Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Novas Relações na Matriz de Transformação da Transformada Numérica de Pascal

Arquimedes J. A. Paschoal[1]
Departamento de Engenharia Mecânica, IFPE/Caruaru
Ricardo M. Campello de Souza[2]
Departamento de Eletrônica e Sistemas, UFPE
Hélio M. de Oliveira[3]
Departamento de Estatística, UFPE

Resumo. Neste artigo, a matriz de transformação da transformada numérica de Pascal (TNP) é investigada e novas relações baseadas na decomposição desta matriz, por meio do produto de Kronecker de duas matrizes de Pascal, são propostas com aplicações na implementação da TNP.

Palavras-chave. Transformada numérica de Pascal, triângulo de Pascal modular, corpos finitos.

1 Preliminares

Uma das principais razões de se pesquisar transformadas numéricas é o fato das mesmas não apresentarem o chamado erro de arredondamento ou truncagem, uma vez que toda a aritmética se efetua em um corpo finito. Recentemente foi introduzida a transformada numérica de Pascal (TNP) [11], definida sobre o corpo finito $GF(p)$ e baseada no triângulo de Pascal modular. Esta transformada apresenta o interessante aspecto de que seu comprimento e a característica do corpo são independentes, o que não acontece nas demais transformadas numéricas conhecidas na literatura [3], [5]. Neste cenário, Uma questão relevante, de um modo geral, é a complexidade aritmética (entendida aqui como o número de multiplicações e adições) necessária ao cálculo da transformada. Muitos algoritmos eficientes têm sido desenvolvidos visando reduzir esta complexidade aritmética [3]. A utilização do triângulo de Pascal [2] na definição da TNP permite que sejam exploradas relações bem conhecidas, o que leva a implementações eficientes da mesma [12].

Definição 1.1. A transformada numérica de Pascal (TNP) da sequência $v = (v_0, ..., v_{N-1})$, $v_i \in GF(p)$, é a sequência $V = (V_0, V_1, ..., V_{N-1}), V_k \in GF(p)$, em que

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

[1]arquimedes.paschoal@caruaru.ifpe.edu.br
[2]ricardo@ufpe.br
[3]hmo@de.ufpe.br https://arxiv.org/a/deoliveira_h_1.html

DOI: 10.5540/03.2018.006.01.0404

Em formato matricial, tem-se $V = P_N v$, em que os elementos de P_N são $[P_N]_{i,k} := C^i_{i+k}, i, k = 0, 1, \cdots, N-1$.

Teorema 1.1. *(Transformada Inversa) A TNP inversa da sequência $V = (V_0, ..., V_{N-1})$, $V_k \in GF(p)$, é a sequência $v = (v_0, ..., v_{N-1}), v_i \in GF(p)$, em que*

$$v_i = \sum_{k=0}^{N-1} \left[(-1)^{i+k} \sum_{j=Max(i,k)}^{N-1} C^i_j C^k_j \right] V_k. \tag{2}$$

Algumas propriedades da TNP de comprimento $N = p$, sobre $GF(p)$, podem ser verificadas [11]:
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 a 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,

$$M(N) = \frac{p(p+1)}{2}, \quad A(N) = \frac{p(p-1)}{2}. \tag{3}$$

2 Decomposição da Matriz de Pascal Modular

A matriz de Pascal sobre $GF(p)$ apresentada em [11] pode ser decomposta como o produto de Kronecker de duas matrizes de Pascal quando a ordem desta matriz puder ser fatorada como o produto $N = Lp$. Esta importante propriedade tem relação com a autoestrutura da TNP.

Teorema 2.1. *A matriz de Pascal P_N, em que $N = Lp$, sobre o corpo finito $GF(p)$, pode ser obtida a partir do produto de Kronecker $P_N = P_L \otimes P_p$, em que P_L e P_p são matrizes de Pascal de ordem L e p, respectivamente.*

Prova. Pela definição do produto de Kronecker, tem-se que os elementos da matriz $A \otimes B$, em que A é uma matriz $m \times n$ e B é uma matriz $p \times q$, são obtidos multiplicando-se cada elemento da matriz A pela matriz B, obtendo-se assim uma matriz $mp \times nq$. Como as matrizes de Pascal são quadradas, tem-se $m = n = L$ e $p = q$. Então, a matriz resultante do produto de Kronecker possui ordem Lp. Considere o produto de Kronecker $P_N = P_L \otimes P_p$, em que

$$P_L = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & C^1_2 & \cdots & C^1_L \\ \vdots & \vdots & \ddots & \vdots \\ 1 & C^{L-1}_L & \cdots & C^{L-1}_{2L-2} \end{bmatrix} \quad e \quad P_p = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & C^1_2 & \cdots & C^1_p \\ \vdots & \vdots & \ddots & \vdots \\ 1 & C^{p-1}_p & \cdots & C^{p-1}_{2p-2} \end{bmatrix}.$$

DOI: 10.5540/03.2018.006.01.0404

Tem-se,

$$P_N = P_L \otimes P_p = \begin{bmatrix} P_p & P_p & \cdots & P_p \\ P_p & C_2^1 P_p & \cdots & C_L^1 P_p \\ \vdots & \vdots & \ddots & \vdots \\ P_p & C_L^{L-1} P_p & \cdots & C_{2L-2}^{L-1} P_p \end{bmatrix}.$$

Sejam r e s os índices que identificam os blocos formados pelas cópias da matriz P_p multiplicada pelos termos binomiais de P_L. Então $r, s = 0, 1, ..., L-1$ e $[P_L]_{r,s} = C_{r+s}^r$. A matriz $P_N = P_L \otimes P_p$ é formada pelos elementos obtidos pela multiplicação $C_{r+s}^r C_{\widehat{i}+\widehat{j}}^{\widehat{j}}$, em que $\widehat{i}, \widehat{j} = 0, 1, ..., p-1$. Note que os índices das linhas (i) e das colunas (j) da matriz P_N são dados por

$$i = \widehat{i} + rp, \quad j = \widehat{j} + sp,$$

em que[1] $r = \lfloor \frac{i}{p} \rfloor$ e $s = \lfloor \frac{j}{p} \rfloor$. Assim,

$$(P_L \otimes P_p)_{i,j} = C_{r+s}^r C_{\widehat{i}+\widehat{j}}^{\widehat{j}} (\text{mod } p) = \frac{(r+s)!}{r!s!} \cdot \frac{[(i+j)-(r+s)p]!}{(i-rp)!(j-sp)!}.$$

Deseja-se provar que

$$(P_L \otimes P_p)_{i,j} = \frac{(r+s)!}{r!s!} \cdot \frac{[(i+j)-(r+s)p]!}{(i-rp)!(j-sp)!} = C_{i+j}^i (\text{mod } p). \tag{4}$$

Fixando os valores de r e s, a prova é feita por indução em i. Por simetria, a prova por indução em j é semelhante.

i) Passo base: $i = 0 \Rightarrow r = 0$. Então

$$\frac{(0+s)!}{0!s!} \cdot \frac{[(0+j)-(0+s)p]!}{(0-0p)!(j-sp)!} = 1 = C_{0+j}^0. \tag{5}$$

ii) Passo da Indução:

$$(P_L \otimes P_p)_{i+1,j} = \frac{[(i+1+j)-(r+s)p]}{(i+1-rp)} \cdot \frac{(r+s)!}{r!s!} \cdot \frac{[(i+j)-(r+s)p]!}{(i-rp)!(j-sp)!}. \tag{6}$$

Supondo que a equação (4) é verdadeira, então

$$(P_L \otimes P_p)_{i+1,j} = \frac{[(i+1+j)-(r+s)p]}{(i+1-rp)} \cdot C_{i+j}^i \equiv C_{i+j+1}^{i+1} (\text{mod } p). \tag{7}$$

□

[1] $\lfloor x \rfloor$ denota a função piso de x.

Este teorema tem consequências que derivam das propriedades do produto de Kronecker, a saber, se A e B são duas matrizes quaisquer, então

1. Associatividade: $A \otimes B \otimes C = (A \otimes B) \otimes C = A \otimes (B \otimes C)$.
2. Se A e B são matrizes triangulares então $A \otimes B$ é uma matriz triangular.
3. Se A e B são matrizes simétricas então $A \otimes B$ é uma matriz simétrica.
4. Os autovalores de $A \otimes B$ são obtidos a partir do produto dos autovalores de A pelos autovalores de B. Esta propriedade auxilia na determinação da autoestrutura da TNP.

Exemplo 2.1. A matriz da TNP de comprimento $N = 5$ possui 1 autovalor no corpo base $GF(5)$ e 4 autovalores no corpo de extensão $GF(5^2)$. Então, é possível determinar de que forma os autovalores da TNP de comprimento $N = 25$ estão distribuídos em relação a $GF(5)$ e a $GF(5^2)$. O produto de autovalores no corpo base produz um autovalor no corpo base e o produto de um autovalor no corpo base por um autovalor no corpo de extensão produz um autovalor no corpo de extensão. Neste caso, o produto de autovalores pertencentes a $GF(5^2)$ produz metade dos autovalores em $GF(5^2)$ e metade em $GF(5)$. A Tabela 2.1 mostra a distribuição de autovalores da TNP de comprimento $N = 25$.

Tabela 2.1: Distribuição de Autovalores da TNP de comprimento N=25.

$\times$	1 em $GF(5)$	4 em $GF(5^2)$
1 em $GF(5)$	1 em $GF(5)$	4 em $GF(5^2)$
4 em $GF(5^2)$	4 em $GF(5^2)$	8 em $GF(5)$
		8 em $GF(5^2)$

□

Observação. Apesar de existir a TNP para qualquer comprimento, a fatoração da matriz da TNP por meio de um produto de Kronecker só existe nas condições de Teorema 2.1.

A Proposição 2.1 permite identificar quais as potências de um elemento primitivo do corpo de extensão que produzem elementos no corpo base.

Proposição 2.1. *Se* $\beta = \alpha^{\left(\frac{p^m-1}{p-1}\right)}$, *em que* α *é um elemento primitivo do corpo de extensão* $GF(p^m)$, *então,* $\beta \in GF(p)$. *Ademais, os elementos* β^k, *em que* $k = 1, 2, \cdots, p-1$ *pertencem a* $GF(p)$.

Prova. Observe que

$$\beta^{(p-1)} = \alpha^{p^m-1} = 1,$$

e, portanto, $\beta \in GF(p)$. Como as potências de um elemento no corpo base estão no corpo base, e os elementos do corpo base possuem ordens que são divisores de $(p-1)$, segue-se que $\beta^k \in GF(p), k = 1, 2, \cdots, p-1$. □

Proposição 2.2. *Se* $(\pi(x))$ *é o polinômio gerador de* $GF(p^m)$, *então, pelas Relações de Girard pode-se identificar qual o valor da primeira potência do elemento primitivo que se encontra no corpo base, a saber*

$$\beta = \alpha^{\left(\frac{p^m-1}{p-1}\right)} = (-1)^m \pi(0). \tag{8}$$

Prova. Seja $\pi(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ o polinômio gerador de $GF(p^m)$, em que $a_m = 1$. Então se α e os seus conjugados são as raízes de $\pi(x)$, pelas relações de Girard tem-se

$$\alpha\alpha^p \cdots \alpha^{p^{m-1}} = (-1)^m \frac{a_0}{a_n} = (-1)^m \pi(0),$$
$$\alpha^{1+p+p^2+\cdots+p^{m-1}} = \alpha^{\left(\frac{p^m-1}{p-1}\right)} = (-1)^m \pi(0)$$

e resultado segue.

□

3 Os Autovalores Distintos da Matriz P_{p^r}

Nesta seção os autovalores distintos da matriz de transformação da TNP de ordem p^r são encontrados. As operações realizadas a seguir são feitas módulo p.

Proposição 3.1. *A matriz de transformação da TNP sobre $GF(p)$, em que p é um primo ímpar, cuja ordem é $N = p^r$ satisfaz $P_N^3 = I_N$, em que I_N é a matriz identidade de ordem N.*

Prova. A matriz de transformação da TNP cujo comprimento é $N = p^r$ satisfaz

$$P_N^2 = LP_N L, \tag{9}$$

em que

$$L = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Uma vez que $L^2 = I_N$, então $P_N^4 = LP_N LLP_N L = LP_N^2 L$. Mas

$$LP_N^2 L = LLP_N LL = P_N$$

e assim

$$P_N^4 = P_N \Rightarrow P_N^3 = I_N.$$

□

Proposição 3.2. *Os autovalores associados à matriz de transformação da TNP de ordem $N = p^r$, sobre $GF(p)$, em que p é um primo ímpar, satisfazem $\lambda^3 = 1$.*

Prova. Se v é uma autosequência da TNP com autovalor associado λ, então $P_N v = \lambda v$.
Da Proposição 3.1 pode-se escrever $P_N^3 v = \lambda^3 v = v$ e o resultado segue. □

Uma decorrência da Proposição 3.2 é que todos os autovalores da matriz de transformação da TNP de ordem p^r estão no corpo base $GF(p)$ se, e somente se, $3|(p-1)$. O exemplo a seguir ilustra de que forma estes resultados podem ser usados para encontrar os autovalores da TNP.

DOI: 10.5540/03.2018.006.01.0404

Exemplo 3.1. Considere a TNP de comprimento $N = 25$ sobre GF(5). Note que como $3 \nmid (p-1)$, então, o único autovalor sobre GF(5) é $\lambda = 1$. Os autovalores sobre $GF(5^2)$ são α^8 e α^{16}, em que α é um elemento primitivo do corpo. Esses autovalores (1, α^8 e α^{16}) possuem multiplicidades 9, 8 e 8, respectivamente.

Sobre $GF(7)$, a matriz de transformação da TNP de comprimento $N = 7^2$ possui todos os seus autovalores em $GF(7)$. Esses autovalores $\{1, 2$ e $4\}$ possuem multiplicidades 17, 16 e 16, respectivamente.

3.1 Uma forma alternativa da matriz de transformação inversa da TNP

Novas relações na matriz de transformação da TNP foram obtidas, as quais permitem uma implementação mais simples da TNP inversa proposta em [11]. Este resultado tem aplicação no cálculo desta inversa (Eq. (2)).

Proposição 3.3. *(Transformada de Pascal Inversa para $N = p^r$) A matriz de transformação da TNP inversa de comprimento $N = p^r$ é a matriz de elementos*

$$\left[P_N^{-1}\right]_{i,j} = \sum_{k=0}^{p^r-1} C_{i+k}^{i} C_{j+k}^{j} \equiv C_{2(p^r-1)-(i+j)}^{(p^r-1)-i}. \tag{10}$$

Prova. Uma consequência imediata da Proposição 3.1 é que $P_N^{-1} = P_N^2$. A partir da Definição 1.1, observa-se que os elementos da matriz P_N^2 são dados por

$$[P_N^2]_{i,j} = \sum_{k=0}^{p^r-1} C_{i+k}^{i} C_{j+k}^{j}. \tag{11}$$

A ação da matriz L na Equação (9) é mapear a posição (i, j) da matriz $[P_N]$ na posição $(p^r - 1 - i, p^r - 1 - j)$ da matriz P_N^2; assim, o resultado segue. □

A Proposição 3.3 permite reescrever a expressão da TNP inversa, Equação (2), para o caso em que $N = p^r$, na forma

$$v_i = \sum_{k=0}^{N-1} C_{2(p-1)-(i+k)}^{p-1-i} V_k. \tag{12}$$

4 Conclusões

Neste trabalho novas relações na matriz de transformação da TNP são apresentadas, com aplicações na transformada numérica de Pascal (TNP). Mostra-se que, para ordens que são múltiplas da característica do corpo, é possível decompor a matriz de Pascal modular como o produto de Kronecker de matrizes de Pascal de ordens iguais aos fatores envolvidos nesta fatoração. Como consequência direta das propriedades do produto de Kronecker, segue-se que os autovalores da matriz de Pascal original podem ser encontrados a partir dos autovalores das matrizes envolvidas na fatoração. Uma nova expressão para a TNP inversa de comprimento $N = p^r$ foi apresentada. Aplicações da TNP nas áreas de sistemas de comunicação multiusuário, codificação de canal e criptografia estão sendo investigadas.

Referências

[1] R. Bacher, R. Chapman, Symmetric Pascal matrices modulo p, *European J. Combinatorics* 25: 459–473, 2004. http://dx.doi.org/10.1016/j.ejc.2003.06.001

[2] 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*, vol.31, 1205–1216, 2010. http://dx.doi.org/10.1016/j.ejc.2009.10.009

[3] R. E. Blahut, *Fast Algorithms for Signal Processing*, 2nd Edition, Cambridge University Press, 2010.

[4] 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

[5] R. M. Campello de Souza and H. M. de Oliveira, Hartley number-theoretic transforms, *IEEE International Symposium on Information Theory*, ISIT, Washington DC, 2001. http://dx.doi.org/2001.10.1109/ISIT.2001.936073

[6] 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* 24:587–597, 2009. http://dx.doi.org/10.1016/j.image.2009.04.003

[7] 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*, 235–241, 1999. https://arxiv.org/abs/1505.04140

[8] H. M. de Oliveira, J. Miranda, R. M. Campello de Souza, Spread spectrum based on finite field Fourier transforms, ICSECIT, *International Conference on Systems Engineering, Communications and Information Technologies* 2001. http://arxiv.org/abs/1503.08109

[9] H. M. de Oliveira, R. M. Campello de Souza, A. N. Kauffman, Orthogonal multilevel spreading sequence design, *Coding, Communications and Broadcasting*, 291–303, 2000. http://arxiv.org/abs/1502.05881

[10] A. Edelman and G. Strang, Pascal matrices, *American Mathematical Monthly*, Mar., p. 189, 2004. http://dx.doi.org/10.2307/4145127

[11] A. J. A. Paschoal, R. M. Campello de Souza, H. M. de Oliveira, A transformada numérica de Pascal, *XXXIII Simpósio Brasileiro de Telecomunicações* - SBrT 2015, pp. 59–62, setembro 2015. http://www2.ee.ufpe.br/codec/Pascal.pdf

[12] A. J. A. Paschoal, R. M. Campello de Souza, Algoritmos rápidos para a transformada numérica de Pascal, *Submetido ao Congresso Nacional de Matemática Aplicada e Computacional - CNMAC 2017.*

[13] J.M. Pollard, The fast Fourier transform in a finite field, *Mathematics of Computation*, vol 25, 114, April 1971.

