreas de aplicação para as novas ferramentas introduzidas neste trabalho.

II. PRELIMINARES

Pascal em seu *Traité du Triangle Arithmétique* (1654) explorou as propriedades do triângulo que hoje é conhecido como triângulo de Pascal, também conhecido como triângulo de Tartaglia (italianos), triângulo de Yang Hui (chineses) ou ainda, triângulo aritmético. Em verdade, o trabalho de Pascal foi o resultado de uma das conversas frutíferas com Pierre de Fermat [7].

Existem muitos formatos de apresentação do referido triângulo.

1	1
1 1	1 1
1 2 1	1 2 1
1 3 3 1	1 0 0 1
1 4 6 4 1	1 1 0 1 1
⋮ ⋮	⋮ ⋮
(a)	(b)

Fig. 1: (a) Triângulo de Pascal. (b) Triângulo de Pascal sobre GF(3).

O triângulo de Pascal foi explorado por Newton na determinação do conhecido binômio de Newton.

Existem muitas definições para a matriz de Pascal de ordem *N* [8]. Aqui usaremos a definição a seguir:

$$[P_{ik}] := C_{i+k}^{i},$$

em que C_{i+k}^{i} denota a combinação de $(i+k)$, i a i.

A matriz de Pascal definida assim pode ser decomposta como o produto de uma matriz triangular superior por uma matriz triangular inferior. Tal decomposição é conhecida como decomposição de Cholesky [8], [9].

Exemplo 1: Decomposição de uma matriz de Pascal de ordem 5.

$$P_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{bmatrix},$$

$$L_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}, U_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$P_5 = L_5 U_5.$$

Mostra-se que, para todo *N*, a fatoração de Cholesky $P_N = L_N U_N$ é sempre possível [8], [9], em que L_N é uma matriz triangular inferior de elementos

$$L_{ik} := \begin{cases} C_i^k, & i > k, \\ 0, & caso\ contrário, \end{cases}$$

Arquimedes Paschoal, Engenharia Mecânica, Instituto Federal de Pernambuco,Caruaru,Brasil,E-mail: arquimedes.paschoal@caruaru.ifpe.edu.br. Hélio M. Oliveira, Departamento de Matemática e Estatística, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mail: hmo@ufpe.br. Ricardo Campello, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil. E-Mail: ricardo@ufpe.br.

e $U_N = {L_N}^T$. A matriz inversa de Pascal é obtida por meio de $P_N^{-1} = U_N^{-1}L_N^{-1}$, em que

$$ {L_{ik}}^{-1} = \begin{cases} (-1)^{i-k}C_i^k, & i > k, \\ 0, & caso\ contrário. \end{cases} \quad (1) $$

Algumas propriedades da matriz de Pascal são:

(i) P_N é simétrica e positiva definida.
(ii) Determinante de P_N é igual a 1.
(iii) Os autovalores das matrizes P_N e P_N^{-1} são reais e positivos.

III. A TRANSFORMADA NUMÉRICA DE PASCAL

A transformada de Pascal apresentada neste trabalho relaciona sequências com elementos em GF(p), sendo, portanto, denominada transformada numérica de Pascal (TNP).

Definição: A Transformada numérica de Pascal da sequência $\mathrm{v} = (\mathrm{v}_0, \mathrm{v}_1, \dots, \mathrm{v}_{\mathrm{N}-1})$, $\mathrm{v_i} \in \mathrm{GF(p)}$, é a sequência $\mathrm{V} = (\mathrm{V}_0, \mathrm{V}_1, \dots, \mathrm{V}_{\mathrm{N}-1})$, $\mathrm{V_k} \in \mathrm{GF(p)}$, em que

$$ V_k := \sum_{i=0}^{N-1} C_{i+k}^i \, v_i \ (mod\ p). \quad (2) $$

Em formato matricial, escreve-se $V = Pv$, em que os elementos da matriz são $[P]_{i,k} = C_{i+k}^i$.

Exemplo 2: Considere a matriz de Pascal de ordem 4 sobre GF(5),

$$ P_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 1 & 0 \\ 1 & 4 & 0 & 0 \end{bmatrix}. $$

A TNP da sequência $v = (2,2,1,1)$ é a sequência $V = [1\ 3\ 4\ 0]$.

Teorema 1 (Transformada Inversa) - A TNP inversa da sequência $V = (V_0, V_1, \dots, V_{N-1})$, $V_k \in GF(p)$, é a sequência $v = (v_0, v_1, \dots, v_{N-1})$, $v_i \in GF(p)$, em que

$$ v_i = \sum_{k=0}^{N-1} \left[(-1)^{i+k} \sum_{j=Max(i,k)}^{N-1} C_j^i C_j^k \right] V_k. \quad (3) $$

Prova: Considerando-se a fatoração de Cholesky, pode-se escrever $\mathrm{P_N^{-1}} = \mathrm{U_N^{-1}L_N^{-1}}$. Da expressão (1), e considerando-se que $\mathrm{U_N} = \mathrm{L_N}^{\mathrm{T}}$, chega-se a

$$ [P_N^{-1}]_{i,k} = (-1)^{i+k} \sum_{j=Max(i,k)}^{N-1} C_j^i C_j^k $$

e o resultado segue. ∎

Por meio da relação de Pascal, é possível obter uma definição alternativa da TNP.

Proposição 1: As componentes da sequência V podem ser escritas em função da componente V_0 e dos valores da sequência $v = (v_0, v_1, \dots, v_{\mathrm{N}-1})$ por meio de

$$ V_k = V_0 + \sum_{i=0}^{N-2} \left[\sum_{r=i}^{k} C_{i+r}^r \right] v_{i+1} \quad (4) $$

em que $\mathrm{V}_0 = \sum_{\mathrm{i}=0}^{\mathrm{N}-1} \mathrm{v_i}$.

Prova:

Partindo-se da relação de Pascal

$$ C_{i+k}^i = C_{i+k-1}^{i-1} + C_{i+(k-1)}^i. $$

Multiplicando-se ambos os lados desta expressão por $\mathrm{v_i}$ e somando em $\mathrm{i} = 0, 1, \cdots, \mathrm{N}-1$, chega-se a

$$ V_k = V_{k-1} + \sum_{i=0}^{N-2} C_{i+k}^i \, v_{i+1}. \quad (5) $$

Substituindo-se sucessivamente os valores $k = 1,2, \cdots$ resulta em

$$ V_k = V_0 + \sum_{i=0}^{N-2} \left[\sum_{r=i}^{k} C_{i+r}^r \right] v_{i+1}. $$

Sobre corpos finitos é possível obter TNPs cujas matrizes de transformação são do tipo triangular superior em relação à diagonal secundária.

Proposição 2: Se p é um número primo, então, $C_{p+r}^k \equiv 0\ (mod\ p)$, $r = 0, 1, 2, \dots, k-1$.

Prova:

$k!\ C_{p+r}^k = (p+r)(p+r-1) \dots (p+r-k+1)$;

como $0 \le r \le k-1$, então p é um dos fatores do lado direito da expressão anterior. Assim, podemos escrever $k!\ C_{p+r}^k \equiv 0\ (\mathrm{mod}\ p)$, o que implica que $p|k!$ ou $p|C_{p+r}^k$. Mas a primeira opção implica que $p|j$ para algum j tal que $1 \le j \le k \le p-1$, o que não é possível. Portanto, $p|C_{p+r}^k$ ou $C_{p+r}^k \equiv 0\ (\mathrm{mod}\ p)$. ∎

Este resultado tem implicações referentes às matrizes de transformação das TNP cujo comprimento é um número primo.

Proposição 3: A matriz de transformação da TNP, definida sobre GF(p), cujo comprimento N é um número primo, p, tem todos os elementos abaixo de sua diagonal secundária iguais a zero.

Prova: Por definição, o elemento P_{ik} da matriz de transformação da TNP é dado por C_{i+k}^i. Os elementos abaixo da diagonal secundária são tais que $i + k \ge N\ (= p)$, ou seja, $i + k = p + r$ para algum r tal que $0 \le r \le k-1$. Portanto, para estes elementos, podemos escrever

$$ C_{i+k}^i = C_{p+r}^{p+r-k} = C_{p+r}^k $$

e, da proposição 1, o resultado segue. ∎

Exemplo 2: Matriz de transformação da TNP de comprimento 5 sobre GF(5):

$$P_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Algumas propriedades dessa família de TNP podem ser verificadas:

i) A TNP de um impulso é uma constante.
ii) A TNP de uma constante é um impulso deslocado.
iii) Uma dada componente V_k depende apenas das componentes $v_i, 0 \leq i \leq p-1-k$.
iv) A inversa da matriz P_p é triangular inferior em relação à diagonal secundária. Seus elementos são os mesmos de P_p porém aparecem refletidos em relação à esta diagonal.
v) A soma dos elementos das linhas de P_p, com exceção da última linha, é congruente a zero módulo p.
vi) As complexidades multiplicativa e aditiva para se computar a TNP são, respectivamente:

$$M(N) = \frac{p(p+1)}{2}, \quad (6)$$

$$A(N) = \frac{p(p-1)}{2}. \quad (7)$$

IV. PROPRIEDADES DA TNP

P1: Linearidade

$$\sum_{i=0}^{N-1} C_{i+k}^{i} \left(\alpha v_i + \beta u_i\right) = \alpha \sum_{i=0}^{N-1} C_{i+k}^{i} v_i + \beta \sum_{i=0}^{N-1} C_{i+k}^{i} u_i,$$

$$\alpha v + \beta u \leftrightarrow \alpha V + \beta U.$$

P2: Deslocamento no Tempo

Considere a sequência $b = (b_0, b_1, \ldots, b_{N-1})$ em que $b_i = v_{i-m}$. Então, $b \leftrightarrow B$, em que

$$B_k = \sum_{i=-m}^{N-1-m} C_{i+m+k}^{i+m} v_i.$$

P3: Impulso

A TNP da sequência $\delta[n] = [1\ 0\ \cdots\ 0\ 0]$ é a sequência $V = [V_0\ V_1 \cdots V_{N-1}]$, em que $V_k = 1,\ \forall k$.

P4: Constante

A TNP da sequência constante unitária $v = (1, 1, \ldots, 1)$ é a sequência $V = [V_0\ V_1 \cdots V_{N-1}]$ em que $V_k = C_{N+k}^{k+1}$.

V. COMENTÁRIOS

Transformadas definidas sobre corpos finitos tem sido aplicadas em diversas áreas, tais como:

- Marcas d'água digital [14].
- Multiplexação e Sistemas de múltiplo acesso [15], [16].
- Codificação de canal [17], [18].
- Criptografia [19], [20].
- Espalhamento espectral [21], [22].
- Processamento de Sinais [2], [23].
- Comunicação multiusuário [24].

Especificamente, diversas versões de transformadas sobre corpos finitos vêm sendo aplicadas, de modo que as propriedades e a viabilidade da aplicação da TNP, nestes cenários, precisa ser investigada.

VI. CONCLUSÕES

Neste trabalho uma nova transformada linear sobre corpos finitos é proposta, a transformada numérica de Pascal (TNP). A matriz de transformação da TNP de comprimento N, P_N, é obtida por meio do triângulo de Pascal, com seus elementos considerados módulo p, sendo uma matriz simétrica com determinante igual a 1. A matriz P_N admite a fatoração de Cholesky, por meio da qual chega-se à TNP inversa. Algumas propriedades da TNP foram apresentadas e, por meio da relação de Pascal, uma definição alternativa recursiva para a TNP foi proposta.

Um caso de interesse especial observado é a TNP de comprimento p sobre $GF(p)$. Esta transformada, denominada TNP prima, tem matriz P_p triangular superior em relação à diagonal secundária, portanto, apresentando uma implementação direta com complexidade aritmética inferior a das outras. Algumas possíveis aplicações da TNP nas áreas de sistemas de comunicação multiusuário e codificação de canal estão sendo investigadas.

REFERÊNCIAS

[1] F. J. García-Ugalde, B. Psenicka, M. O. Jiménez-Salinas, "Z Transformation by Pascal Matrix and its Applications in the Design of IIR Filters", *Journal of Applied Research and Technology*, 9 (2011) 355-366.

[2] S. Gudvangen, and H. Buskerud. "Practical applications of number theoretic transforms." NORSIG-99, Norwe (1999).

[3] T. J. Goodman, M. F. Aburdene, "A Hardware Implementation of the discrete Pascal transform for image processing", *SPIE-IS&T*, 2006.

[4] L. Aceto, "Some applications of the Pascal matrix to the study of numerical methods for differential equations", *Bollettino dell'Unione Matematica Italiana*, Serie 8, Vol. 8-B (2005) 639–651.

[5] G. S. Call, and D. J. Velleman, "Pascal's Matrices", *The American Mathematical Monthly*, Vol. 100, (1993) 372-376.

[6] B. Birregah, P. K. Dohb, K. H. Adjallah, "A systematic approach to matrix forms of the Pascal triangle: The twelve triangular matrix forms and relations", *European Journal of Combinatorics*, 31 (2010) 1205-1216.

[7] C. Cobeli and A. Zaharescu, "Promenade around Pascal Triangle - Number Motives", *Bull. Math. Soc. Sci. Math. Roumanie* Tome 56.104 (2013), 73-98.

[8] A. Edelman and G. Strang, "Pascal Matrices" *American Mathematical Monthly*, Mar. 2004, p. 189.

[9] G. Strang, *Introduction to Linear Algebra*, 3rd edition, Wellesley-Cambridge Press, 2003.

[10] M. E. A. El-Mikkawy, "On solving linear systems of the Pascal type", *Applied Mathmatics and Computation*, 2003.

[11] X-G. Lv, T-Z. Huang, Z-G. Ren, "A new algorithm for linear systems of the Pascal type", *Journal of Computational and Applied Mathematics* 225 (2009) 309-315, 2009.

[12] R. Bacher, R. Chapman, "Symmetric Pascal matrices modulo p", *European J. Combinatorics* 25 (2004), 459-473.

[13] M. F. Aburdene and T. Goodman, "The Discrete Pascal Transform and its Applications," *IEEE Signal Processing Letters*, vol. 12, (2005), pp. 493-495.

[14] R. J. S. Cintra, V. S. Dimitrov, H. M. de Oliveira, R. M. Campello de Souza, "Fragile watermarking using finite field trigonometrical transforms", *Signal Processing: Image Communication* 24 (2009) 587-597. http://arxiv.org/abs/1502.00296

[15] H. M. de Oliveira, R. M. Campello de Souza, A. N. Kauffman, "Efficient multiplex for band-limited channels: Galois-Field division multiple access", Workshop on Coding and Cryptography, (1999) 235-241.

[16] J. P. C. L. Miranda, H. M. de Oliveira, "On Galois-Division Multiple Access Systems: Figures of Merit and Performance Evaluation", XIX Simposio Brasileiro de Telecomunicacoes, 2001, Fortaleza, CE, Brazil. http://arxiv.org/abs/1502.03698

[17] R. E. Blahut, *Theory and practice of error control codes*. Addison-Wesley, 1983.

[18] R. M. Campello de Souza, E. S. V. Freire, H. M. de Oliveira, "Fourier codes", Tenth International Symposium on Communications Theory and Applications, Ambleside, United Kingdom, 275-370, 2009. http://arxiv.org/abs/1503.03293

[19] J. L. Massey, "The discrete Fourier transform in coding and cryptography." *IEEE Inform* (1998).

[20] J. B. Lima, E. A. O. Lima and F. Madeiro. "Image encryption based on the finite field cosine transform." *Signal Processing: Image Communication* 28.10 (2013): 1537-1547.

[21] H. M. de Oliveira, J. Miranda, R. M. Campello de Souza, "Spread Spectrum Based on Finite Field Fourier Transforms", ICSECIT 2001–International Conference on Systems Engineering, Communications and Information Technologies. http://arxiv.org/abs/1503.08109

[22] H. M. de Oliveira, R. M. Campello de Souza, A. N. Kauffman, "Orthogonal multilevel spreading sequence design", *Coding, Communications and Broadcasting,* 291-303. http://arxiv.org/abs/ 1502.05881

[23] H. M. de Oliveira, T. H. Falk, R. F. G. Távora, "Decomposição de Wavelets Sobre Corpos Finitos", *Revista da Sociedade Brasileira de Telecomunicaçoes* 17 (2002), 38-47.

[24] R. M. Campello de Souza, H. M. de Oliveira, "Eigensequences for Multiuser Communication over the Real Adder Channel",VI International Telecommunications Symposium (ITS2006). http://arxiv.org/abs/1502.03400