

EDUCAÇÃO MATEMÁTICA E SUAS TECNOLOGIAS 2

Felipe Antonio Machado Fagundes Gonçalves
(Organizador)

 **Atena**
Editora
Ano 2019

Felipe Antonio Machado Fagundes Gonçalves
(Organizador)

Educação Matemática e suas Tecnologias 2

Atena Editora
2019

2019 by Atena Editora
Copyright © Atena Editora
Copyright do Texto © 2019 Os Autores
Copyright da Edição © 2019 Atena Editora
Editora Executiva: Prof^a Dr^a Antonella Carvalho de Oliveira
Diagramação: Natália Sandrini
Edição de Arte: Lorena Prestes
Revisão: Os Autores

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

Conselho Editorial

Ciências Humanas e Sociais Aplicadas

Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa
Prof^a Dr^a Cristina Gaio – Universidade de Lisboa
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná
Prof^a Dr^a Ivone Goulart Lopes – Istituto Internazionale delle Figlie de Maria Ausiliatrice
Prof^a Dr^a Juliane Sant’Ana Bento – Universidade Federal do Rio Grande do Sul
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense
Prof^a Dr^a Lina Maria Gonçalves – Universidade Federal do Tocantins
Prof^a Dr^a Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof^a Dr^a Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará
Prof^a Dr^a Vanessa Bordin Viera – Universidade Federal de Campina Grande
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

Ciências Agrárias e Multidisciplinar

Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul
Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano
Prof^a Dr^a Daiane Garabeli Trojan – Universidade Norte do Paraná
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul
Prof^a Dr^a Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

Ciências Biológicas e da Saúde

Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria
Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás
Prof.^a Dr.^a Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará
Prof.^a Dr.^a Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof.^a Dr.^a Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão
Prof.^a Dr.^a Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa
Prof.^a Dr.^a Vanessa Bordin Viera – Universidade Federal de Campina Grande

Ciências Exatas e da Terra e Engenharias

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Prof.^a Dr.^a Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

Conselho Técnico Científico

Prof. Msc. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo
Prof.^a Dr.^a Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico
Prof. Msc. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro
Prof.^a Msc. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia
Prof. Msc. Leonardo Tullio – Universidade Estadual de Ponta Grossa
Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista
Prof. Msc. André Flávio Gonçalves Silva – Universidade Federal do Maranhão
Prof.^a Msc. Renata Luciane Polsaque Young Blood – UniSecal
Prof. Msc. Daniel da Silva Miranda – Universidade Federal do Pará

Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)	
E24	Educação matemática e suas tecnologias 2 [recurso eletrônico] / Organizador Felipe Antonio Machado Fagundes Gonçalves. – Ponta Grossa (PR): Atena Editora, 2019. – (Educação Matemática e suas Tecnologias; v. 2) Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-85-7247-348-4 DOI 10.22533/at.ed.484192405 1. Matemática – Estudo e ensino – Inovações tecnológicas. 2. Tecnologia educacional. I. Gonçalves, Felipe Antonio Machado Fagundes. II. Série. CDD 510.7
Elaborado por Maurício Amormino Júnior – CRB6/2422	

Atena Editora
Ponta Grossa – Paraná - Brasil
www.atenaeditora.com.br
contato@atenaeditora.com.br

APRESENTAÇÃO

A obra “Educação Matemática e suas tecnologias” é composta por quatro volumes, que vêm contribuir de maneira muito significativa para o Ensino da Matemática, nos mais variados níveis de Ensino. Sendo assim uma referência de grande relevância para a área da Educação Matemática. Permeados de tecnologia, os artigos que compõem estes volumes, apontam para o enriquecimento da Matemática como um todo, pois atinge de maneira muito eficaz, estudantes da área e professores que buscam conhecimento e aperfeiçoamento. Pois, no decorrer dos capítulos podemos observar a matemática aplicada a diversas situações, servindo com exemplo de práticas muito bem sucedidas para docentes da área. A relevância da disciplina de Matemática no Ensino Básico e Superior é inquestionável, pois oferece a todo cidadão a capacidade de analisar, interpretar e inferir na sua comunidade, utilizando-se da Matemática como ferramenta para a resolução de problemas do seu cotidiano. Sem dúvidas, professores e pesquisadores da Educação Matemática, encontrarão aqui uma gama de trabalhos concebidos no espaço escolar, vislumbrando possibilidades de ensino e aprendizagem para diversos conteúdos matemáticos. Que estes quatro volumes possam despertar no leitor a busca pelo conhecimento Matemático. E aos professores e pesquisadores da Educação Matemática, desejo que esta obra possa fomentar a busca por ações práticas para o Ensino e Aprendizagem de Matemática.

Felipe Antonio Machado Fagundes Gonçalves

SUMÁRIO

CAPÍTULO 1	1
O ALGORITMO ESPECTRAL COMO ALTERNATIVA AO ALGORITMO K-MEANS EM CONJUNTO DE DADOS ARTIFICIAIS	
Luciano Garim Garcia Leonardo Ramos Emmendorfer	
DOI 10.22533/at.ed.4841924051	
CAPÍTULO 2	16
NOVAS RELAÇÕES NA MATRIZ DE TRANSFORMAÇÃO DA TRANSFORMADA NUMÉRICA DE PASCAL	
Arquimedes José De Araújo Paschoal Ricardo Menezes Campello De Souza Hélio Magalhães De Oliveira	
DOI 10.22533/at.ed.4841924052	
CAPÍTULO 3	24
ALGORITMOS RÁPIDOS PARA O CÁLCULO DA TRANSFORMADA NUMÉRICA DE PASCAL	
Arquimedes José De Araújo Paschoal Ricardo Menezes Campello De Souza	
DOI 10.22533/at.ed.4841924053	
CAPÍTULO 4	32
ANÁLISE DE CÁLCULO DIFERENCIAL USANDO O SOFTWARE GEOGEBRA	
Amanda Barretos Lima Garuth Brenda Anselmo Mendes Isabela Geraldo Reghin Rosângela Teixeira Guedes	
DOI 10.22533/at.ed.4841924054	
CAPÍTULO 5	46
DEFLEXÃO EM VIGAS DE CONCRETO ARMADO SOLUÇÃO ANALÍTICA E NUMÉRICA VIA MÉTODO DAS DIFERENÇAS FINITAS	
Mariana Coelho Portilho Bernardi Adilandri Mércio Lobeiro Jeferson Rafael Bueno Thiago José Sepulveda da Silva	
DOI 10.22533/at.ed.4841924055	
CAPÍTULO 6	57
MODELO MATEMÁTICO PARA AUXILIAR O PLANEJAMENTO DA MANUTENÇÃO PREVENTIVA DE MOTORES ELÉTRICOS	
Thalita Monteiro Obal Jonatas Santana Obal	
DOI 10.22533/at.ed.4841924056	

CAPÍTULO 7	64
PRINCÍPIO DA SUPERPOSIÇÃO E SOLUÇÃO NUMÉRICA DO PROBLEMA DE FLUXO EM AQUÍFERO CONFINADO	
João Paulo Martins dos Santos Alessandro Firmiano de Jesus Edson Wendland	
DOI 10.22533/at.ed.4841924057	
CAPÍTULO 8	83
RESONANT ORBITAL DYNAMICS OF CBERS SATELLITES	
Jarbas Cordeiro Sampaio Rodolpho Vilhena de Moraes Sandro da Silva Fernandes	
DOI 10.22533/at.ed.4841924058	
CAPÍTULO 9	91
TESTES ADAPTATIVOS ENVOLVENDO O CONTEÚDO DE DERIVADAS: UM ESTUDO DE CASO COM ALUNOS DE ENGENHARIA CIVIL	
Patrícia Liane Grudzinski da Silva Claudia Lisete Oliveira Groenwald	
DOI 10.22533/at.ed.4841924059	
CAPÍTULO 10	104
LOCALIZAÇÃO DE FALTAS EM LINHAS DE TRANSMISSÃO POR ANÁLISE DE SINAIS TRANSITÓRIOS DE TENSÃO	
Danilo Pinto Moreira de Souza Eliane da Silva Christo Aryfrance Rocha Almeida	
DOI 10.22533/at.ed.48419240510	
CAPÍTULO 11	116
MODELAGEM DA PROPAGAÇÃO DE FUMAGINA CAUSADA POR MOSCA-BRANCA EM CULTURAS AGRÍCOLA	
Gustavo Henrique Petrolí Norberto Anibal Maidana	
DOI 10.22533/at.ed.48419240511	
CAPÍTULO 12	133
LOS SUBNIVELES DE DESARROLLO DEL ESQUEMA DE DERIVADA: UN ESTUDIO EXPLORATORIO EN EL NIVEL UNIVERSITARIO	
Claudio Fuentealba Edelmira Badillo Gloria Sánchez-Matamoros Andrea Cárcamo	
DOI 10.22533/at.ed.48419240512	
CAPÍTULO 13	143
OTIMIZAÇÃO BASEADA EM CONFIABILIDADE PARA A MINIMIZAÇÃO DE FUNÇÕES MATEMÁTICAS	
Márcio Aurélio da Silva Fran Sérgio Lobato Aldemir Ap Cavalini Jr Valder Steffen Jr	
DOI 10.22533/at.ed.48419240513	

CAPÍTULO 14	156
SEQUÊNCIAS: INTERVALARES E FUZZY	
Gino Gustavo Maqui Huamán	
Ulcilea Alves Severino Leal	
Geraldo Nunes Silva	
DOI 10.22533/at.ed.48419240514	
CAPÍTULO 15	164
VALIDAÇÃO DO MÉTODO DOS ELEMENTOS DISCRETOS PARA O ESCOAMENTO DE GRÃOS DE SOJA	
Rodolfo França de Lima	
Vanessa Faoro	
Manuel Osório Binelo	
Dirceu Lima dos Santos	
Adriano Pilla Zeilmann	
DOI 10.22533/at.ed.48419240515	
CAPÍTULO 16	181
TAREAS DE GENERALIZACIÓN POR INDUCCIÓN PARA FORMAR EL CONCEPTO DE POTENCIA	
Landy Sosa Moguel	
Guadalupe Cabañas-Sánchez	
Eddie Aparicio Landa	
DOI 10.22533/at.ed.48419240516	
CAPÍTULO 17	192
SINCRONISMO EM UM NOVO MODELO METAPOPOPULACIONAL COM TAXA DE MIGRAÇÃO INDEPENDENTE DA DENSIDADE	
Francisco Helmuth Soares Dias	
Jacques Aveline Loureiro da Silva	
DOI 10.22533/at.ed.48419240517	
CAPÍTULO 18	199
SIMULAÇÃO 3D DO FLUXO DE AR DE UM SISTEMA REAL DE ARMAZENAGEM DE GRÃOS	
Vanessa Faoro	
Rodolfo França de Lima	
Aline Tampke Dombrowski	
Manuel Osório Binelo	
DOI 10.22533/at.ed.48419240518	
CAPÍTULO 19	207
CONTROLE ÓTIMO DO FLUXO DE ÁGUA EM UMA FÔRMA DE GELO	
Xie Jiayu	
João Luis Gonçalves	
DOI 10.22533/at.ed.48419240519	
CAPÍTULO 20	213
CÓDIGOS CÍCLICOS DEFINIDOS POR ANULAMENTO	
Conrado Jensen Teixeira	
Osnel Broche Cristo	
DOI 10.22533/at.ed.48419240520	

CAPÍTULO 21	216
ANÁLISE TEÓRICO-EXPERIMENTAL DE DISPERSÃO DE UM CONTAMINANTE COM TRANSFORMAÇÕES INTEGRAIS E INFERÊNCIA BAYESIANA	
Bruno Carlos Lugão	
Diego Campos Knupp	
Pedro Paulo Gomes Watts Rodrigues	
Antônio José da Silva Neto	
DOI 10.22533/at.ed.48419240521	
CAPÍTULO 22	225
ANÁLISE WAVELET DE TACOGRAMAS TEÓRICOS E EXPERIMENTAIS	
Ronaldo Mendes Evaristo	
Kelly Cristiane Iarosz	
Silvio Luiz Thomaz de Souza	
Ricardo Luiz Viana	
Moacir Fernandes de Godoy	
Antonio Marcos Batista	
DOI 10.22533/at.ed.48419240522	
CAPÍTULO 23	235
CONSTRUÇÃO DE UM AEROMODELO DE MACARRÃO NO ENSINO DE MATEMÁTICA E FÍSICA	
Alissan Sarturato Firão	
Ernandes Rocha de Oliveira	
Zulind Luzmarina Freitas	
DOI 10.22533/at.ed.48419240523	
SOBRE O ORGANIZADOR	239

ALGORITMOS RÁPIDOS PARA O CÁLCULO DA TRANSFORMADA NUMÉRICA DE PASCAL

Arquimedes José De Araújo Paschoal

Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - Campus Caruaru – Departamento de Engenharia Mecânica Caruaru – PE

Ricardo Menezes Campello De Souza

Universidade Federal de Pernambuco – Departamento de Eletrônica e Sistemas Recife – PE

RESUMO: Este artigo propõe algoritmos rápidos para computar a Transformada Numérica de Pascal (TNP) de comprimentos n e m . As simetrias da matriz da TNP, bem como sua fatoração como um produto de Kronecker, foram usadas para se obter uma redução da complexidade multiplicativa para se implementar a transformada. Os algoritmos propostos resultaram em uma redução da complexidade entre 84% e 99,9%. Considerando o critério de complexidade multiplicativa, os melhores resultados são obtidos quando o comprimento da TNP é uma potência de um primo.

PALAVRAS –CHAVE: Transformada Numérica de Pascal, Triângulo de Pascal Modular, Algoritmos Rápidos, Produto de Kronecker.

ABSTRACT: This paper proposes fast algorithms for computing the Pascal Number Theoretic Transform (PNTT) of blocklengths

and m . The symmetries of the PNTT as well as its factorization as a Kronecker product were explored to reduce the multiplicative complexity for implementing the transform. The proposed algorithms resulted in a complexity reduction from 84% to 99.9%. Taking into account the multiplicative complexity criterion, the best results are obtained when the blocklength of the PNTT is a prime power.

KEYWORDS: Pascal Number-Theoretic Transform, Modular Pascal Triangle, Fast Algorithms, Kronecker Product.

1 | INTRODUÇÃO

Transformadas discretas desempenham um papel relevante em Engenharia e suas aplicações devem-se principalmente à existência de algoritmos rápidos para sua computação. Neste cenário, transformadas definidas sobre corpos finitos são atraentes porque não apresentam o chamado erro de arredondamento ou truncagem, uma vez que empregam aritmética módulo p . Este trabalho aborda as chamadas transformadas numéricas, isto é, transformadas definidas sobre o corpo finito $GF(p)$. Algumas áreas da Engenharia Eletrônica, tais como Processamento Digital de Sinais, Códigos Corretores de Erros e Criptografia, entre outras, têm sido beneficiadas

com o uso de tais transformadas [3, 4]. Uma questão importante para a implementação de uma dada transformada é a complexidade multiplicativa necessária para sua computação. Muitos algoritmos têm sido desenvolvidos visando reduzir esta complexidade. Estes algoritmos, implementados em Processadores Digitais de Sinais (DSP), em FPGA ou em circuitos integrados de aplicação específica (ASIC), permitem o desenvolvimento de equipamentos capazes de processar informações em tempo real.

Recentemente, uma nova transformada definida sobre corpos finitos, a Transformada Numérica de Pascal (TNP), foi introduzida [5]. A TNP se baseia no triângulo de Pascal modular e apresenta propriedades, decorrentes de sua estrutura autossimilar, que podem ser usadas na concepção de algoritmos rápidos. Neste trabalho são propostos algoritmos rápidos para computar a TNP. Na Seção 2, a definição da TNP é apresentada. Nas Seções 3, 4 e 5 são desenvolvidos algoritmos rápidos para a computação da TNP de comprimentos $N = p$, $N = k_p$ 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 [2]. Neste artigo, foi adotada a definição a seguir, que emprega aritmética sobre o corpo finito $GF(p)$.

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

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

A complexidade multiplicativa direta do cálculo da TNP de comprimento N , por meio da Definição 2.1, é $M(N) = N^2$. Pode-se mostrar [5] que, para $N = p$, a matriz da TNP é uma matriz triangular superior. Neste caso, a complexidade multiplicativa direta, incluindo-se as multiplicações triviais (multiplicações por ± 1), é

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

É possível reduzir esta complexidade multiplicativa observando certas simetrias decorrentes da estrutura do triângulo de Pascal. Assim, inicialmente considera-se um

exemplo em que tais simetrias podem ser observadas e exploradas.

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

$$V_k := \sum_{i=0}^6 c_{i+k}^i v_i \pmod{7}.$$

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

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

Note que:

- I. Os coeficientes não nulos da segunda linha da matriz P 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 às outras linhas ímpares.

3 I A TNP DE COMPRIMENTO PRIMO

As simetrias do triângulo de Pascal modular [1], observadas no Exemplo 2.1, levam 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

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

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

$$M_{par}(p) = 1 + 2 + \dots + \left(\frac{p-1}{2}\right) = \left(\frac{p^2-1}{8}\right),$$

$$M_{impar}(p) = 1 + 2 + \dots + \left(\frac{p-1}{2}\right) + p = \left(\frac{p^2-1}{8}\right) + p.$$

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

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

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 da TNP. Para se obter uma expressão que não inclua multiplicações triviais, é necessário contabilizar quantos termos são congruentes a ± 1 módulo p na matriz P_N . Assim, por exemplo, para o caso $N = 11$ tem-se, pela Eq.(3), $M(11) = 20$. Todavia, uma análise da matriz P_{11} revela que o número de multiplicações não triviais é 17. Na Tabela 3.1 são apresentadas 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)).

	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

Tabela 3.1: Comparativo da complexidade multiplicativa da TNP de comprimento p , sobre \mathbb{F}_p , de acordo com as Equações (2) e (3).

4 | A TNP DE COMPRIMENTO $N = kp$

Quando a matriz da TNP possui uma ordem do tipo $N = kp, k > 1$ então é possível decompor esta matriz como o produto de Kronecker $P_N = P_k \otimes P_p$ [6].

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 $\hat{V}_0 = (V_0, V_1, \dots, V_4)$, $\hat{V}_1 = (V_5, V_6, \dots, V_9)$, $\hat{V}_2 = (V_{10}, V_{11}, \dots, V_{14})$, $\hat{v}_0 = (v_0, v_1, \dots, v_4)$, $\hat{v}_1 = (v_5, v_6, \dots, v_9)$, $\hat{v}_2 = (v_{10}, v_{11}, \dots, v_{14})$.

No cálculo de \hat{V}_0 as parcelas $(P_5\hat{v}_0, P_5\hat{v}_1 e P_5\hat{v}_2)$ foram computadas e armazenadas, de modo que, na computação das componentes, não é necessário efetuar nenhuma outra multiplicação por, mas apenas multiplicações para cada termo binomial.

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

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

Prova. Note que quando $p = 2$ ou $p=3$ só existem multiplicações triviais. A prova

deste Teorema pode ser feita considerando-se , ou seja,

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

Note que o vetor coluna v possui k componentes, em que cada uma possui dimensão p . Armazenando-se todos os produtos resultantes da multiplicação da primeira linha da matriz P_N pelo vetor v , evitam-se multiplicações adicionais no cálculo das outras componentes de V . Cada produto requer $M(p)$ multiplicações, conforme Eq.(3). Note a existência de uma submatriz $(k-1) \times (k-1)$ em que as únicas multiplicações necessárias são pelos termos binomiais e envolve p multiplicações cada. O resultado segue.

Na Tabela 4.1 é apresentada a complexidade multiplicativa $M(N)$, dada pela Eq.(4), para o cálculo da TNP de comprimento $N = kp$. Para efeito de comparação é mostrada a complexidade multiplicativa direta, bem como a redução nesta complexidade proporcionada pelo algoritmo rápido.

N	10	15	20	30	35
M(N)	9	26	53	137	194
N^2	100	225	400	900	1225
Redução (%)	91	88,44	86,75	84,77	84,16

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

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 da TNP pode ser decomposta como $P_N = P_p \otimes P_{p^{r-1}}$

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

$$M(p^r) = p^{r-1}M(p) + (r-1)p^{r-1} \left(\frac{p^2 - 3p + 2}{2} \right), \quad (5)$$

em que $M(p)$ é dado pela Eq.(3).

Prova. A prova é feita por indução em r .

Passo Base: Fazendo-se $r = 1$, na Eq.(5), resulta em $M(p) = M(p)$

Passo da Indução: Considera-se a Eq.(5) verdadeira e faz-se $N = p^{r+1}$.

Expressando $P_{p^{r+1}}$ na forma $P_{p^{r+1}} = P_p \otimes P_{p^r}$, tem-se

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

em que os vetores \hat{V}_k e \hat{v}_i possuem p^r componentes, $i, k = 0, 1, \dots, p-1$. 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. Devido à estrutura triangular superior da matriz $P_{p^{r+1}}$, a quantidade de coeficientes binomiais é dada por

$$1 + 2 + \cdots + (p-2) = \left(\frac{p^2 - 3p + 2}{2} \right),$$

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

$$\begin{aligned} M(p^{r+1}) &= pM(p^r) + p^r \left(\frac{p^2 - 3p + 2}{2} \right) \\ &= p^r M(p) + (r-1)p^r \left(\frac{p^2 - 3p + 2}{2} \right) + p^r \left(\frac{p^2 - 3p + 2}{2} \right) \\ &= p^r M(p) + rp^r \left(\frac{p^2 - 3p + 2}{2} \right). \end{aligned}$$

e o resultado segue.

Na Tabela 5.1 é apresentada a complexidade multiplicativa $M(N)$, dada pela Eq.(5), 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, bem como a redução nesta complexidade proporcionada pelo algoritmo rápido.

N	25	125	625	3.125	15.625
M(N)	40	350	2.500	16.250	100.000
$5^r \left(\frac{5^r + 1}{2} \right)$	325	7.875	195.625	4.884.375	122.078.125
Redução (%)	87,69	95,55	98,72	99,66	99,92

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

6 | CONCLUSÕES

Neste trabalho são apresentados algoritmos rápidos para computar a Transformada Numérica de Pascal. O fato da TNP usar uma matriz de Pascal modular, trazendo consigo todo um conjunto de propriedades e de simetrias, produz um cenário promissor para a construção de algoritmos rápidos para sua computação. Tendo em vista que a matriz da TNP é triangular superior, quando sua ordem N é uma potência de um número primo p , foram propostos algoritmos rápidos para a computação de transformadas de comprimentos $N = kp$ e $N = p^r$. Os algoritmos propostos resultaram em uma redução de complexidade multiplicativa entre 84% e 99,9%. Em relação a esta complexidade, os melhores resultados são obtidos quando o comprimento da TNP é uma potência de um primo.

REFERÊNCIAS

- [1] Bacher, R.; Chapman, R. Symmetric Pascal matrices modulo , **European Journal of Combinatorics**, 25: 459-473, 2004. DOI: 10.1016/j.ejc.2003.06.001.
- [2] Birregah, B.; Dobb, P. K.; Adjallah, K. H. A systematic approach to matrix forms of the Pascal triangle: The twelve triangular matrix forms and relations, **European Journal of Combinatorics**, 31:1205-1216, 2010. DOI: 10.1016/j.ejc.2009.10.009.
- [3] Lima, J. B.; Novaes, L. F. G. Image encryption based on the fractional Fourier transform over finite fields, **European Journal of Combinatorics**, 94:521-530,2014. DOI: 10.1016/j.sigpro.2013.07.020.
- [4] Lima, P. H. E. S.; Lima, J. B.; Campello de Souza, R. M. Fractional Fourier, Hartley, cosine and sine number-theoretic transforms based on matrix functions, **Circuits, Systems and Signal Processing**, 36:2893-2916, 2017. DOI: 10.1007/s00034-016-0447-8.
- [5] Paschoal, A. J. A., Campello de Souza, R. M.; De Oliveira, H. M. A transformada numérica de Pascal, In: **XXXIII Simpósio Brasileiro de Telecomunicações – SBrT 2015**, p. 59-62, setembro 2015.
- [6] Paschoal, A. J. A.; Campello de Souza, R. M. Algoritmos rápidos para a transformada numérica de Pascal, In: **XXXVII Congresso Nacional de Matemática Aplicada e Computacional – CNMAC 2017**. Vol 6, n.1, p. 010310-1: 010310-7, DOI: 10.5540/03.2018.006.01.0310.

SOBRE O ORGANIZADOR

FELIPE ANTONIO MACHADO FAGUNDES GONÇALVES Mestre em Ensino de Ciência e Tecnologia pela Universidade Tecnológica Federal do Paraná(UTFPR) em 2018. Licenciado em Matemática pela Universidade Estadual de Ponta Grossa (UEPG), em 2015 e especialista em Metodologia para o Ensino de Matemática pela Faculdade Educacional da Lapa (FAEL) em 2018. Atua como professor no Ensino Básico e Superior. Trabalha com temáticas relacionadas ao Ensino desenvolvendo pesquisas nas áreas da Matemática, Estatística e Interdisciplinaridade.

Agência Brasileira do ISBN
ISBN 978-85-7247-348-4

