SBrT 2021 1570733927

q-Análogos em Corpos Finitos: Definição, Propriedades Algébricas e Aplicação em Geradores de Números Pseudo-Aleatórios

Carlos E. C. Souza, Ravi B. D. Figueiredo, Daniel P. B. Chaves e Cecilio Pimentel

***Resumo*— Neste trabalho é definido o q-análogo do corpo finito $\mathbb{Z}_p$, denotado por $[\mathbb{Z}_p]_q$. São derivadas várias propriedades de $[\mathbb{Z}_p]_q$ e são estabelecidas as condições necessárias para que o mapeamento entre $\mathbb{Z}_p$ e $[\mathbb{Z}_p]_q$ seja uma bijeção, definindo uma permutação. Os q-análogos em corpos finitos são empregados para construir geradores de números pseudo-aleatórios (PRNG, *pseudo-random number generator*) e suas propriedades estatísticas são analisadas. Simulações computacionais utliizando a suíte estatística NIST evidenciam que os geradores propostos geram sequências com boas propriedades estatísticas e taxa máxima de geração de bits.**

***Palavras-Chave*— q-Análogos, corpos finitos, teoria dos números, geradores de números pseudo-aleatórios.**

***Abstract*— In this work we define the q-analog of the finite field $\mathbb{Z}_p$, denoted as $[\mathbb{Z}_p]_q$. We derive several properties of $[\mathbb{Z}_p]_q$ and investigate the necessary conditions to obtain a bijection between $\mathbb{Z}_p$ and $[\mathbb{Z}_p]_q$, defining a permutation. We employ the q-analogs in finite fields to design a pseudo-random number generator (PRNG) and its statistical properties are analyzed. Computer simulations show that the proposed pseudo-random number generator generates binary sequences with good statistical properties and maximal bit rate generation.**

***Keywords*— q-Analogs, finite fields, number theory, pseudo-random number generators.**

I. Introdução

q-Análogos, também denominados q-deformações, são generalizações de objetos matemáticos tais como múmeros e funções, parametrizados em função de um parâmetro q, de forma que no limite $q \to 1$ o objeto original é recuperado [1]. Inicialmente, os q-análogos foram definidos sobre o conjunto dos números inteiros no contexto de combinatória [2]. Trabalhos recentes propõem a generalização do conceito de q-análogos para conjuntos numéricos mais gerais, como os números racionais e reais [3], [4].

Em outro contexto, alguns trabalhos vêm considerando a introdução da q-deformação em mapas caóticos reais, com o objetivo de investigar o efeito da q-deformação na dinâmica caótica [5], [6], [7], [8]. A introdução da q-deformação, portanto, incorpora um grau de liberdade adicional na dinâmica complexa gerada por mapas caóticos, sendo as q-deformações potenciais generalizações para agregar uma camada adicional de complexidade à dinâmica caótica. Além disso, o conceito de caos discreto foi desenvolvido em [9] e mapas caóticos sobre conjuntos discretos vêm sendo aplicados com sucesso no projeto de geradores de números pseudo-aleatórios (PRNG, *pseudo-random number generator*) [10]. Estes mapas têm a vantagem de utilizar operações de ponto fixo, diminuindo o efeito de erros sistemáticos decorrentes de processos de quantização e arredondamentos característicos de sistemas definidos sobre os números reais [11].

Para que a camada adicional de complexidade incorporada pela deformação dos q-análogos possa ser aplicada em sistemas definidos em conjuntos discretos, é necessário estabelecer o conceito de q-deformação nesses conjuntos, como por exemplo, corpos finitos. Até onde chega o conhecimento dos autores, o conceito de q-análogos em corpos finitos ainda não está definido na literatura.

Neste trabalho é definido o q-análogo do corpo finito $\mathbb{Z}_p$, o conjunto das classes de equivalência dos números inteiros módulo p, em que p é um número primo. A versão q-deformada de $\mathbb{Z}_p$ é denotada por $[\mathbb{Z}_p]_q$. São investigadas algumas propriedades algébricas de $[\mathbb{Z}_p]_q$ e é demonstrado que quando q é um gerador do grupo multiplicativo associado a $\mathbb{Z}_p$, o mapeamento entre $\mathbb{Z}_p$ e $[\mathbb{Z}_p]_q$ é uma bijeção, ou seja, $[\mathbb{Z}_p]_q$ é uma permutação de $\mathbb{Z}_p$. Esta permutação é empregada no projeto de um PRNG e as propriedades estatísticas das sequências binárias geradas são analisadas com a suíte estatística NIST [12]. O PRNG proposto é aprovado em todos os testes da suíte NIST usando uma taxa máxima de geração de bits, ou seja, todos os bits da representação binária são utilizados para gerar a sequência binária do PRNG. Como geralmente os geradores propostos na literatura não empregam todos os bits da representação binária, o PRNG proposto além de apresentar boas propriedades estatísticas possui como vantagem uma alta taxa de geração de bits.

O restante deste trabalho está dividido conforme detalhado a seguir. Na Seção II é feita uma breve revisão de conceitos fundamentais de q-análogos e corpos finitos. A definição e investigação de propriedades algébricas dos q-análogos em corpos finitos é apresentada na Seção III. Na Seção IV é feita uma aplicação de q-análogos em corpos finitos no projeto de geradores de números pseudo-aleatórios e suas propriedades estatísticas são analisadas com a suíte NIST [12]. Por fim, na Seção V são apresentadas as considerações finais.

II. Preliminares

Nesta seção são revisadas algumas definições e propriedades elementares de q-análogos. Também é feita uma breve

Os autores são do Departmento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, e-mails: {carlos.ecsouza, ravi.figueiredo, daniel.chaves, cecilio.pimentel}@ufpe.br. Este trabalho foi parcialmente financiado pelo CNPq, pela CAPES e pela FACEPE.

introdução ao conceito de corpos finitos, sendo apresentadas propriedades necessárias para a compreensão do restante deste trabalho. Mais detalhes sobre q-análogos são encontrados em [1], [2] e sobre corpos finitos em [13].

Seja n um inteiro não negativo e seja $q \in \mathbb{R}$. O q-análogo de n (também denominado q-deformação de n), denotado por $[n]_q$, é definido por

$$[n]_q \triangleq \frac{1-q^n}{1-q}. \tag{1}$$

Alternativamente, $[n]_q$ pode ser escrito como a série de potências em q

$$[n]_q = 1 + q + q^2 + \cdots + q^{n-1}. \tag{2}$$

O q-análogo de zero é definido, por convenção, por $[0]_q = 0$. É evidente, a partir de (1), que $[1]_q = 1$. No limite $q \to 1$ temos que $\lim_{q\to 1}[n]_q \triangleq [n]_{q\to 1} = n$. q-Análogos também podem ser definidos pela relação de recorrência

$$[n+1]_q = q[n]_q + 1. \tag{3}$$

Seja p um número primo e seja $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ o conjunto das classes de equivalência dos inteiros módulo p. O conjunto $\mathbb{Z}_p$ com as operações de adição e multiplicação definem o corpo finito $(\mathbb{Z}_p, +, \times)$ de característica p, também denotado por GF(p) (*Galois Field*). Quando não houver ambiguidade, o corpo finito $(\mathbb{Z}_p, +, \times)$ será referido como o corpo finito $\mathbb{Z}_p$. Dado o conjunto $\mathbb{Z}_p$, o subconjunto $\mathbb{Z}_p - \{0\} = \{1, 2, \ldots, p-1\}$ é um grupo Abeliano de ordem $p-1$ sob a operação de multiplicação em $\mathbb{Z}_p$ e será denotado por $G = (\mathbb{Z}_p - \{0\}, \times)$. O grupo G é um grupo cíclico e um gerador de G é um elemento $g \in G$ tal que qualquer elemento $n \in G$ é dado por uma potência de g, ou seja, $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{p-2}\}$. O número de geradores distintos de um grupo cíclico com ordem l é dado pela função phi de Euler $\phi(l)$ [14]. Como G possui ordem $p-1$, o número de geradores distintos de G é $\phi(p-1)$.

III. q-Análogos em Corpos Finitos

Nesta seção é definido o q-análogo em $\mathbb{Z}_p$. São derivadas várias propriedades algébricas dos q-análogos em $\mathbb{Z}_p$ e estabelecidas as condições necessárias para que a q-deformação seja uma operação de permutação. No restante do artigo, todas as operações são definidas módulo p.

Definição 1. *Seja o corpo finito $\mathbb{Z}_p$ e seja $q \in \mathbb{Z}_p, q \neq 0$. O q-análogo de $n \in \mathbb{Z}_p, n \neq 0$ é definido por*

$$[n]_q \triangleq \frac{q^n - 1}{q-1} \pmod p \tag{4}$$

e o q-análogo de $n = 0$ é definido por

$$\begin{cases} [0]_1 \triangleq 0 \\ [0]_q \triangleq (1-q)^{-1} \pmod p,\ q \neq 1 \end{cases} \tag{5}$$

em que $(\cdot)^{-1}$ denota o inverso multiplicativo de $(\cdot)$ em $\mathbb{Z}_p$.

Similarmente ao caso dos q-análogos clássicos, os q-análogos definidos em corpos finitos podem ser escritos como uma série de potências em q

$$[n]_q = (1 + q + q^2 + \cdots + q^{n-1}) \pmod p. \tag{6}$$

Definição 2. *Seja $q \in \mathbb{Z}_p, q \neq 0$. O q-análogo do conjunto $\mathbb{Z}_p$ é definido pelo conjunto $[\mathbb{Z}_p]_q \triangleq \{[0]_q, [1]_q, [2]_q, \ldots, [p-1]_q\}$.*

Quando $q = 1$ o mapeamento entre $\mathbb{Z}_p$ e $[\mathbb{Z}_p]_q$ é a transformação identidade, conforme demonstrado na proposição a seguir.

Proposição 1. $[n]_1 \equiv n \pmod p, \forall n \in \mathbb{Z}_p$.
Demonstração: Usando (6) temos que $[n]_1 = 1 + 1^1 + 1^2 + \cdots + 1^{n-1} \equiv n \pmod p$, pois $n < p$, $\forall n \in \mathbb{Z}_p$.

A proposição seguinte aborda um ponto importante no comportamento de mapas iterativos e sequências, a análise de pontos fixos. Da definição da q-deformação é simples verificar que 1 é um ponto fixo para qualquer valor de q.

Proposição 2. $[1]_q \equiv 1 \pmod p, \forall q \in \mathbb{Z}_p, q \neq 0$.
Demonstração: Segue diretamente de (4).

Enunciamos agora um teorema sobre a q-deformação de zero, afirmando que esta nunca pode ser igual a zero, ou seja, zero nunca é ponto fixo da q-deformação.

Teorema 1. $[0]_q \neq 0, \forall q \neq 1$.
Demonstração: Suponha que $[0]_q \equiv 0 \pmod p$, então segue de (5) que $(1-q)^{-1} \equiv 0 \pmod p$ e portanto $0 \times (1-q) \equiv 1 \pmod p$, o que é uma contradição.

A partir de (6), segue que $[n]_q, n \geq 1$ pode ser alternativamente definido pela relação de recorrência

$$[n+1]_q = (q[n]_q + 1) (\mathrm{mod}\, p) \tag{7}$$

enquanto $[0]_q$ é definido separadamente por (5). Desta forma, para gerar o conjunto $[\mathbb{Z}_p]_q$ calculamos inicialmente $[0]_q$ e em seguida determinamos o restante dos q-análogos de forma iterativa a partir de $[1]_q = 1$. Neste caso, a aplicação iterativa da q-deformação gera uma dinâmica iterativa discreta sobre $\mathbb{Z}_p$ gerada por (7) que está associada com a geração de sequências numéricas definidas em $\mathbb{Z}_p$.

Definição 3. *O q-análogo inverso de $[n]_q \in [\mathbb{Z}_p]_q$, isto é, $n \in \mathbb{Z}_p$, é definido por*

$$q^n = 1 + (q-1)[n]_q \pmod p. \tag{8}$$

Observe que (8) pode ser escrita como

$$n = \log_q(1 + (q-1)[n]_q) \pmod p \tag{9}$$

em que $\log_q(\cdot)$ é o logaritmo discreto de $(\cdot)$ na base q no conjunto $\mathbb{Z}_p$. Para a demonstração do resultado principal deste trabalho, o Teorema 2, são necessários três lemas, os quais são enunciados a seguir.

Lema 1. *Dados $n \neq 0$ e $q \neq 1$, então $[n]_q \equiv 0 \pmod p$ se, e somente se, $q^n \equiv 1 \pmod p$.*
Demonstração: Suponha que $[n]_q \equiv 0 (\mathrm{mod} p)$, portanto segue da Eq. (8) que $q^n \equiv 1 \pmod p$. Agora, suponha que $q^n \equiv 1 \pmod p$, então aplicando a Eq. (8) obtemos $(q-1)[n]_q \equiv 0 (\mathrm{mod} p)$. Consequentemente, p divide $(q-1)$ ou p divide $[n_q]$. Como $q - 1 < p$, então $q - 1$ não possui fatores p e portanto p necessariamente divide $[n]_q$. Desta forma, concluímos que $[n]_q \equiv 0 \pmod p$.

O lema seguinte mostra que $p-1$ sempre é q-deformado em zero, para qualquer valor de $q \neq 1$.

Lema 2. $[p-1]_q \equiv 0 \pmod p), \forall q \in \mathbb{Z}_p, q \neq 1$. *Demonstração: Do Lema 1,* $[p-1]_q \equiv 0 \pmod p$ *se, e somente se,* $q^{p-1} \equiv 1 \pmod p$. *Agora, observe que* $q^{p-1} \equiv 1 \pmod p$ *é verdadeiro para todo* $q \neq 1$ *pelo pequeno teorema de Fermat [14].*

O próximo lema estabelece que existe um e apenas um elemento em $\mathbb{Z}_p$ que é q-deformado em zero quando q é um gerador do grupo multiplicativo G.

Lema 3. *Se* q *é um gerador de* G*, existe um único* $n \in \mathbb{Z}_p$ *com* $n \neq 0$ *tal que* $[n]_q \equiv 0 \pmod p$.
Demonstração: Suponha que existem $n, m \in \mathbb{Z}_p$ *tais que* $[n]_q \equiv 0 \pmod p$ *e* $[m]_q \equiv 0 \pmod p$. *Portanto, do Lema 1, segue que* $q^n \equiv 1 \pmod p$ *e* $q^m \equiv 1 \pmod p$ *e consequentemente* $q^m \equiv q^n \pmod p$. *Como* q *é gerador de* G*, as potências de* q *são necessariamente distintas, logo* $q^m \equiv q^n \pmod p$ *é verdadeiro se, e somente se,* $n = m$.

De posse dos três lemas anteriores, podemos enunciar o resultado principal sobre a q-deformação em corpos finitos, que associa uma bijeção entre $\mathbb{Z}_p$ e $[\mathbb{Z}_p]_q$ com o parâmetro de deformação q, ou seja, a q-deformação define uma permutação sobre $\mathbb{Z}_p$.

Teorema 2. *Se* q *é um gerador de* G*, o mapeamento entre* $\mathbb{Z}_p$ *e* $[\mathbb{Z}_p]_q$ *é uma bijeção.*
Demonstração: Sejam $n, m \in \mathbb{Z}_p$ *com* $n \neq m$ *e tais que* $[n]_q \equiv [m]_q \pmod p$. *Vamos assumir, sem perda de generalidade, que a representação de* $[n]_q$ *em potências de* q *tem mais termos que a represenção de* $[m]_q$*, logo* $[n]_q - [m]_q = q^m + q^{m+1} + \cdots + q^{n-1}$. *Como* $[n]_q \equiv [m]_q \pmod p$*, então segue que* $q^m + q^{m+1} + \cdots + q^{n-1} \equiv 0 \pmod p$*, que pode ser escrito como* $q^m(1 + q + q^2 + \cdots + q^{n-m-1}) \equiv 0 \pmod p$*, ou equivalentemente* $q^m[n-m]_q \equiv 0 \pmod p$. *Desta forma, temos que ou* p *divide* q^m *ou* p *divide* $[n-m]_q$. *Como* $q < p$*, então* q^m *não possui fatores* p *e consequentemente* p *não divide* q^m. *Segue que* p *necessariamente divide* $[n-m]_q$ *e portanto* $[n-m]_q \equiv 0 \pmod p$. *Do Lema 2 temos que* $[n-m]_q \equiv [p-1]_q \equiv 0 \pmod p$. *Como* q *é um gerador de* G*, pelo Lema 3, existe um único elemento em* $\mathbb{Z}_p$ *com que é deformado em zero, que é o próprio* $p-1$*, portanto* $n-m = p-1$. *Agora, observe que o único par possível* (n, m) *em* $\mathbb{Z}_p$ *que satisfaz esta condição é o par* $(n, m) = (p-1, 0)$ *e obviamente* $[p-1]_q \not\equiv [0]_p \pmod p$. *Como assumimos inicialmente que* $[n]_q \equiv [m]_q \pmod p$*, chegamos a uma contradição, concluindo, portanto, a demonstração.*

O Teorema 2 garante que se q for um gerador de G, o conjunto $[\mathbb{Z}_p]_q$ é uma permutação do conjunto $\mathbb{Z}_p$. Neste caso, o q-análogo de $\mathbb{Z}_p$ é interpretado como um elemento do grupo de permutações S_p. Obviamente, o número de geradores de G é menor que p, e portanto o conjunto de todas os q-análogos gerados por geradores de G é um subconjunto de S_p.

IV. Aplicação: Geradores de Números Pseudoaleatórios

Nesta seção, utilizamos a dinâmica discreta gerada pela aplicação iterativa da q-deformação para projetar um PRNG e analisamos suas propriedades estatísticas utilizando a suíte estatística NIST.

A q-deformação como aplicação iterativa define um mapa discreto com uma estrutura linear sobre $\mathbb{Z}_p$. Consideramos que a sequência inicial é dada por $\{0, 1, 2, \ldots, p-1\}$. Em seguida, calculamos a sequência q-deformada a partir de (6), observando que a deformação de zero é definida particularmente por (5). Esta sequência possui estrutura similar às sequências geradas pela classe de geradores de números pseudo-aleatórios lineares denominados LCG (*linear congruential generator*), que são geradores utilizados em diversas plataformas pela simplicidade da implementação e boas propriedades estatísticas.

Como a q-deformação em corpos finitos está associada a uma dinâmica discreta em $\mathbb{Z}_p$, os elementos de $[\mathbb{Z}]_p$ podem ser intrepretados como uma sequência obtida pela permutação dos elementos em $\mathbb{Z}_p$. Desta forma, sendo a q-deformação uma permutação (se q é um gerador de G), o período das sequências geradas pela q-deformação é igual à cardinalidade do conjunto $\mathbb{Z}_p$. Para a implementação de um PRNG, os elementos destas sequências são transformados em suas representações binárias. Em seguida, é extraído um subconjunto de bits desta representação, e os bits extraídos são concatenados para formar a sequência binária gerada pelo PRNG. Isto define uma taxa $r = k/b$, em que k é o número de bits extraídos de cada elemento e b é o número de bits na representação binária.

Para analisar as propriedades estatísticas das sequências binárias geradas, utilizamos a suíte estatística NIST versão SP800-22 [12]. Cada teste do NIST é realizado com um nível de confiança $\alpha = 0{,}01$, sendo este o valor recomendado em [12]. Os testes são realizados com um conjunto de 200 subsequências binárias, cada uma com comprimento 10^6. Para isto, inicialmente escolhemos os parâmetros p e q para definir a q-deformação. Em particular, utilizamos o primo de Mersenne $p = 2^{31} - 1$ e $q = 16807$. Desta forma, cada elemento q-deformado de $\mathbb{Z}_p$ é representado com 31 bits. Os testes realizados indicam que PRNG proposto é aprovado na bateria de testes NIST quando utiliza-se todos os bits da representação binária, isto é, obtém-se a taxa máxima $r = 1$.[1] Esta característica é uma vantagem em relação a geradores usuais da literatura com taxa $r < 1$ [15], [16], [10].

A Tabela I mostra os resultados obtidos com a suíte NIST para o PRNG proposto com os parâmetros indicados. Para critério de comparação, também incluímos o resultado do teste NIST para o PRNG baseado no mapa de Arnold proposto em [10]. Na tabela é listado cada um dos testes do NIST e a proporção de sequências aprovadas em cada teste. Quando um teste é composto de múltiplas instâncias (estes são indicados por um *), apresentamos apenas o menor valor obtido. Para os parâmetros considerados, a proporção mínima de sequências que devem obter sucesso no teste é $0{,}965$. O PRNG proposto

[1] Para gerar as sequências binárias de entrada do teste NIST calculamos a permutação de $\{0, 1, 2, \ldots, N\}$ para um valor suficientemente grande de N para gerar 200 milhões de bits.

TABELA I
PROPORÇÕES OBTIDAS COM AS SUÍTE ESTATÍSTICA NIST PARA AS SEQUÊNCIAS BINÁRIAS GERADAS PELO PRNG PROPOSTO E PARA O PRNG PROPOSTO EM [10]. O VALOR MÍNIMO PARA APROVAÇÃO É 0,965. NOS TESTES MÚLTIPLOS (INDICADOS POR *) É APRESENTADO APENAS O VALOR MÍNIMO.

Teste Estatístico	q-Análogos	Arnold
Frequency	0,985	0,995
Block Frequency	0,995	0,985
Cumulative Sums*	0,985	0,99
Runs	0,995	0,985
Longest Run	0,98	0,99
Rank	0,995	1
FFT	0,97	0,985
Non Overlapping Template*	0,97	0,965
Overlapping Template	0,985	0,985
Universal	0,98	0,97
Approximate Entropy	0,99	0,99
Random Excursions*	0,974	0,976
Random Excursions Variant*	0,982	0,968
Serial*	0,98	0,985
Linear Complexity	0,985	0,985

em [10] utiliza o mapa de Arnold discreto definido sobre o anel de inteiros $\mathbb{Z}_{3^m}$. Para $m = 20$ podemos utilizar uma representação de 32 bits para cada elemento gerado pela aplicação iterativa do mapa de Arnold discreto. Em particular, o PRNG proposto em [10] tem taxa máxima $r = 0{,}75$ para obtenção de aprovação em todos os testes do NIST. Portanto, se for utilizada uma taxa maior que a taxa máxima ocorre uma degradação nas proprieadades estatísticas das sequências binárias e em consequência a reprovação no NIST.

Calculando a média para os PRNG baseados na q-deformação e no mapa de Arnold a partir das proporções indicadas na Tabela I, obtemos $0{,}9834$ e $0{,}9836$, respectivamente, indicando que os dois PRNG possuem uma média de aprovação equivalente. Desta forma, ambos os PRNG conseguem gerar sequências binárias com boas propriedades estatísticas. Entretanto, o PRNG proposto neste trabalho possui taxa superior, que é taxa máxima permitida $r = 1$, resultando em uma maior capacidade de geração de bits para conjuntos discretos com cardinalidade equivalente, em comparação com o PRNG proposto em [10].

Uma outra comparação pode ser feita com um PRNG baseado em mapas caóticos reais. Em [15] é proposto um PRNG baseado no mapa logístico sobre os números reais. No referido trabalho, é empregado o mapa logístico com parâmetro de controle variável com o objetivo de melhorar a estatística das sequências binárias obtidas. Cada amostra caótica gerada pela iteração do mapa logístico é representada com 32 bits e desta representação binária extrai-se o bit menos significativo, e taxa resultante é $r = 1/32$. Para avaliar a qualidade das sequências binárias obtidas em [15], também é utlizada a suíte NIST e as sequências passam em todos os testes com uma média de aprovação de $0{,}989$. Esta média é um pouco superior à taxa obtida pelo PRNG proposto neste trabalho, entretanto o PRNG proposto possui uma maior capacidade de geração de bits por amostra devido à sua taxa superior.

V. CONCLUSÕES

Neste trabalho definimos e analisamos algumas propriedades algébricas de q-análogos em corpos finitos $\mathbb{Z}_p$. Estabelecemos as condições necessárias para as quais a q-deformação é uma permutação dos elementos de $\mathbb{Z}_p$. Apresentamos uma possível aplicação dos q-análogos como um PRNG e simulações numéricas utilizando a suíte estatística NIST evidenciam que o PRNG proposto possui boas propriedades estatísticas. Além disso, o PRNG proposto possui taxa máxima de geração de bits, enquanto na literatura, em geral, são consideradas taxas baixas para a obtenção de boas propriedades estatísticas.

Um prosseguimento natural deste trabalho, atualmente em andamento pelos autores, é a definição de q-análogos em corpos de extensão $\mathrm{GF}(p^k)$, bem como a busca por novas aplicações de q-análogos em corpos finitos. Uma possibilidade de aplicação para os q-análogos é utilizar a dinâmica iterativa gerada pela aplicação sucessiva da q-deformação em processos de cifragem, em que os parâmetros p e q podem ser considerados chaves secretas. Para valores elevados de p torna-se inviável buscar todos os valores de q que são geradores de G e em seguida gerar todas as permutações de $\mathbb{Z}_p$ para todos os valores possíveis de q para realizar uma busca por força bruta. No caso do cálculo da transformação inversa, o problema recai em um problema de logaritmo discreto, que em geral é um problema computacionalmente inviável.

Ainda em consequência dos resultados apresentados neste trabalho, um outro prosseguimento, também em andamento pelos autores, é investigar o efeito da q-deformação em sistemas definidos em estruturas discretas, como por exemplo mapas caóticos discretos. Alguns trabalhos recentes analisam o efeito da q-deformação na dinâmica de mapas caóticos reais conhecidos, como o mapa logístico e o mapa de Hénon. Entretanto, no caso de mapas caóticos discretos, ainda não existem análises do efeito da q-deformação na dinâmica destes mapas e nas suas propriedades estatísticas.

REFERÊNCIAS

[1] P. C. Victor Kac, *Quantum calculus*, 1st ed., ser. Universitext. Springer-Verlag, New York, 2002.

[2] R. R. George E. Andrews, Richard Askey, *Special functions*, ser. Encyclopedia of mathematics and its applications 71. Cambridge University Press, 1999.

[3] S. Morier-Genoud and V. Ovsienko, "On q-deformed real numbers," *Experimental Mathematics*, p. 1–9, Oct. 2019.

[4] ——, "q-deformed rationals and q-continued fractions," *Forum of Mathematics, Sigma*, vol. 8, March 2020.

[5] V. Patidar, G. Purohit, and K. K. Sud, "Dynamical behavior of q-deformed Henon map," *International Journal of Bifurcation and Chaos*, vol. 21, no. 05, pp. 1349–1356, July 2011.

[6] S. Behnia, M. Yahyavi, and R. Habibpourbisafar, "Watermarking based on discrete wavelet transform and q-deformed chaotic map," *Chaos, Solitons & Fractals*, vol. 104, pp. 6–17, Nov. 2017.

[7] J. Cánovas and M. Muñoz-Guillermo, "On the dynamics of the q-deformed logistic map," *Physics Letters A*, vol. 383, no. 15, pp. 1742–1754, may 2019.

[8] G.-C. Wu, M. Niyazi Çankaya, and S. Banerjee, "Fractional q-deformed chaotic maps: A weight function approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 12, p. 121106, Dec. 2020.

[9] L. Kocarev, J. Szczepanski, J. M. Amigo, and I. Tomovski, "Discrete chaos-I: Theory," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 53, no. 6, pp. 1300–1309, June 2006.

[10] C. E. C. Souza, D. P. B. Chaves, and C. Pimentel, "One-dimensional pseudo-chaotic sequences based on the discrete Arnold's cat map over Z3m," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 1, pp. 491–495, Jan. 2021.

[11] B. Chirikov and F. Vivaldi, "An algorithmic view of pseudochaos," *Physica D: Nonlinear Phenomena*, vol. 129, no. 3, pp. 223 – 235, May 1999.

[12] L. E. B. III *et al.*, *SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Gaithersburg, MD, United States: Nat. Inst. Std. & Technol., 2010.

[13] R. J. McEliece, *Finite fields for computer scientists and engineers*, 1st ed., ser. The Kluwer international series in engineering and computer science Information theory SECS23. Kluwer Academic Publishers, 1987.

[14] G. H. Hardy, E. M. Wright, D. R. Heath-Brown, and J. H. Silverman, *An Introduction to the Theory of Numbers*, 6th ed. Oxford University Press, 2008.

[15] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 1, pp. 291–293, Jan. 2019.

[16] R. Lan, J. He, S. Wang, Y. Liu, and X. Luo, "A parameter-selection-based chaotic system," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 3, pp. 492–496, March 2019.