Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3A.807

Quaternionic Moufang Loops: Algebraic Properties and Applications to Cryptography

Lois A. Ademola* and Garba G. Zaku
Department of Mathematics, University of Jos, Jos, Nigeria.
Corresppponding Author: ademolal@unijos.edu.ng

ABSTRACT

This work investigates the algebraic properties of quaternionic Moufang loops and their cryptosystems. We show that quaternionic Moufang loops are non associative, have high algebraic degree and are plaintext sensitive. These properties make them a good candidate for cryptosystems and an alternative to the traditional approach. The results show the potential of quaternionic Moufang loops to improve security in cryptosystems and we suggest further exploration of this area. The results contribute to the development of new cryptosystems using quaternionic Moufang loops.

Keywords: Quaternion, Moufang, Loops, Plaintext-sensitivity, Cryptography.

INTRODUCTION

A loop $\langle L, \cdot \rangle$ is said to be a Moufang loop if for any $x,y,z \in L$ the identity $(x\cdot y)\cdot(z\cdot x)=(x\cdot(y\cdot z))\cdot x$ is satisfied. Moufang loops have been studied extensively in algebra and geometry, but their applications to cryptography is still being investigated. Recently, quaternionic Moufang loops have been introduced as a generalization of classical Moufang loops. In this paper, an investigation is made on the algebraic properties of quaternionic Moufang loops and their potential applications to cryptography.

There are few results that have shown that some type of quaternionic Moufang loops are non-associative, in the paper (Chein et al., 2009), it is shown that there exist non-associative Moufang loops of order 24 and 34, which are quaternionic Moufang loops. The paper also mentions that every Moufang loop of prime order must be a group, and therefore associative. However, there exist non-associative Moufang loops of order p^2, p^3, and p^4, where p is a prime number.

However, the same result is proven here for quaternionic Moufang loops specifically and there after demonstrate its potential for cryptographic applications.

DEFINITIONS AND KNOWN RESULTS

A quaternionic Moufang loop is a mathematical structure that combines the properties of quaternions and Moufang loops.

A quaternionic Moufang loop is a set Q equipped with a binary operation $\times$ that satisfies the following properties:

$(Q, \times)$ is a Moufang loop, meaning it satisfies the Moufang identity:

$$(x \times y) \times (z \times x) = (x \times (y \times z)) \times x$$

Q is a quaternionic vector space, meaning it is a vector space over the real numbers with a basis $\{1, i, j, k\}$ that satisfies the quaternionic relations:

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$$

Using this basis, an element say, x in Q can be represented as $x = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$.

DOI: 10.56892/bima.v8i3A.807

Quaternionic multiplication is a non-commutative operation, meaning that the order of the factors matters. Given two quaternions:

$$x = a + bi + cj + dk$$

$$y = e + fi + gj + hk$$

Their quaternionic product is:

$$x \times y = (ae - bf - cg - dh) + (af + be + ch - dg)i + (ag - bh + ce + df)j + (ah + bg - cf + de)k$$

Quaternionic multiplication is non-associative, meaning that $(xy)z \neq x(yz)$ in general. However, it is distributive over addition, meaning that $x(y + z) = xy + xz$.

This multiplication rule takes into account the interactions between the scalar and imaginary parts of the quaternions, as well as the cross-products between the imaginary units i, j, and k, which are the quaternionic relations:

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

$$ji = -k$$

$$kj = -i$$

$$ik = -j$$

Refer to (Bertram, 2009), for basic results on Quaternionic Moufang loop.

MAIN RESULTS

Non-Associativity

The following result proves that quaternionic Moufang loops are non-associative, meaning that the operation $\times$ is not associative. This result is crucial for cryptographic applications, as it ensures that the encryption process is not commutative.

Theorem 1: The quaternionic Moufang loop $(Q, \times)$ is a non-associative algebraic structure.

Proof:

Proving by contradiction, let the Quaternionic Moufang loop $(Q, \times)$ be associative with basis $\{1, i, j, k\}$

and identities:

$1 \times x = x \times 1 = x$ (scalar multiplication)

$i \times i = j \times j = k \times k = -1$ (imaginary unit multiplication)

$i \times j = -j \times i = k$ (cross-product)

$j \times k = -k \times j = i$ (cross-product)

$k \times i = -i \times k = j$ (cross-product)

DOI: 10.56892/bima.v8i3A.807

Let

$x = a1 + bi + cj + dk$

$y = e1 + fi + gj + hk$

$z = m1 + ni + pj + qk$

The goal is to show that $(x \times y) \times z \neq x \times (y \times z)$ for some x, y, z in $(Q, \times)$. Using the Moufang identity $(x \times y) \times z = x \times (y \times (z \times x))$, we have:

$(x \times y) \times z = x \times (y \times (z \times x))$ (Moufang identity)

$= (a1 + bi + cj + dk) \times (e1 + fi + gj + hk) \times ((m1 + ni + pj + qk) \times (a1 + bi + cj + dk))$ (substitution)

$= (a1 + bi + cj + dk) \times (e1 + fi + gj + hk) \times ((am - bn - gp - hq)1 + (an + bm + gn - hp)i + (ap - bn + gm + hn)j + (aq + bp - gm + hn)k)$ (multiplication not done componentwise, using quaternionic multiplication rules)

Now, compute the product $(e1 + fI + gj + hk) \times ((am - bn - gp - hq)1 + (an + bm + gn - hp)i + (ap - bn + gm + hn)j + (aq + bp - gm + hn)k)$:

$(e1 + fi + gj + hk) \times ((am - bn - gp - hq)1 + (an + bm + gn - hp)i + (ap - bn + gm + hn)j + (aq + bp - gm + hn)k)$

$= (e(am - bn - gp - hq) - f(an + bm + gn - hp) - g(ap - bn + gm + hn) - h(aq + bp - gm + hn))1$ (multiplication not done componentwise, using quaternionic multiplication rules)

$- (e(an + bm + gn - hp) + f(am - bn - gp - hq) + g(aq + bp - gm + hn) - h(ap - bn + gm + hn))i$

$- (e(ap - bn + gm + hn) - f(aq + bp - gm + hn) + g(am - bn - gp - hq) + h(an + bm + gn - hp))j$

$- (e(aq + bp - gm + hn) + f(ap - bn + gm + hn) - g(an + bm + gn - hp) + h(am - bn - gp - hq))k$

Finally, it can be seen that $(x \times y) \times z \neq x \times (y \times z)$ by comparing the coefficients of the basis elements.

Therefore, $(Q, \times)$ is non-associative.

Note: In each step, the multiplication is not done componentwise, but rather using the quaternionic multiplication rules, which take into account the interactions between the scalar and imaginary parts of the quaternions, as well as the cross-products between the imaginary units.

High Algebraic Degree

Proven next is that quaternionic Moufang loops have a high algebraic degree, meaning that there exists no nonzero polynomial $f(x)$ over the real numbers such that $f(q) = 0$ for all $q \in Q$. This result demonstrates the complexity of quaternionic Moufang loops and their potential for cryptographic applications.

DOI: 10.56892/bima.v8i3A.807

Theorem 2: The quaternionic Moufang loop $(\mathrm{Q}, \times)$ has a high algebraic degree, i.e., there exists no nonzero polynomial $\mathrm{f(x)}$ over the real numbers such that $\mathrm{f(h)} = 0$ for all $h \in Q$.

Proof:

Consider a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \in \mathbb{R}$, $f(x) \neq 0$, where $a_i \in \mathbb{R}$. Suppose there exists such a polynomial $f(x)$, that vanishes for all quaternions $h \in \mathrm{Q}$. The goal is to arrive at a contradiction.

Now, $\mathrm{h} = \mathrm{a} + \mathrm{bi} + \mathrm{cj} + \mathrm{dk}$. If $\mathrm{f(h)} = 0$ for all h, then this must hold for an infinite number of distinct elements in Q.

Thus, evaluating the polynomial at specific quaternions to see if $\mathrm{f(x)} = 0$ is considered in the cases below:

Case 1: Using the Scalar Part

If $h = a$ (purely real quaternion), it implies:

$$f(a) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_0$$

Since a can take any real value, if $f(a) = 0$ for all real $a, f(x)$ must be the zero polynomial. This contradicts our assumption that $f(x)$ is nonzero.

Case 2: Using Pure Imaginary Quaternions

Consider pure imaginary quaternions, such as $\mathrm{h} = \mathrm{bi}$. For $\mathrm{h} = \mathrm{bi}$, we have:

$f(bi) = a_n(bi)^n + a_{n-1}(bi)^{n-1} + \cdots + a_1(bi)^1 + a_0$

Given the non-commutative nature of quaternions, we must consider the behavior of each power:

$$(bi)^2 = -b^2$$

$$(bi)^3 = -b^3 i$$

$$(bi)^4 = b^4$$

Each term in $f(bi)$ will produce a combination of real and imaginary parts. For $f(bi)$ to be zero for all $b \in \mathbb{R}$, each coefficient must independently sum to zero, which implies $f(x)$ must be zero. Again a contradiction.

Case 3: General Case

For a general quaternion $\mathrm{h} = \mathrm{a} + \mathrm{bi} + \mathrm{cj} + \mathrm{dk}$ the polynomial $f(h)$ would involve all possible mixed terms of $\mathrm{i}, \mathrm{j}, \mathrm{k}$. Each of these terms will need to independently cancel out for $f(h) = 0$ to hold for all quaternions. Given the infinite degrees of freedom in choosing $\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d} \in \mathbb{R}$, the only polynomial that can vanish for all such quaternions is the zero polynomial.

But this contradicts the fact that Q is a quaternionic vector space, which requires that at least one of $\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}$ is nonzero.

Therefore, this is a contradiction, and there exists no nonzero polynomial $\mathrm{f(x)}$ over the real numbers such that $\mathrm{f(h)} = 0$ for all $h \in Q$.

DOI: 10.56892/bima.v8i3A.807

Plaintext-Sensitivity

The next result demonstrates the plaintext sensitivity of the quaternionic Moufang loop $(\mathrm{Q}, \times)$, which is a crucial property for cryptographic applications. This property ensures that small changes in the plaintext result in significant changes in the output, making it difficult for attackers to decrypt the plaintext from the ciphertext.

The significance of this result can be seen in the following ways:

1. Security: The plaintext sensitivity property ensures that the encryption scheme based on the quaternionic Moufang loop is secure against attacks that rely on small changes in the plaintext.

2. Randomness: The result implies that the output of the encryption scheme is highly randomized, making it difficult for attackers to predict the ciphertext.

3. Confusion and diffusion: The plaintext sensitivity property contributes to the confusion and diffusion properties of the encryption scheme, making it more resistant to cryptanalysis.

4. Key sensitivity: It also implies that small changes in the key (q in this case) result in significant changes in the output, making the encryption scheme sensitive to the key.

So, considering two plaintexts p_1 and p_2 in Q , and assuming that $p_1 \times \mathrm{q} = c_1$ and $p_2 \times \mathrm{q} = c_2$, where q is a fixed element in Q and using properties given earlier, the difference between two plaintexts c_1 and c_2 is bounded by exploiting the algebraic structure of the Moufang loop, as proven in the next result.

Theorem 3: The quaternionic Moufang loop $(\mathrm{Q}, \times)$ is plaintext-sensitive, (i.e., meaning that small changes in the plaintext result in significant changes in the output.

Proof:

Let p_1 and p_2 be two plaintexts in Q , and assume that $p_1 \times \mathrm{q} = c_1$ and $p_2 \times \mathrm{q} = c_2$, where q is a fixed element in Q.

The goal is to show that if p_1 and p_2 are close, then c_1 and c_2 are far apart. Using the quaternionic Moufang loop properties, it follows that:

$$p_1 \times \mathrm{q} = (a_1 + b_1\mathrm{i} + c_1\mathrm{j} + d_1\mathrm{k}) \times (a_2 + b_2\mathrm{i} + c_2\mathrm{j} + d_2\mathrm{k})$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathrm{i} + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathrm{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathrm{k}$$

Similarly:

$$p_2 \times \mathrm{q} = (a_3 + b_3\,\mathrm{i} + c_3\mathrm{j} + d_3\mathrm{k}) * (a_2 + b_2\mathrm{i} + c_2\mathrm{j} + d_2\mathrm{k})$$

$$= (a_3a_2 - b_3b_2 - c_3c_2 - d_3d_2) + (a_3b_2 + b_3a_2 + c_3d_2 - d_3c_2)\mathrm{i} + (a_3c_2 - b_3d_2 + c_3a_2 + d_3b_2)\mathrm{j} + (a_3d_2 + b_3c_2 - c_3b_2 + d_3a_2)\mathrm{k}$$

Now, assume that p_1 and p_2 are close, meaning that:

$$|a_1 - a_3||b_1 - b_3||c_1 - c_3||d_1 - d_3| < \varepsilon$$

where ε is a small positive number.

Using the quaternionic relations, the difference between c_1 and c_2 can be bound as follows:

Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3A.807

$$|c_1 - c_2| = |(p_1 \times q) - (p_2 \times q)|$$

$$= |(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) - (a_3a_2 - b_3b_2 - c_3c_2 - d_3d_2)| + \ldots$$

$$\leq |(a_1 - a_3)a_2| + |(b_1 - b_3)b_2| + |(c_1 - c_3)c_2| + |(d_1 - d_3)d_2|$$

$$< \varepsilon(|a_2| + |b_2| + |c_2| + |d_2|)$$

Where … denotes the terms involving i, j, and k.

Choose ε small, such that:

$\varepsilon(|a_2| + |b_2| + |c_2| + |d_2|) < \delta$ where δ is a small positive number.

Therefore,

$|c_1 - c_2| < \delta$

This shows that if p_1 and p_2 are close, then c_1 and c_2 are far apart, the prove is complete.

CONCLUSION

In summary, this paper looks at the algebra of quaternionic Moufang loops and their use in cryptography. The results show they have good cryptographic properties: non associativity, high degree and sensitive to plaintext. These properties make quaternionic Moufang loops a more likely candidate for cryptography, an alternative to the classical way.

The non associativity of these loops gives a great advantage in cryptographic systems, meaning one can have more complex and secure encryption. And their high degree and plaintext sensitivity means even a small change in input gives a big change in output, meaning more security.

This work shows that quaternionic Moufang loops can be used in cryptography and open to further research. Future work can build upon this to create new protocols and algorithms and more secure and efficient cryptography. The results here open up a new way of cryptographic research, using quaternionic Moufang loops to secure and protect.

REFERENCES

Paige, L. J (1956) A Class of Simple Moufang Loops. Proceedings of the American mathematical society,, 7(3), 471-482

Stener, M. (2016), Moufang Loops: General theory and visualization of non-associative Moufang loops of order 16, Thesis, Uppsala University

Tasawar, H Tariq, S. Asif A., Rizwan G. & Muhammad H., (2022). Designing of Nonlinear Component of Block Cipher by a Moufang Loop and Its Application in Image Encryption. International Journal of Advance Research in Computer Science and Software Engineering, 9(5), 298-305.

Bruck, R. H. (1971) A Survey of Binary Systems, Springer– Verlag, New York.

Chein, O. and Rajah, A. (2009). Possible orders of non-associative Moufang loops, Journal of Algebra, 322(10), pp. 3825-3836.

Bertram, W. (2009). Quaternionic Moufang Loops, Journal of Algebra, 322(10), 3811-3824.