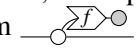
Graphical Algebraic Geometry

From Ideals and Varieties to Qudit ZH Completeness

Dichuan (David) Gao Razin A. Shaikh Aleks Kissinger

Algebraic geometry has proven useful in several fields in computer science, for example in robotics [1], computer vision [16], and cryptography [12]. Conversely, computational techniques have become influential in algebraic geometry with the advent of computer algebra systems [11]. Of particular interest to us is the use of algebraic geometry in quantum information theory. Algebraic geometry can be used to design classical codes with good asymptotic behavior [22, 4, 15, 26, 27], and these classical AG codes lift to quantum error correction (QEC) codes with equally good properties [2, 21, 13, 18, 17, 24, 25].

The ZH calculus natively supplies classical non-linearity [3]. In the qubit case, this means it supplies all classical boolean functions. In the qudit case, boolean functions become polynomials [23]. Thus there are maps of the form $n \xrightarrow{f} m$ in the ZH calculus, corresponding to componentwise-polynomial functions f of the computational basis. Maps of the form  are projectors onto the subspace spanned by basis elements that are roots of f. This suggests there is a "classical backbone" of ZH that reasons about affine varieties (solution sets of polynomials) over finite fields.

Classical algebraic structure inherent in quantum calculi is often best characterized by languages of the Graphical Linear Algebra (GLA) family. For example, the CSS codes resulting from classical $\mathbb{F}_2$-linear codes correspond to the phase-free fragment of the ZX calculus [19], which is picked out by the language of interacting bialgebras [6]. Similarly, the language of interacting Hopf algebras [7, 28] picks out the phase-free fragment of the qudit ZX calculus, which models the linear-relational core of qudit computation. Expanding the algebraic structure from linear to affine algebra, the language of graphical affine algebra [5] picks out the phase-free ZX with a Pauli X gate, which is the affine-relational core of qubit computation [9]. Finally, the language of affine Lagrangian relations picks out the stabilizer fragment of the ZX calculus [10].

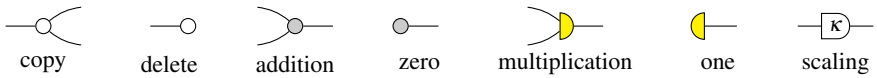
The motivating question of this paper is: can we extend GLA in a principled and simple way, to pick out the nonlinear "classical backbone" of the ZH calculus, corresponding to algebraic geometry over finite fields? If so, can we provide a sound and complete set of rewrite rules for that extension?

The answers to both questions turn out to be yes. We construct a diagrammatic language, which we call graphical algebraic geometry (GAG), for a span semantic of affine varieties over finite fields. We prove that it is universal, sound, and complete. Furthermore, we show the intimate connection between GAG and the Galois-Qudit ZH calculus [23, 14]. Using a catalysis-style argument [20], we leverage the completeness of GAG to solve the open problem of finding a complete set of rewrite rules for the Galois-Qudit ZH calculus.

The Polynomial Fragment

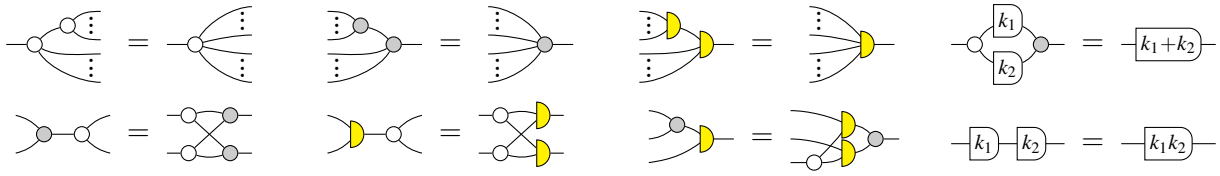
Throughout this project, we use the convention that p denotes a prime number, and $q = p^t$ is some natural number power of p, and $\mathbb{F}_q$ denotes the finite field of size q.

Our first step is to construct a PROP with polynomials as its morphisms. Consider the Lawvere theory $\mathbb{L}_{\mathsf{CAlg}_q}$ of commutative algebras over a finite field $\mathbb{F}_q$, which is generated by the following operations:

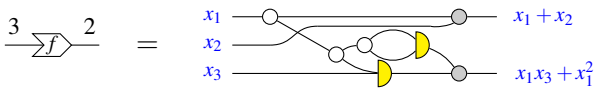


for all $\kappa \in \mathbb{F}_q$

modulo the usual axioms of commutative algebras, an extract of which is given below:



Morphisms of a Lawvere theory are (dually) homomorphisms between the algebras of that theory that are free and finitely generated [8]. For $\mathbb{L}_{\mathsf{CAlg}_q}$, a morphism is just a tuple of polynomials over $\mathbb{F}_q$. For example, for the polynomial tuple $f = (x_1 + x_2,\ x_1x_3 + x_1^2) \in (\mathbb{F}_q[x_1, x_2, x_3])^2$, we have



(1)

Structured Spans of Affine Varieties

In general, for a field k, a k-rational affine variety is (for our purposes) a subset of a space k^n carved out by some polynomial constraints:

$$V(f_1, \ldots, f_m)^{(k)} = \{\mathbf{x} \in k^n : f_1(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0\}. \tag{2}$$

If $V_1 \subset k^{n_1}, V_2 \subset k^{n_2}$ are affine varieties, a morphism $V_1 \to V_2$ is just a polynomial function $g \in (k[x_1, \ldots, x_{n_1}])^{n_2}$ such that $g(V_1) \subset V_2$. These form a category $\mathsf{AffVar}_k^{(k)}$. When k is finite, this category is equivalent to the category of finite sets: every subset of $\mathbb{F}_q^n$ is an affine variety; and every function between subsets is a polynomial mapping. However, treating these as algebraic constructs is crucial to our results.

On a variety $V(f_1, \ldots, f_m)^{(k)}$, any other polynomial f in the ideal generated by $f_1, \ldots, f_m$ also vanishes. Thus we think of varieties always as varieties *of ideals*.

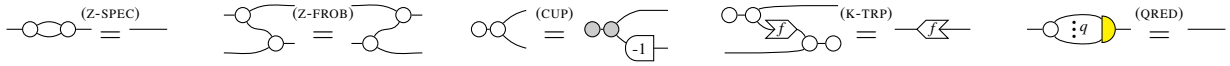
In particular, the spaces $\mathbb{F}_q^n$ themselves are trivial varieties $V(0)^{(\mathbb{F}_q)} = \mathbb{F}_q^n$. Let $G : \{\mathbb{F}_q^n : n \in \mathbb{N}\} \hookrightarrow \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ be the inclusion of these among all $\mathbb{F}_q$-rational varieties. A G-structured span of affine varieties is a diagram in $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ of the form $\mathbb{F}_q^n \leftarrow V \rightarrow \mathbb{F}_q^m$, modulo the usual notion of isomorphisms of spans.

These G-structured spans of affine varieties form a PROP ${}_G\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$, where composition is the usual composition of spans by pullback. This forms the target semantic of graphical algebraic geometry: the Lawvere theory $\mathbb{L}_{\mathsf{CAlg}_q}$ suffices as a language of the "forward-going" polynomials; we now seek a language for a span-semantic of polynomials.

Graphical Algebraic Geometry

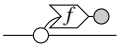
To create a graphical language for algebraic geometry over finite fields, we take the Lawvere theory $\mathbb{L}_{\mathsf{CAlg}_q}$, freely adjoin it to its own opposite, to obtain a self-dual PROP $\mathbb{L}_{\leftrightarrow} = \mathbb{L}_{CAlgq} + \mathbb{L}_{\mathsf{CAlg}_q}^{op}$. This has semantics in ${}_G\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$ by sending a polynomial $f \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$ to the "graph" span $(k^n = k^n \xrightarrow{f} k^m)$, and dually, to the "cograph" span $(k^m \xleftarrow{f} k^n = k^n)$.

We then find a set of rewrite rules E which tell us how generators of $\mathbb{L}_{CAlgq}$ and $\mathbb{L}_{CAlgq}^{op}$ should interact. We show an extract of E in below.

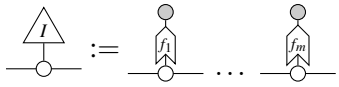


Here, f ranges over the generators of $\mathbb{L}_{\mathsf{CAlg}_q}$. This yields a the PROP $\mathbb{L}_{\mathrm{Span}_q} = \mathbb{L}_{\leftrightarrow}/E$. The rule set E is sound for our semantic, meaning that the functor $\mathbb{L}_{\leftrightarrow} \to_G \mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$ factors through $\mathbb{L}_{\mathrm{Span}_q}$, yielding a semantic functor $[-]_q : \mathbb{L}_{\mathrm{Span}_q} \to_G \mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$. Our main result is:

Theorem. *The semantic functor $[-]_q$ is well-defined as a PROP morphism, and fully faithful. In other words, $\mathbb{L}_{\mathrm{Span}_q}$ is a sound, universal, and complete language for ${}_G\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$.*

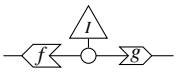
For any polynomial mapping $f \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$, we have in $\mathbb{L}_{\mathrm{Span}_q}$ diagrams of the form 

whose semantic is the span $\mathbb{F}_q^n \leftarrow V(f) \hookrightarrow \mathbb{F}_q^n$. These can be shown to respect the generation of ideals in the way we expect, so that we may safely speak of gadgets of the form



$$\left(\mathbb{F}_q^n \leftarrow V(I) \hookrightarrow \mathbb{F}_q^n\right) \tag{3}$$

where I is the ideal generated by $f_1, \ldots, f_m$. From these we may build diagrams in "span normal form"



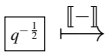
$$\overset{[-]_q}{\longmapsto} \quad \left(\mathbb{F}_q^m \xleftarrow{f} V(I) \xrightarrow{g} \mathbb{F}_q^{m'}\right) \tag{4}$$

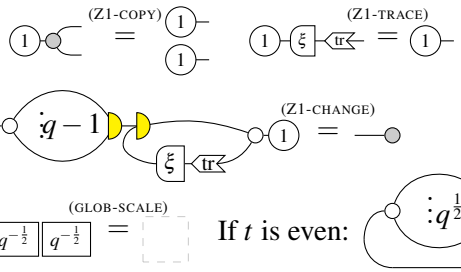
Thus all structured spans are expressible in our graphical language. Conversely, every diagram in $\mathbb{L}_{\mathrm{Span}_q}$ can be rewritten, using our rewrite rules, into span normal form. Completeness, then, is shown by demonstrating that two diagrams in span normal form, if they correspond to isomorphic spans, are rewriteable into each other.

Because $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ is secretly equivalent to FinSet, so our semantic category is in fact equivalent to ${}_G\mathrm{Span}(\mathsf{FinSet})$, which is in other words the category of $\mathbb{N}$-entried matrices of q-power dimensions. The (x,y)-th entry of a matrix corresponds to the number of points in the variety sitting above points $x \in \mathbb{F}_q^n$ and $y \in \mathbb{F}_q^m$. In this way the language $\mathbb{L}_{\mathrm{Span}_q}$ is also sound, universal, and complete for $\mathsf{Mat}_{\mathbb{N}}$.

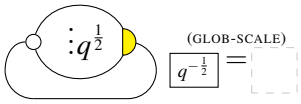
In general, the problem of rewriting two diagrams in $\mathbb{L}_{\mathrm{Span}_q}$ is #P-hard. This can be seen by the fact that determining the $\mathsf{Mat}_{\mathbb{N}}$ semantics of no-input-no-output diagrams in $\mathbb{L}_{\mathrm{Span}_q}$, where $q = 2$, is the same as solving a #SAT instance.

Completeness of the Qudit ZH Calculus

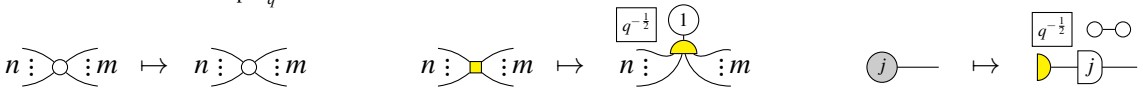
Now we show that the qudit ZH calculus [23, 14] can be obtained as a fairly minimal extension of $\mathbb{L}_{\mathrm{Span}_q}$. Consider the free dagger-PROP $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$ generated by $\mathbb{L}_{\mathrm{Span}_q}$ together with the additional generators:  $\sum_{i \in \mathbb{F}_q} \omega^{\mathrm{tr}(i)} |i\rangle$ and  $q^{-\frac{1}{2}}$, and the following additional rules:



(5)

If t is odd: If t is even: 

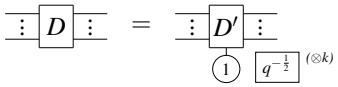
where $\mathrm{tr}(x) = x^p + \cdots + x^{p^t}$ is the field trace polynomial, and ξ is any element of $\mathbb{F}_q$ with $\mathrm{tr}(\xi) = 1$. This extension is sufficient to represent the entirety of the qudit ZH Calculus over $\mathbb{F}_q$. We illustrate by defining a functor $\iota_{\mathsf{ZH}} : \mathsf{ZH} \to \mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$ on the generators of ZH as follows:



Z spider H spider j-state

This functor is consistent with the matrix semantics of ZH and $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$. Thus, we choose $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$ as our axiomatization of ZH. First we show just how minimal an extension $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$ is over $\mathbb{L}_{\mathrm{Span}_q}$:

Proposition. *Any diagram D in $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$ factors into a diagram D' containing only the generators of $\mathbb{L}_{\mathrm{Span}_q}$ and a single* *, up to a finite scalar. In other words, the following rewrite holds in $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$:*



(6)

So a single copy of the state in the fourier basis is sufficient to extend the expressive power of $\mathbb{L}_{\mathrm{Span}_q}$ to cover the entirety of the qudit ZH Calculus. This allows us to apply a catalysis-style argument to obtain, from the completeness of $\mathbb{L}_{\mathrm{Span}_q}$:

Theorem (Completeness of Galois-Qudit ZH). *If D_1 and D_2 are diagrams in the Galois-Qudit ZH Calculus over $\mathbb{F}_q$, and $[\![D_1]\!] = [\![D_2]\!]$, then D_1 can be rewritten into D_2 using the rewrite rules of $\mathbb{L}_{\mathrm{Span}_q}^{\mathsf{Fourier}}$.*

References

[1] Amir Ali Ahmadi, Georgina Hall, Ameesh Makadia & Vikas Sindhwani (2017): *Geometry of 3D Environments and Sum of Squares Polynomials*, doi:10.48550/arXiv.1611.07369. Available at http://arxiv.org/abs/1611.07369. ArXiv:1611.07369 [math].

[2] A. Ashikhmin, S. Litsyn & M. A. Tsfasman (2001): *Asymptotically Good Quantum Codes*. *Physical Review A* 63(3), p. 032311, doi:10.1103/PhysRevA.63.032311. Available at http://arxiv.org/abs/quant-ph/0006061. ArXiv:quant-ph/0006061.

[3] Miriam Backens & Aleks Kissinger (2019): *ZH: A Complete Graphical Calculus for Quantum Computations Involving Classical Non-linearity*. *Electronic Proceedings in Theoretical Computer Science* 287, pp. 23–42, doi:10.4204/EPTCS.287.2. Available at http://arxiv.org/abs/1805.02175v2.

[4] Elwyn R. Berlekamp (1968): *Algebraic coding theory*, 1st ed edition. McGraw-Hill series in systems science, McGraw-Hill, New York.

[5] Filippo Bonchi, Robin Piedeleu, Pawel Sobocinski & Fabio Zanasi (2019): *Graphical Affine Algebra*. In: *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE, Vancouver, BC, Canada, pp. 1–12, doi:10.1109/LICS.2019.8785877. Available at https://ieeexplore.ieee.org/document/8785877/.

[6] Filippo Bonchi, Pawel Sobocinski & Fabio Zanasi (2014): *Interacting Bialgebras Are Frobenius*. In: *Foundations of Software Science and Computation Structures*, Springer, Berlin, Heidelberg, pp. 351–365, doi:10.1007/978-3-642-54830-7-23. Available at https://link.springer.com/chapter/10.1007/978-3-642-54830-7_23. ISSN: 1611-3349.

[7] Filippo Bonchi, Pawel Sobocinski & Fabio Zanasi (2017): *Interacting Hopf Algebras*. *Journal of Pure and Applied Algebra* 221(1), pp. 144–184, doi:10.1016/j.jpaa.2016.06.002. Available at http://arxiv.org/abs/1403.7048. ArXiv:1403.7048 [cs].

[8] Eugenia Cheng (2020): *Distributive laws for Lawvere theories*. *Compositionality* 2, p. 1, doi:10.32408/compositionality-2-1. Available at http://arxiv.org/abs/1112.3076. ArXiv:1112.3076 [math].

[9] Cole Comfort (2021): *Distributive Laws, Spans and the ZX-Calculus*, doi:10.48550/arXiv.2102.04386. Available at http://arxiv.org/abs/2102.04386. ArXiv:2102.04386 [math].

[10] Cole Comfort & Aleks Kissinger (2022): *A Graphical Calculus for Lagrangian Relations*. *Electronic Proceedings in Theoretical Computer Science* 372, pp. 338–351, doi:10.4204/EPTCS.372.24. Available at http://arxiv.org/abs/2105.06244. ArXiv:2105.06244 [cs].

[11] David A. Cox, John Little & Donal O'Shea (2015): *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics, Springer International Publishing, Cham, doi:10.1007/978-3-319-16721-3. Available at https://link.springer.com/10.1007/978-3-319-16721-3.

[12] Steven D. Galbraith (2012): *The mathematics of public key cryptography*, 1st ed. edition. Cambridge University Press, Cambridge ;.

[13] Carlos Galindo & Fernando Hernando (2015): *Quantum codes from affine variety codes and their subfield-subcodes*. *Designs, Codes and Cryptography* 76(1), pp. 89–100, doi:10.1007/s10623-014-0016-8. Available at http://arxiv.org/abs/1403.4060. ArXiv:1403.4060 [cs].

[14] Dichuan Gao (2024): *The Qudit ZH Calculus for Arbitrary Finite Fields: Universality and Application*, doi:10.48550/arXiv.2406.02219. Available at http://arxiv.org/abs/2406.02219. ArXiv:2406.02219 [quant-ph].

[15] V. D. Goppa (1981): *Codes on algebraic curves*. *Dokl. Akad. Nauk SSSR* 259(6), pp. 1289–1290.

[16] Richard Hartley & Andrew Zisserman (2004): *Multiple View Geometry in Computer Vision*. Cambridge University Press, Cambridge, UNITED KINGDOM. Available at http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=256634.

[17] Lingfei Jin (2014): *Quantum Stabilizer Codes from Maximal Curves*. *IEEE Transactions on Information Theory* 60(1), pp. 313–316, doi:10.1109/TIT.2013.2287694. Available at http://arxiv.org/abs/1311.2705. ArXiv:1311.2705 [cs].

[18] Lingfei Jin & Chaoping Xing (2013): *Euclidean and Hermitian Self-orthogonal Algebraic Geometry Codes and Their Application to Quantum Codes*, doi:10.48550/arXiv.1308.3575. Available at http://arxiv.org/abs/1308.3575. ArXiv:1308.3575 [cs].

[19] Aleks Kissinger (2022): *Phase-free ZX diagrams are CSS codes (...or how to graphically grok the surface code)*, doi:10.48550/arXiv.2204.14038. Available at http://arxiv.org/abs/2204.14038. ArXiv:2204.14038 [quant-ph].

[20] Aleks Kissinger, Neil J. Ross & John van de Wetering (2024): *Catalysing Completeness and Universality*. In: *Proceedings 21st International Conference on Quantum Physics and Logic (QPL)*, doi:10.48550/arXiv.2404.09915.

[21] Ryutaroh Matsumoto (2002): *Algebraic geometric construction of a quantum stabilizer code*. *IEEE Transactions on Information Theory* 48(7), pp. 2122–2124, doi:10.1109/TIT.2002.1013156. Available at http://arxiv.org/abs/quant-ph/0107129. ArXiv:quant-ph/0107129.

[22] I. S. Reed & G. Solomon (1960): *Polynomial Codes Over Certain Finite Fields*. *Society for Industrial and Applied Mathematics. Journal of the Society of Industrial and Applied Mathematics* 8(2), p. 5, doi:10.1137/0108018. Available at https://www.proquest.com/docview/915806723/citation/5084A7F7789946BBPQ/1. Num Pages: 5 Place: Philadelphia, United States Publisher: Society for Industrial and Applied Mathematics.

[23] Patrick Roy, John van de Wetering & Lia Yeh (2023): *The Qudit ZH-Calculus: Generalised Toffoli+Hadamard and Universality*. *Electronic Proceedings in Theoretical Computer Science* 384, pp. 142–170, doi:10.4204/EPTCS.384.9. Available at http://arxiv.org/abs/2307.10095. ArXiv:2307.10095 [quant-ph].

[24] Pradeep Kiran Sarvepalli & Andreas Klappenecker (2006): *Nonbinary Quantum Codes from Hermitian Curves*. In Marc P. C. Fossorier, Hideki Imai, Shu Lin & Alain Poli, editors: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer, Berlin, Heidelberg, pp. 136–143, doi:10.1007/11617983_13.

[25] Shaska (2008): *Quantum codes from algebraic curves with automorphisms*. *Condensed Matter Physics* 11(2), p. 383, doi:10.5488/CMP.11.2.383. Available at http://www.icmp.lviv.ua/journal/zbirnyk.54/016/abstract.html.

[26] M. A. Tsfasman, S. G. Vlădutx & Th. Zink (1982): *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*. *Mathematische Nachrichten* 109(1), pp. 21–28, doi:10.1002/mana.19821090103. Available at https://onlinelibrary.wiley.com/doi/10.1002/mana.19821090103.

[27] S. G. Vlâdut & V. G. Drinfel'd (1983): *Number of points of an algebraic curve*. *Functional Analysis and Its Applications* 17(1), pp. 53–54, doi:10.1007/BF01083182. Available at https://link.springer.com/article/10.1007/BF01083182. Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 1 Publisher: Kluwer Academic Publishers-Plenum Publishers.

[28] Fabio Zanasi (2018): *Interacting Hopf Algebras: the theory of linear systems*, doi:10.48550/arXiv.1805.03032. Available at http://arxiv.org/abs/1805.03032. ArXiv:1805.03032 [math].