Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, v. 6, n. 1, 2018.

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

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Algoritmos Rápidos para o Cálculo da Transformada Numérica de Pascal

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

Resumo. Recentemente, introduziu-se a transformada numérica de Pascal (TNP). Este artigo propõe algoritmos rápidos para computar a TNP de comprimentos $N = kp$ e $N = p^r$.

Palavras-chave. Transformada numérica de Pascal, triângulo de Pascal modular, algoritmos rápidos, produto de Kronecker.

1 Introdução

O desenvolvimento de algoritmos rápidos para o cálculo de transformadas discretas é bastante comum nas áreas de processamento de sinais, processamento de imagens, entre outras. Tais algoritmos, em geral, exploram aspectos de simetria existentes na matriz de transformação. Recentemente, uma nova transformada definida sobre corpos finitos, a transformada numérica de Pascal (TNP), foi introduzida [7]. A TNP se baseia no triângulo de Pascal modular e apresenta propriedades que podem ser usadas na concepção de algoritmos para sua computação.

Neste trabalho são propostos algoritmos rápidos para computar a TNP. Na Seção 2, a definição da TNP é reapresentada. Nas Seções 3, 4 e 5 são desenvolvidos algoritmos rápidos para a computação da TNP de comprimentos $N = p$, $N = kp$ e $N = p^r$, respectivamente. Na Seção 6 são apresentadas as conclusões do trabalho.

2 Preliminares

Existem, pelo menos, 12 definições para a matriz de Pascal, todas baseadas no triângulo de Pascal [3]. Neste trabalho, foi adotada a definição a seguir, que emprega aritmética sobre o corpo finito $GF(p)$. Até onde os autores têem conhecimento, esta é a única transformada definida sobre corpos finitos cujo comprimento independe da característica do corpo.

[1]arquimedes.paschoal@caruaru.ifpe.edu.br
[2]ricardo@ufpe.br

DOI: 10.5540/03.2018.006.01.0310

Definição 2.1. A Transformada numérica de Pascal (TNP) da sequência $v = (v_0, ..., v_{N-1})^T$, $v_i \in GF(p)$, é a sequência $V = (V_0, V_1, ..., V_{N-1})^T, V_k \in GF(p)$, em que

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

A complexidade multiplicativa do cálculo da TNP de comprimento N, é $M(N) = N^2$. Pode-se mostrar [7] que, para $N = p$, a matriz de transformação da TNP é uma matriz triangular superior. Neste caso, a complexidade multiplicativa direta, isto é, aquela decorrente da Definição 2.1, incluindo-se as multiplicações triviais, é

$$M(N) = \frac{p}{2}(p+1). \tag{2}$$

É possível reduzir esta complexidade multiplicativa observando certas simetrias decorrentes da estrutura do triângulo de Pascal. Assim, vamos considerar inicialmente um exemplo onde tais simetrias possam ser observadas e exploradas.

Exemplo 2.1. Considere a TNP de comprimento $N = 7$ da sequência $v = (v_0, v_1, \cdots, v_6)^T$, $v_i \in GF(7)$, $V = (V_0, V_1, \cdots, V_6)^T, V_k \in GF(7)$, em que

$$V_k = \sum_{i=0}^{6} C_{i+k}^{i} v_i (mod \ \ 7).$$

Em formato matricial, tem-se $V = P_7 v$,

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \\ V_6 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 3 & 6 & 3 & 1 & 0 & 0 \\ 1 & 4 & 3 & 6 & 0 & 0 & 0 \\ 1 & 5 & 1 & 0 & 0 & 0 & 0 \\ 1 & 6 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{bmatrix}.$$

Note que:
i) Os coeficientes não nulos da segunda linha da matriz P_7, a saber, 1, 2, 3, 4, 5 e 6 são congruentes, módulo 7, aos inteiros 1, 2, 3, -3, -2 e -1, respectivamente. Assim, V_1 pode ser escrita como $V_1 = (v_0 - v_5) + 2(v_1 - v_4) + 3(v_2 - v_3)$, reduzindo-se de seis para três o número de multiplicações para sua computação. O mesmo raciocínio pode ser aplicado às outras linhas pares.
ii) Os coeficientes não nulos das linhas ímpares são simétricos. Explorando-se esta simetria, V_2, por exemplo, pode ser computada como $V_2 = (v_0 + v_4) + 3(v_1 + v_3) + 6v_2$, reduzindo-se o número de multiplicações de cinco para três. O mesmo raciocínio pode ser empregado em relação às outras linhas ímpares.

DOI: 10.5540/03.2018.006.01.0310

3 A TNP de comprimento primo

As simetrias do triângulo de Pascal modular, observadas no Exemplo 2.1, nos conduzem ao resultado mostrado a seguir.

Proposição 3.1. *A TNP de comprimento $N = p$, em que p é um número primo ímpar, pode ser computada por meio de um algoritmo de complexidade multiplicativa dada por*

$$M(N) = M(p) = \frac{(p^2 - 4p + 3)}{4}. \tag{3}$$

Prova. Se $M_{par}(p)$ e $M_{impar}(p)$ denotam, respectivamente, as complexidades multiplicativas associadas às linhas pares e às linhas ímpares no cálculo da TNP de comprimento p, então pode-se escrever $M(p) = M_{par}(p) + M_{impar}(p)$, em que

$$M_{par}(p) = 1 + 2 + \cdots + (\frac{p-1}{2}) = (\frac{p^2-1}{8}),$$
$$M_{impar}(p) = 1 + 2 + \cdots + (\frac{p-1}{2}) + p = (\frac{p^2-1}{8}) + p.$$

Uma vez que a primeira linha somente requer multiplicações triviais, e cada uma das $(p-1)$ linhas subsequentes possui pelo menos uma multiplicação trivial, resulta

$$M(p) = M_{par}(p) + M_{impar}(p) - p - (p-1) = \frac{(p^2 - 4p + 3)}{4}.$$

□

Em verdade, o valor para $M(p)$ indicado na Eq.(3) é uma cota superior para a complexidade multiplicativa, uma vez que existe a possibilidade de se ter outras multiplicações triviais na matriz de transformação da TNP. Para se obter uma expressão da complexidade multiplicativa que não inclua as multiplicações triviais, é necessário contabilizar quantos termos são congruentes a ± 1 módulo p na matriz P_N Assim, por exemplo, para o caso $N = 11$, a Eq.(3) nos fornece 20 multiplicações. Todavia, uma análise da matriz P_{11} nos revela que o número de multiplicações não triviais é 17.

A Tabela 3.1 mostra as complexidades multiplicativas para o cálculo da TNP, cujo comprimento N é um número primo ímpar, considerando-se os métodos: i) Método Direto (Eq.(2)); ii) Método rápido baseado na Proposição 3.1 (Eq.(3)).

Tabela 3.1: Comparativo da complexidade multiplicativa da TNP de comprimento $N = p$, $p > 2$ sobre $GF(p)$, de acordo com as Equações (2) e (3).

	Comprimento						
Método	7	11	13	17	19	23	29
Eq. (2)	28	66	91	153	190	276	435
Eq. (3)	6	20	30	56	72	110	182

4 A TNP de comprimento $N=kp$

Quando a matriz de transformação da TNP, definida sobre $GF(p)$, possui uma ordem do tipo $N = kp$, $k > 1$, então é possível decompor esta matriz como o produto de Kronecker de duas matrizes, isto é, $P_N = P_k \otimes P_p$ [8]

Exemplo 4.1. Considere a matriz da TNP sobre $GF(5)$ de comprimento $N = 15$,

$$P_{15} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 \\ 1 & 3 & 1 & 0 & 0 & 1 & 3 & 1 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 4 & 0 & 2 & 4 & 1 & 3 & 0 & 3 & 1 & 4 & 2 & 0 \\ 1 & 3 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 3 & 4 & 3 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 0 & 3 & 1 & 4 & 2 & 0 & 1 & 2 & 3 & 4 & 0 \\ 1 & 3 & 1 & 0 & 0 & 3 & 4 & 3 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note que P_{15} pode ser escrita como

$$P_{15} = \begin{bmatrix} P_5 & P_5 & P_5 \\ P_5 & 2P_5 & 3P_5 \\ P_5 & 3P_5 & P_5 \end{bmatrix}$$

e a complexidade multiplicativa para a TNP de comprimento $N = 15$, sobre $GF(5)$, pode ser expressa em função da complexidade da TNP para $N = 5$.
Assim,

$$V = \begin{bmatrix} \hat{V_0} \\ \hat{V_1} \\ \hat{V_2} \end{bmatrix} = \begin{bmatrix} P_5 & P_5 & P_5 \\ P_5 & 2P_5 & 3P_5 \\ P_5 & 3P_5 & P_5 \end{bmatrix} \begin{bmatrix} \hat{v_0} \\ \hat{v_1} \\ \hat{v_2} \end{bmatrix},$$

em que

$$\hat{V_0} = (V_0, V_1, \cdots, V_4), \quad \hat{V_1} = (V_5, V_6, \cdots, V_9), \quad \hat{V_2} = (V_{10}, V_{11}, \cdots, V_{14}),$$
$$\hat{v_0} = (v_0, v_1, \cdots, v_4), \quad \hat{v_1} = (v_5, v_6, \cdots, v_9), \quad \hat{v_2} = (v_{10}, v_{11}, \cdots, v_{14}).$$

No cálculo de $\hat{V_0}$ computamos e armazenamos as parcelas ($P_5\hat{v_0}$, $P_5\hat{v_1}$ e $P_5\hat{v_2}$), de modo que, na computação das outras componentes ($\hat{V_1}$ e $\hat{V_2}$), não é necessário efetuar nenhuma outra multiplicação por P_5, apenas p multiplicações são realizadas para cada termo binomial.

□

Teorema 4.1. *A TNP de comprimento $N = kp$, em que p é um número primo ímpar, pode ser computada por meio de um algoritmo de complexidade multiplicativa dada por*

$$M(N) = M(kp) = \frac{(p^2 - 4p + 3)}{4}k + p(k-1)^2. \tag{4}$$

Prova. Note que quando $p = 2$ ou $p = 3$ só existem multiplicações triviais. A prova deste Teorema pode ser feita considerando a matriz de transformação da TNP na forma $P_N = P_k \otimes P_p$, ou seja

$$V = \begin{bmatrix} \widehat{V}_0 \\ \widehat{V}_1 \\ \vdots \\ \widehat{V}_{k-1} \end{bmatrix} = \begin{bmatrix} P_p & P_p & \cdots & P_p \\ P_p & C_2^1 P_p & \cdots & C_k^1 P_p \\ \vdots & \vdots & \ddots & \vdots \\ P_p & C_k^{k-1} P_p & \cdots & C_{2k-2}^{k-1} P_p \end{bmatrix} \begin{bmatrix} \widehat{v}_0 \\ \widehat{v}_1 \\ \vdots \\ \widehat{v}_{k-1} \end{bmatrix}.$$

Note que o vetor coluna v possui k componentes, em que cada uma possui dimensão p. A idéia aqui é armazenar todos os produtos resultantes da multiplicação da primeira linha da matriz P_N pelo vetor v, evitando-se multiplicações adicionais no cálculo das outras componentes de V. Esta multiplicação requer $M(p)$ multiplicações, conforme Eq. (3). Ademais, note a existência de uma submatriz $(k-1) \times (k-1)$ em que as únicas multiplicações necessárias, usando-se esta abordagem, são pelos termos binomiais e envolve p multiplicações cada. O resultado segue.

□

A Tabela 4.1 mostra a complexidade multiplicativa para o cálculo da TNP de comprimento $N = kp$, em que p é um número primo maior do que 3. Para efeito de comparação é mostrada a complexidade multiplicativa direta. Para o caso em que k é uma potência de p, existe um algoritmo mais eficiente em termos de complexidade multiplicativa, conforme descrito na seção 5.

Tabela 4.1: Complexidade multiplicativa da TNP de comprimento $N = 5k, k > 1$.

N	10	15	20	30	35
M(N)	9	26	53	137	194
N^2	100	225	400	900	1225

5 A TNP de comprimento $N = p^r$

Quando o comprimento da transformada é do tipo $N = p^r$, então é possível usar o fato de que a matriz de transformação pode ser decomposta como o produto de Kronecker $P_N = P_p \otimes P_{p^{r-1}}$.

Teorema 5.1. *A TNP de comprimento $N = p^r$, em que p é um número primo ímpar, pode ser computada por meio de um algoritmo de complexidade multiplicativa dada por*

$$M(p^r) = p^{r-1}M(p) + (r-1)p^{r-1}\frac{(p-1)(p-2)}{2}, \tag{5}$$

em que $M(p)$ é dado pela Eq. (3).

Prova. A prova é feita por indução em r.

Passo Base: $r = 1$ em (5), resulta $M(p) = M(p)$.
Passo da indução: Assuma que (5) é verdadeira e faça $N = p^{r+1}$. Expressando $P_{p^{r+1}}$ na forma $P_{p^{r+1}} = P_p \otimes P_{p^r}$, tem-se

$$V = \begin{bmatrix} \hat{V}_0 \\ \hat{V}_1 \\ \hat{V}_2 \\ \vdots \\ \hat{V}_{p-1} \end{bmatrix} = \begin{bmatrix} P_{p^r} & P_{p^r} & \cdots & P_{p^r} & P_{p^r} \\ P_{p^r} & 2P_{p^r} & \cdots & (p-1)P_{p^r} & 0 \\ P_{p^r} & 3P_{p^r} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ P_{p^r} & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} \hat{v}_0 \\ \hat{v}_1 \\ \hat{v}_2 \\ \vdots \\ \hat{v}_{p-1} \end{bmatrix},$$

em que os vetores $\hat{V}_k$ e $\hat{v}_i$ possuem p^r componentes, $i, k = 0, 1 \cdots, p-1$. Observe que

$$\hat{V}_0 = P_{p^r}\hat{v}_0 + P_{p^r}\hat{v}_1 + \cdots + P_{p^r}\hat{v}_{p-1},$$

em que cada uma das p parcelas contribui com $M(p^r)$ multiplicações, resultando em uma quantidade de multiplicações igual a $pM(p^r)$. As linhas restantes só contêm multiplicações por coeficientes binomiais. Assim, devido à estrutura triangular superior desta matriz, a quantidade de coeficientes binomiais é dada por

$$1 + 2 + \cdots + (p-2) = \frac{(p-1)(p-2)}{2},$$

com p^r multiplicações para cada componennte. Assim, resulta

$$\begin{aligned} M(p^{r+1}) &= pM(p^r) + p^r \frac{(p-1)(p-2)}{2} \\ &= p^r M(p) + (r-1)p^r \frac{(p-1)(p-2)}{2} + p^r \frac{(p-1)(p-2)}{2} \\ &= p^r M(p) + rp^r \frac{(p-1)(p-2)}{2} \end{aligned}$$

e o resultado segue. □

A Tabela 5.1 mostra a complexidade multiplicativas para o cálculo da TNP de comprimento $N = p^r$, em que p é um primo maior do que 3. Para efeito de comparação é mostrada a complexidade multiplicativa direta.

Tabela 5.1: Complexidade multiplicativa da TNP de comprimento $N = 5^r, r > 1$.

N	25	125	625	3.125	15.625
M(N)	40	350	2.500	16.250	100.000
$5^r(\frac{5^r+1}{2})$	325	7.875	195.625	4.884.375	122.078.125

6 Conclusões

Neste trabalho são apresentados algoritmos rápidos para a computação da transformada numérica de Pascal sobre $GF(p)$. O fato da TNP empregar uma matriz de Pascal modular, trazendo consigo todo um conjunto de propriedades e de simetrias, produz um cenário promissor para a definição de transformadas numéricas de baixa complexidade multiplicativa. Baseado no fato de que a matriz da TNP é triangular superior, quando sua ordem N é um número primo p, foram propostos algoritmos rápidos para a computação de transformadas de comprimentos $N = kp$ e $N = p^r$. A fatoração da matriz da TNP como um produto de Kronecker, apesar de restrita a certas ordens, contribui para a redução da complexidade multiplicativa.

Referências

[1] M. F. Aburdene and T. Goodman, The Discrete Pascal Transform and its Applications, *IEEE Signal Processing Letters*, vol. 12, 493–495, 2005. http://dx.doi.org/10.1109/LSP.2005.849498

[2] 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

[3] 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

[4] C. Cobeli and A. Zaharescu, Promenade around Pascal Triangle - Number Motives, *Bull. Math. Soc. Sci. Math. Roumanie* Tome 56.104, 73–98, 2013. http://www.jstor.org/stable/43679285

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

[6] S. Gudvangen, and H. Buskerud. Practical applications of number theoretic transforms. *Norsk symposium i signalbehandling, NORSIG-99*, At Asker, Norway 1999.

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

[8] A. J. A. Paschoal, R. M. Campello de Souza, H. M. de Oliveira, Novas Relações no Triangulo de Pascal Modular, *Submetido ao Congresso Nacional de Matemática Aplicada e Computacional - CNMAC 2017* - CNMAC 2017. http://www2.ee.ufpe.br/codec/Pascal.pdf

