Connecting Projective Geometry over Finite Fields and Rings to Quantum Information: A Unified Framework

Faysal El Khettabi[1]

[1]faysal.el.khettabi@gmail.com , LinkedIn: faysal-el-khettabi-ph-d-4847415

The Beauty of Expanding Knowledge

Abstract

This report synthesizes recent explorations into the rich interplay between projective metric geometry over finite fields and rings and fundamental concepts in quantum information theory. Focusing on projective spaces $PG(n,p)$ and their associated quadratic forms, Clifford algebras, and symmetry groups, we highlight the crucial role of finite fields like $\mathbb{F}_4$ and rings like $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ in providing a mathematical foundation for quantum logic, state classification, and generalized symmetries relevant to quantum computation. We argue that moving beyond traditional field-based arithmetic, particularly by incorporating modulo 4 considerations, is essential for unlocking the full structure of quantum resources and operations. This unified framework offers a powerful geometric and algebraic language for describing quantum phenomena.

1 Introduction

The mathematical description of quantum mechanics conventionally relies on complex Hilbert spaces. However, finite algebraic and geometric structures are increasingly recognized as powerful tools for modeling quantum information processing, particularly in areas like quantum error correction and the study of quantum contextuality. This report outlines a framework that connects projective metric geometry over finite fields and rings, Clifford algebras, and concepts essential to quantum computing, drawing insights from existing literature and recent discussions. We emphasize the necessity of exploring the full spectrum of arithmetic contexts, including finite fields like $\mathbb{F}_2$ and $\mathbb{F}_4$, and rings like $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, to capture crucial quantum distinctions. This work is part of a broader exploration into the mathematical foundations of hypercomplex numbers and their applications [1], specifically aiming to reconnect Quantum Information as

a unified framework grounded in the powerset of ordered sets $\{1, \ldots, n\}$ under ZF set theory and its representation by projective geometries $PG(n, 2)$ as introduced with Veldkamp space in literature such as [4]. A finite-dimensional vector space V over a field F, endowed with a quadratic form Q, forms a metric vector space (V, Q). The associated polar form $B(x, y) = Q(x + y) - Q(x) - Q(y)$ satisfies $B(x, x) = 2Q(x)$. Formulations for such structures and their Clifford algebras can be found in literature such as [2]. However, this prior work has not conducted the modular analysis related to $B(x, x) = 2Q(x) \pmod 4$ that is central to the original motivation of this paper. Furthermore, while [4] introduces $PG(n, 2)$ via Veldkamp space, our approach emphasizes the foundational role of the powerset of ordered sets under ZF set theory [1] as a critical basis for this geometric representation.

2 Projective Metric Geometry and Algebraic Structures

The Clifford algebra $Cl(V, Q)$ associated with (V, Q) provides an algebraic framework for the geometry of (V, Q). The Lipschitz group, a subgroup of the invertible elements in $Cl(V, Q)$, is particularly important as it maps surjectively onto the weak orthogonal group $O'(V, Q)$, which preserves the quadratic form. Projecting to the projective space $PG(V, Q)$, the action of a quotient of the Lipschitz group on the projective metric space reveals the structure of the projective orthogonal group $PO'(V, Q)$. These connections, sometimes termed kinematic mappings, highlight deep links between algebraic structures and geometric transformations. For $F = \mathbb{F}_2$, $PG(n, 2)$ can be viewed as the projective geometry of the powerset of a set with $n + 1$ elements.

3 Arithmetic Contexts: Fields and Rings

The choice of the underlying arithmetic structure profoundly influences the properties of Q and B:

- $\mathbb{F}_2$: In characteristic 2, $B(x, x) = 2Q(x) \equiv 0$ for all x. The bilinear form B is always alternating. Q cannot be uniquely recovered from B. Geometric structures in $PG(n, 2)$ are closely tied to symplectic geometry and are relevant for classical binary codes.

- $\mathbb{F}_4$: Also of characteristic 2, but with four elements $\{0, 1, \omega, \omega^2\}$ where $\omega^2 + \omega + 1 = 0$. In field arithmetic, $B(x, x) = 2Q(x) = 0$. However, the structure of $\mathbb{F}_4$ allows for a crucial interpretation modulo 4.

- $\mathbb{Z}_4$: The ring of integers modulo 4 is essential for interpreting $B(x, x)$ modulo 4. While $B(x, x) = 0$ in $\mathbb{F}_4$, by considering the value of $Q(x) \in \mathbb{F}_4$ modulo 2 (as 0 or 1) and calculating $2 \times (Q(x) \pmod 2) \pmod 4$, $B(x, x)$ can be 0 or 2 modulo 4. This distinction is invisible in field arithmetic but is essential for quantum logic.

- $\mathbb{Z}_2 \times \mathbb{Z}_2$: This modular ring, isomorphic to $\mathbb{Z}_4$ under certain conditions, introduces zero divisors, further complicating the algebraic structures, particularly Clifford algebras and the non-degeneracy of the bilinear form. However, it also offers new perspectives on modular structures.

4 Quantum Logic and the Modulo 4 Distinction in PG(6,4)

In $PG(6, 4)$, the modulo 4 interpretation of the quadratic and bilinear forms provides a direct link to quantum information concepts. The value of $Q(x)$ (mod 2) serves as a primary classifier for vectors. This directly determines $B(x, x)$ (mod 4):

- If $Q(x) \equiv 0 \pmod 2$, then $B(x, x) \equiv 0 \pmod 4$. These vectors correspond to *stabilizer-like states*.

- If $Q(x) \equiv 1 \pmod 2$, then $B(x, x) \equiv 2 \pmod 4$. These vectors correspond to *magic-like states*.

This distinction, where $B(x, x)$ (mod 4) acts as an observable label (0 or 2) for the state type determined by $Q(x)$ (mod 2), is fundamental to quantum logic, the resource theory of magic states, and understanding quantum contextuality. [2] Classical literature, focusing on field arithmetic where $B(x, x) = 0$, often does not highlight this crucial distinction, which is a key innovation from quantum information theory.

For example, consider a vector $x = (1, 0, 0, 1, 0, 0, 0)$ in the vector space over $\mathbb{F}_4$ underlying $PG(6, 4)$ (using coordinates x_1 to x_7). For the parabolic quadric $Q(x) = x_1 x_4 + x_2 x_5 + x_3 x_6 + x_7^2$, we have $Q(x) = (1)(1) + (0)(0) + (0)(0) + (0)^2 = 1$. Interpreting $Q(x) = 1$ as 1 (mod 2), we get $B(x, x) = 2Q(x) \equiv 2 \cdot 1 \equiv 2 \pmod 4$. This vector is classified as magic-like. For a vector $y = (1, 0, 0, 0, 0, 0, 0)$, $Q(y) = (1)(0) + (0)(0) + (0)(0) + (0)^2 = 0$. Interpreting $Q(y) = 0$ as 0 (mod 2), we get $B(y, y) = 2Q(y) \equiv 2 \cdot 0 \equiv 0 \pmod 4$. This vector is classified as stabilizer-like.

5 Modulo 4 Arithmetic: A Concrete Perspective for Measurement

To further underscore the physical relevance of modulo 4 arithmetic, we can ground it in the arithmetic of natural numbers. Any natural number $L > 0$ has a unique prime factorization $L = 2^{r_2} \cdot p_1^{h_1} \cdot p_2^{h_2} \cdots$, where p_i are distinct odd primes and $r_2, h_i \geq 0$. The value of L (mod 4) is determined solely by the exponent of 2, r_2, and the sum of the exponents of prime factors congruent to 3 modulo 4. Let $s_3 = \sum_{p_i \equiv 3 \pmod 4} h_i$.

- If $r_2 = 0$, L is odd. $L \pmod 4 \equiv \prod p_i^{h_i} \pmod 4$. Primes $p_i \equiv 1 \pmod 4$ contribute $1^{h_i} \equiv 1 \pmod 4$. Primes $p_i \equiv 3 \pmod 4$ contribute $3^{h_i} \equiv (-1)^{h_i} \pmod 4$. Thus, $L \pmod 4 \equiv (-1)^{s_3} \pmod 4$. This is $1 \pmod 4$ if s_3 is even, and $3 \pmod 4$ if s_3 is odd.

- If $r_2 = 1$, $L = 2 \cdot (\text{odd number})$. $L \pmod 4 \equiv 2 \cdot (\text{odd number}) \pmod 4$. Since any odd number is $1 \pmod 4$ or $3 \pmod 4$, $L \pmod 4 \equiv 2 \cdot 1 \equiv 2 \pmod 4$ or $L \pmod 4 \equiv 2 \cdot 3 = 6 \equiv 2 \pmod 4$. Thus, $L \pmod 4 \equiv 2$ if $r_2 = 1$.

- If $r_2 \geq 2$, $L = 2^{r_2} \cdot (\text{odd number})$. $L \pmod 4 \equiv 2^2 \cdot 2^{r_2 - 2} \cdot (\text{odd number}) \equiv 4 \cdot (\dots) \equiv 0 \pmod 4$. Thus, $L \pmod 4 \equiv 0$ if $r_2 \geq 2$.

This number-theoretic perspective demonstrates that the values modulo 4 (0, 1, 2, 3) are concretely tied to the fundamental prime factorization of any integer. The specific values 0 and 2, crucial for the $B(x, x) \pmod 4$ classification, correspond directly to the power of 2 in the number's factorization ($r_2 \geq 2$ for 0, $r_2 = 1$ for 2). This grounding in natural number arithmetic makes the modulo 4 distinction highly suitable for interpreting measurement outcomes in quantum theory, providing a more concrete basis for the quantum logic encoded in $PG(6, 4)$ than purely field-based arithmetic where $B(x, x)$ is algebraically zero.

6 Nonlinear Transformations and "Twisted" Structures

The study extends to nonlinear transformations that preserve the fundamental quantum logic encoded by the quadratic form. A transformation $x \mapsto x_{new}$ is considered "suitable" if it preserves the quadratic form modulo 4, i.e., $Q(x_{new}) \equiv Q(x) \pmod 4$. This condition, stronger than $Q(x_{new}) \equiv Q(x) \pmod 2$, ensures that the transformation respects the stabilizer/magic state classification. Nonlinear functions f_1, f_2 in a transformation introduce a "twist" to the geometry, analogous to how **twisted octonions** are formed by modifying the multiplication rule of standard octonions. [3] These nonlinear transformations generalize the linear symmetries associated with Clifford algebras and provide models for quantum operations beyond the standard Clifford group, relevant for quantum circuit synthesis and exploring the boundary of quantum contextuality.

7 Further Perspectives and Foundational Insights

7.1 Foundational Aspects: Set Theory and Projective Geometry Representation

Our framework emphasizes the role of $PG(n, 2)$ as the projective geometry of the powerset of a set with $n + 1$ elements. This perspective is rooted in set

theory, specifically the powerset construction on ordered sets $\{1, \ldots, n\}$ under ZF set theory [1]. While literature such as [4] introduces $PG(n, 2)$ using the concept of Veldkamp space, it is critical to note that this approach focuses on the combinatorial properties derived from the cardinality of sets, $|X| = N + 1$, for the definition of combinatorial Grassmannians $G_k(|X|)$, rather than explicitly building upon the foundational structure of ordered sets $\{1, \ldots, N+1\}$ as provided by ZF set theory. Our work highlights the importance of this foundational set-theoretic basis for the geometric representation, providing a more fundamental link between discrete structures and projective geometries relevant to quantum information.

7.2 Revisiting Contextuality and Embeddings: The Necessity of Modulo 4

Some recent literature, such as [5], describes configurations like HC and HS in $PG(6, 2)$ and their projections to $W(5, 2)$, treating the relevant properties and transformations solely under modulo 2 arithmetic. For instance, the parabolic quadric is given as $x_1 x_4 + x_2 x_5 + x_3 x_6 + x_7^2 = 0 \pmod{2}$, and transformations are defined with functions like $f_4(x) = x_3 x_5 + x_7 x_4$ and $f_5(x) = x_4 x_6 + x_7 x_5$, leading to a "skew" embedding in $W(5, 2)$. However, as demonstrated in this paper, treating these structures solely under modulo 2 is insufficient for capturing the full quantum logic and contextuality. The crucial distinction between stabilizer-like and magic-like states, fundamental to quantum contextuality and resource theories, relies on the modulo 4 behavior of $B(x, x) = 2Q(x)$. This distinction is invisible in modulo 2 arithmetic where $B(x, x)$ is always 0. Our work emphasizes that the modulo 4 perspective is the necessary framework for a complete understanding of contextuality and embeddings in these geometries, providing a more robust foundation for quantum information theory.

8 Conclusion

This report has explored the deep connections between projective metric geometry over finite fields and rings and fundamental concepts in quantum information. We have shown how the algebraic structures of quadratic forms and Clifford algebras, particularly in $PG(6, 4)$, provide a powerful framework for encoding quantum logic through the modulo 4 behavior of the quadratic and bilinear forms. This perspective, which goes beyond traditional field arithmetic, is essential for distinguishing quantum resource states and understanding contextuality. Furthermore, we have discussed how nonlinear "twisted" transformations preserving this modulo 4 structure generalize the notion of symmetry and offer insights into quantum operations. Our work highlights the importance of the full spectrum of arithmetic contexts, including $\mathbb{F}_2, \mathbb{F}_4, \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$, and emphasizes the foundational role of set theory in representing these geometries. By embracing these richer mathematical structures, we gain a more complete and robust language for describing and developing quantum computation and

error correction. It is time to fully explore the capabilities offered by these finite geometric and algebraic structures.

Acknowledgments

References

[1] Faysal El Khettabi, A Comprehensive Modern Mathematical Foundation for Hypercomplex Numbers with Recollection of Sir William Rowan Hamilton, John T. Graves, and Arthur Cayley, in HypComNumSetTheGCFEK-FEB2024.pdf.

[2] Hans Havlicek, Projective metric geometry and Clifford algebras, arXiv:2109.11470.

[3] Sultan Catto and Donald Chesley, Twisted Octonions and Their Symmetry Groups, Nuclear Physics B (Proc. Suppl.) 6 (1989) 428-432.

[4] Frederic Saniga, Petr Holweck, and Petr Pracna, Cayley-Dickson Algebras and Finite Geometry Metods, arXiv:1405.6888.

[5] Frédéric Holweck, Henri de Boutray, and Metod Saniga, Three-Qubit-Embedded Split Cayley Hexagon is Contextuality Sensitive, arXiv:1803.07021.