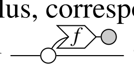
Graphical Algebraic Geometry

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.

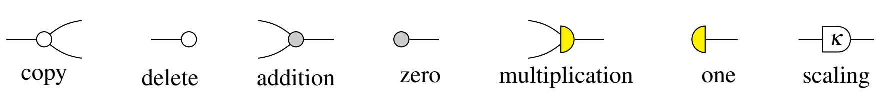
Classical algebraic structure inherent in quantum calculi is often best characterized by languages of the Graphical Linear Algebra (GLA) family. For example, the CSS codes resulting from classical $\mathbb{F}_2$-linear codes correspond to the phase-free fragment of the ZX calculus [19], which is picked 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.

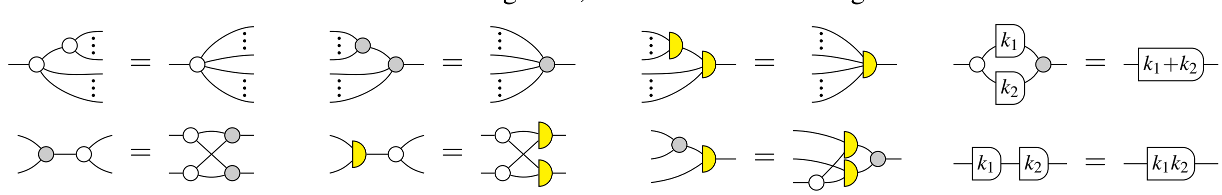
The Polynomial Fragment

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:

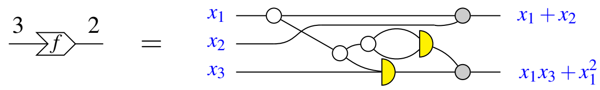


for all $\kappa \in \mathbb{F}_q$

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

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

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 $g \in (k[x_1,\dots,x_{n_1}])^{n_2}$ 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 $V(f_1,\dots,f_m)^{(k)}$, any other polynomial f in the ideal generated by $f_1,\dots,f_m$ also vanishes. Thus we think of varieties always as varieties *of ideals*.

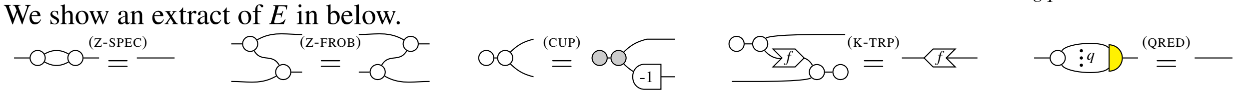
In particular, the spaces $\mathbb{F}_q^n$ themselves are trivial varieties $V(0)^{(\mathbb{F}_q)} = \mathbb{F}_q^n$. Let $G : \{\mathbb{F}_q^n : n \in \mathbb{N}\} \hookrightarrow \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ be the inclusion of these among all $\mathbb{F}_q$-rational varieties.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

These G-structured spans of affine varieties form a PROP ${}_G\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$, 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

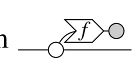
To create a graphical language for algebraic geometry over finite fields, we take the Lawvere theory $\mathbb{L}_{\mathsf{CAlg}_q}$, freely adjoin it to its own opposite, to obtain a self-dual PROP $\mathbb{L}_{\leftrightarrow} = \mathbb{L}_{CAlgq} + \mathbb{L}_{\mathsf{CAlg}_q}^{op}$. This has semantics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

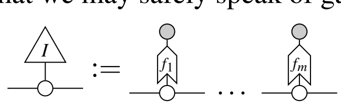
We then find a set of rewrite rules E which tell us how generators of $\mathbb{L}_{CAlgq}$ and $\mathbb{L}_{CAlgq}^{op}$ should interact. We show an extract of E in below.



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

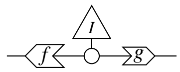
Theorem. *The semantic functor $[-]_q$ is well-defined as a PROP morphism, and fully faithful. In other words, $\mathbb{L}_{\mathsf{Span}_q}$ is a sound, universal, and complete language for ${}_G\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$.*

For any polynomial mapping $f \in (\mathbb{F}_q[x_1,\dots,x_n])^m$, we have in $\mathbb{L}_{\mathsf{Span}_q}$ diagrams of the form  whose semantic is the span $\mathbb{F}_q^n \hookleftarrow V(f) \hookrightarrow \mathbb{F}_q^n$. 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



$\xmapsto{[-]_q} \quad (\mathbb{F}_q^n \hookleftarrow V(I) \hookrightarrow \mathbb{F}_q^n)$ (3)

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



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

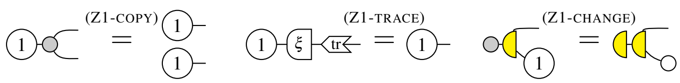
Thus all structured spans are expressible in our graphical language. Conversely, every diagram in $\mathbb{L}_{\mathsf{Span}_q}$ can be rewritten, using our rewrite rules, into span normal form. Completeness, then, is shown by demonstrating that two diagrams in span normal form, if they correspond to 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 ${}_G\mathsf{Span}(\mathsf{FinSet})$, which is in other words the category of $\mathbb{N}$-entried matrices of q-power dimensions. The xyth 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 $\mathbb{L}_{\mathsf{Span}_q}$ is also sound, universal, and complete for $\mathsf{Mat}_{\mathbb{N}}$.

In general, the problem of rewriting two diagrams in $\mathbb{L}_{\mathsf{Span}_q}$ 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 $\mathbb{L}_{\mathsf{Span}_q}$, where $q = 2$, is the same as solving a #SAT instance.

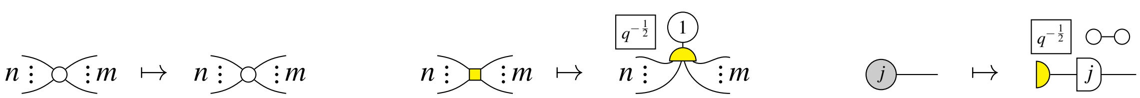
Completeness of the Qudit ZH Calculus

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



(5)

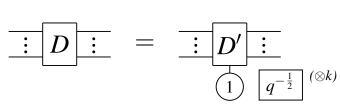
where $\mathrm{tr}(x) = x^p + \cdots + x^{p^t}$ is the field trace polynomial, and ξ is any element of $\mathbb{F}_q$ with $\mathrm{tr}(\xi) = 1$. This extension is sufficient to represent the entirety of the qudit ZH Calculus over $\mathbb{F}_q$. We illustrate by defining a functor $\iota_{\mathsf{ZH}}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



Z spider H spider j-state

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

Proposition. *Any diagram D in $\mathbb{L}_{\mathsf{Span}_q}^{\mathsf{Fourier}}$ factors into a diagram D' containing only the generators of $\mathbb{L}_{\mathsf{Span}_q}$ and a single* (1)—*, up to a finite scalar. In other words, the following rewrite holds in $\mathbb{L}_{\mathsf{Span}_q}^{\mathsf{Fourier}}$:*



(6)

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

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 $\mathbb{L}_{\mathsf{Span}_q}^{\mathsf{Fourier}}$.*

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].

Graphical Algebraic Geometry

From Ideals and Varieties to Qudit ZH Completeness

Dichuan (David) Gao
University of Oxford
Oxford, UK

Razin A. Shaikh
University of Oxford
Oxford, UK

Aleks Kissinger
University of Oxford
Oxford, UK

Abstract

We introduce *Graphical Algebraic Geometry* (GAG), a family of diagrammatic languages extending the Graphical Linear Algebra programme. We construct several languages within this family and prove that they are universal and complete for the corresponding (co)span semantics of commutative algebras and affine varieties. This framework provides clear graphical representations of algebraic structures — such as polynomials, ideals, and varieties — enabling intuitive yet rigorous diagrammatic reasoning.

We showcase two practical viewpoints on GAG. First, we show that instances of counting constraint satisfaction problem (#CSP) are recast as rewrite problems of closed diagrams in GAG. This means that deciding rewriteability in GAG is #P-hard, and GAG can be viewed as a complete and compositional rewrite system for networks of polynomial constraints. Second, we characterize the qudit ZH calculus, a diagrammatic language for quantum computation, as an extension of Graphical Algebraic Geometry. This establishes the correspondence that *Graphical Algebraic Geometry is to the ZH calculus what Graphical Linear Algebra is to the ZX calculus.* Using this construction, we show that computing amplitudes in qudit ZH requires only a constant number of queries to a GAG oracle. Finally, using a catalysis-style argument, we leverage the completeness of GAG to solve the open problem of finding a complete set of rewrite rules for the Qudit ZH calculus.

ACM Reference Format:
Dichuan (David) Gao, Razin A. Shaikh, and Aleks Kissinger. 2026. Graphical Algebraic Geometry From Ideals and Varieties to Qudit ZH Completeness. In *Proceedings of 41st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS).* ACM, New York, NY, USA, 31 pages.

1 Introduction

Algebraic geometry in computer science. Algebraic geometry and commutative algebra have been important influences in several fields in computer science, for example in robotics [1], computer vision [36], and in cryptography [26]. In the converse direction, computational techniques have become influential in algebraic geometry with the advent of computer algebra systems [21].

Of particular interest to us is the use of commutative algebra and geometry in two related areas of research. The first, and perhaps more obvious one, is that of Constraint Satisfaction Problems (CSP) [65]. A CSP instance where constraints are given as polynomials is a problem about an algebraic variety. In particular, in the case where the domain of the CSP is a finite field $\mathbb{F}_q$, the corresponding #CSP instance [41] is to count $\mathbb{F}_q$-rational points in a variety defined by polynomial constraints — a classical and central problem in 20th century algebraic geometry [38, 68]. More recently, cryptographic proof systems such as SNARK and STARK have relied on algebraic techniques over finite fields heavily, demonstrating the continuing relevance of this approach [7, 33].

LICS, Lisbon, Portugal
2026.

The second area is quantum information theory. It has long been known that algebraic geometry can be used to design classical codes with good asymptotic behavior [8, 32, 35, 40, 61, 66, 67], and that via the CSS or stabilizer constructions these classical AG codes lift to quantum error correction (QEC) codes with equally good properties [2, 27, 42, 43, 56, 57, 63, 64]. Such codes also played a central role in the groundbreaking construction of a magic-state distillation protocol with constant overhead [69]. Aside from error correction, algebraic geometry has also served as a useful language for foundational areas of research such as quantum entanglement and quantum contextuality [16, 25, 29, 53, 58].

Graphical linear algebra and its friends. To systematically understand the role algebraic geometry can play in quantum information theory, we propose that graphical calculi would be useful. Graphical calculi are compositional diagrammatic languages based in category theory, equipped with formal "rewrite rules" with which one can manipulate diagrams rigorously as equational terms. They are usually designed to represent some family of physical phenomena or computational processes. For instance, the ZX calculus and its related calculi have become prominent as languages for representing quantum computational processes [14, 15, 22, 48, 49, 59].

When considering the classical algebraic structure inherent in quantum computing, we often encounter fragments of the quantum calculi that are best characterized by languages in the family called Graphical Linear Algebra (GLA) [10, 12, 70]. Broadly speaking, GLA consists of diagrammatic languages that have denotational semantics built from classical algebraic structure. On the semantic side, the GLA story begins with a category of classical maps: for example, the linear maps between $\mathbb{F}_2$ spaces. It then applies the (co)span or the (co)relation construction to that category to obtain a dagger-category. For example, $\mathbb{F}_2$ linear maps give rise to spans of $\mathbb{F}_2$ linear maps, or to $\mathbb{F}_2$ linear subsets. On the syntactic side, it builds a simple diagrammatic language with generators that have clear semantic interpretations, and rewrite rules that characterize denotational equivalence.

Languages in the graphical linear algebra family are excellent at picking out fragments of quantum computation that correspond to some given notion of a "classical-relational backbone". For example, the CSS codes resulting from classical $\mathbb{F}_2$-linear codes correspond to the phase-free fragment of the ZX calculus [46], which is picked out by the language of interacting bialgebras [10], the language that kickstarted the GLA literature. Similarly, the language of interacting Hopf algebras [12, 70] picks out the phase-free fragment of the qudit ZX calculus, which models the linear-relational core of qudit computation. Expanding our algebraic structure from linear to affine algebra, the language of graphical affine algebra [9] picks out the phase-free ZX with a Pauli X gate, which is the affine-relational core of qubit computation [17]. Finally the language of affine Lagrangian relations picks out the stabilizer fragment of the ZX calculus [19].

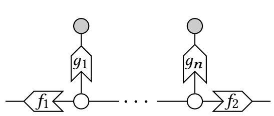
Of course, GLA has applications far beyond quantum computing. For instance, the language for linear relations over a field of rational functions $\mathbb{R}(x)$ models signal flow graphs and linear dynamical systems [6, 11, 24], while the language for affine relations models the fundamental structure of concurrency [9]. The strength of GLA lies in its ability to model a remarkably varied set of physical phenomena using the same formal structure.

The need for a graphical nonlinear algebra. However, existing versions of GLA are not yet sufficient to model the fragment of quantum computation with classical algebraic geometry as its "backbone"; nor can they reason about generic constraint satisfaction problems built on polynomial constraints. This is because commutative algebra involves a multiplication operator (an AND gate in the $\mathbb{F}_2$ case), which is essentially nonlinear (and non-affine for that matter). A graphical calculi that models classical algebraic geometry would need to supply such an operator, or equivalently, to supply the Toffoli gate.

In the realm of quantum computing, the ZH calculus [3, 4] or equivalently the ZX& calculus [17, 18] supply such a gate for the $\mathbb{F}_2$ case, and the Galois-qudit ZH calculus [28, 62] serves as the appropriate version in the nonbinary case. The motivating question of this paper is therefore: can we extend GLA in a principled and simple way, to pick out the nonlinear "classical backbone" of the ZH calculus, corresponding to classical algebraic geometry? If so, can we provide a sound and complete set of rewrite rules for that extension?

The solution: GCA and GAG. The answer is yes. However, unlike in the linear case, in which algebra and geometry coincide, we must deal with a gap between commutative algebra and algebraic geometry, which is bridged by a family of theorems known as the Nullstellensatze [30, 37, 39]. Therefore we construct our extension of GLA in two steps.

First, we develop a language $\mathbb{L}_{\mathrm{Cosp}}$, which we call graphical commutative algebra (GCA). Diagrams in $\mathbb{L}_{\mathrm{Cosp}}$ are built from gates corresponding to copying, addition, scaling, multiplication, and the units of these operators — the standard generators featured in the theory of commutative algebras. Diagrams can be reduced to a pseudonormal form that looks like



(1)

Denotational semantics are given as structured cospans of commutative algebras. In the pseudonormal form (1), the vertical wires denote a commutative algebra quotiented by the ideal $(g_1, \ldots, g_n)$, while f_1 and f_2 denote two algebra morphisms pointing into it. This captures the nonlinear *algebraic* backbone of quantum processes in ZH. Our first main result is a sound and complete rule set for $\mathbb{L}_{\mathrm{Cosp}}$ with respect to this cospan semantic.

Second, we develop languages $\mathbb{L}_{\mathrm{Span}_k}$ and $\mathbb{L}_{\mathrm{Span}_q}$, which we refer to as Graphical Algebraic Geometry (GAG) over algebraically closed fields and finite fields, respectively. Diagrams in these are built from the same generators as diagrams in $\mathbb{L}_{\mathrm{Cosp}}$, but they are subject to further rewrite rules that express the content of the Nullstellensatze. Denotational semantics are given respectively, as structured spans of affine varieties, and of $\mathbb{F}_q$-loci of varieties (or, equivalently, of finite sets). We still have the same pseudonormal form (1), but now the vertical wires with polynomials $g_1, \ldots, g_n$ denote an affine variety carved out by polynomial constraints, and f_1, f_2 are polynomial maps pointing out of it. This captures the nonlinear *geometric* backbone of quantum processes in ZH. Our second main result is that these languages are sound and complete with respect to their span semantics.

Our languages bear a clear relation to CSP instances with polynomial constraints. As will become clear, a diagram of the form g just *is* the CSP instance with constraints $g = 0$, while the diagram g is the #CSP problem of counting the number of points satisfying g. Our language, then, gives a compositional and complete rewrite system for networks of CSP instances with polynomial constraints. Through this view of GAG, we show that determining rewriteability of an arbitrary pair of GAG diagrams is #P-hard. In the special case where the field is $\mathbb{F}_2$, this just reduces to a compositional language for SAT instances. This serves as an algebraic elucidation of two ideas already present in the literature: first, that the ZX& calculus completely models "qubit multirelations" [18]; and second, that the ZH calculus can be used to model #SAT instances, and to reason about optimizations of #SAT algorithms [50, 51].

On the other hand, we justify our claim that *GAG is to ZH what GLA is to ZX* by characterizing the Galois-qudit ZH as an extension of GAG over finite fields. Indeed, we show that once we have access to the "classical backbone" carved out by GAG, any process in ZH can be built by consuming just a single basis state in the Fourier basis, up to a finite number of global scalars.

Outline of the paper. We begin in Section 2 by covering the requisite theoretical background on category theory and algebraic geometry. In Section 3, we discuss the Lawvere theory of commutative algebras, which serve as a building block (the "forward fragment") of our languages. We then construct the (co)span semantic categories of interest, namely, the structured cospan category of commutative algebras, and the structured span category of affine varieties, in Section 4. We prove our first main result in Section 5, where we construct the language $\mathbb{L}_{\mathrm{Cosp}}$ and prove its soundness and completeness for cospans of commutative algebras. The second main result is proven in Section 6, where we construct the languages $\mathbb{L}_{\mathrm{Span}_k}$ and $\mathbb{L}_{\mathrm{Span}_q}$, and prove their soundness and completeness for spans of affine varieties and of rational loci, respectively. In Section 7, we show that closed diagrams in GAG are equivalent to instances of #CSP, and therefore rewriting in GAG is #P-hard. In section 8 we show how the Galois-qudit ZH can be built as an extension of GAG. Finally, in Section 9, we prove the completeness of the qudit ZH calculus by catalysing the completeness of GAG.

2 Background

2.1 Diagrammatic Languages

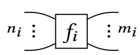
In this section we present the theory of PROPs as it relates to the construction of our diagrammatic languages. For a more in-depth and theoretical discussion of PROPs, we recommend the excellent note by Lack [52].

Definition 2.1. [55] A Product-and-Permutation-Category (PROP) is a strict symmetric monoidal category C with $Ob(C) \cong \mathbb{N}$, whose monoidal product on objects corresponds to addition of natural numbers.

A PROP morphism from C to $\mathcal{D}$ is strict symmetric monoidal functor such that $1_C \mapsto 1_{\mathcal{D}}$, or in other words, the objects are fixed. A PROP isomorphism is a PROP morphism that is fully faithful.

When we speak of a **presentation** of a PROP, we are speaking about a particular data structure, which we describe here with terminology adopted from the graphical linear algebra literature [12].

Definition 2.2. A **signature** is a set $S = \{f_i : n_i \to m_i\}_{i \in \mathcal{I}}$ where each element has a name, a number of inputs, and a number of outputs, and is pictured as a node in a string diagram:



A **diagrammatic term over a signature** S is an inductive structure constructed as in figure 1.

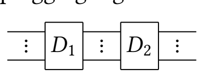
A **diagram** over S is an equivalence class of diagrammatic terms, where the equivalence relation is the one generated by the coherence axioms of strict symmetric monoidal categories, under the standard interpretation of string diagrams as morphisms in strict symmetric monoidal categories.

Definition 2.3. [12] A symmetric monoidal theory (SMT) is a pair of sets (S, E), where

- The set S is a signature, whose elements are also referred to as the generators or the spiders;
- The set $E = \{D_j \sim D'_j\}_{j \in \mathcal{J}}$ is a set of pairs of diagrams over S, where each pair relates two diagrams with the same numbers of inputs and outputs. These pairs are called the relations or rewrite rules;

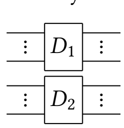
Definition 2.4. For any symmetric monoidal theory (S, E), there is a corresponding PROP $\langle S \rangle / E$, where:

- Morphisms from n to m are equivalence classes of diagrams over S with n input wires and m output wires, where the equivalence relation is the smallest one containing the axioms E while satisfying the laws of transitivity and substitution;
- Composition is plugging together of wires



(2)

- Monoidal product is side-by-side juxtaposition



(3)

Definition 2.5. An SMT (S, E) presents a PROP C if there is a PROP isomorphism $\langle S \rangle / E \cong C$.

Because a presentation, in this sense, lends itself to diagrammatic representation so naturally, we will use **diagrammatic language** for C as a synonym for a presentation of a C.

Often we have a concrete PROP C in mind (for example, the PROP Mat_R of finite matrices over a ring R), and we want to find a presentation for it. It is useful, then, to think of this as constructing a "syntax category" $\langle S \rangle / E$, and a "semantics functor" $[-] : \langle S \rangle / E \to C$. If $[-]$ is well-defined as a PROP morphism, we say that E is *sound* for C. If it is full, we say that S is *universal* for C. If it is faithful, we say that E is *complete* for C. If it is all three at the same time, then it is a PROP isomorphism, and so we have a genuine presentation of C.

The simplest useful examples of presentations of PROPs are Lawvere theories of well-behaved algebraic theories, which we now define.

Definition 2.6 (Lawvere Theory)**.** A Lawvere theory is a PROP $\mathbb{L}$ whose monoidal product is also its category-theoretical product, admitting a strictly identity-on-objects and product-preserving functor $\aleph_0 \to L$, where $\aleph_0$ is a skeleton of the category of finite sets and functions.

Intuitively, a Lawvere theory is a PROP equipped with a cartesian structure (of copying and deleting).

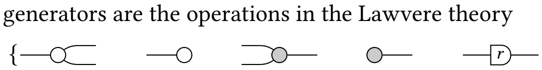
A model of a Lawvere theory $\mathbb{L}$ is a finite product preserving functor $\mathbb{L} \to \mathsf{Set}$. The models of a fixed Lawvere theory form a category $\mathsf{Mod}(\mathbb{L})$.

Proposition 2.7. *(Standard Fact on Lawvere Theories. See for example [13]) Let T be a monad on* Set *that is finitary (i.e. it preserves filtered colimits). Then there is a Lawvere theory $\mathbb{L}_T$, defined by the equational theory of T, such that*

$$\mathsf{Mod}(\mathbb{L}_T) \simeq \mathsf{Alg}(T) \tag{4}$$

where $\mathsf{Alg}(T)$ *denotes the Eilenberg-Moore category of T. Moreover, $\mathbb{L}_T$ is equivalent to the opposite of* $\mathrm{Kl}\,T|_{fin}$*, the Kleisli category of T restricted to finite objects.*

For instance, suppose we want to find a presentation for the category Mat_R of finite matrices over a ring R. Let T be the monad sending a set X to the free R-module generated by X. Then Mat_R is equivalent to the opposite of $\mathrm{Kl}\,T|_{fin}$. The Lawvere theory for finite-dimensional R modules is therefore equivalent to Mat_R. But the Lawvere theory is also, in itself, a neatly presented PROP: the generators are the operations in the Lawvere theory

{ 

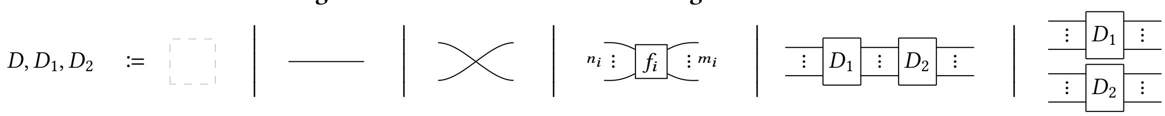
$\forall r \in R$}

(copy, delete, add, zero, scaling by r) and the rewrite rules are the usual axioms of R-modules. This yields a diagrammatic presentation of the PROP Mat_R, as we wanted.

However, in the GLA literature, the target PROP is usually more complicated than the Kleisli category of an algebraic monad. In particular, it usually has a dagger structure. Building presentations of such PROPs requires us to be able to synthesize larger PROPs out of smaller ones. The simplest way to do this is via PROP sum.

Definition 2.8. [70] Let C and $\mathcal{D}$ be PROPs. Their sum $C + \mathcal{D}$ is their coproduct in the category of PROPs.

Figure 1: Recursive Definition of Diagrammatic Terms



Proposition 2.9. *[70] If C has a presentation (S_1, E_1), and $\mathcal{D}$ has a presentation (S_2, E_2), then $C + \mathcal{D}$ has presentation $(S_1 \sqcup S_2, E_1 \sqcup E_2)$*

In the sum of PROPs, morphisms coming from two different PROPs of course do not interact. To endow interactive behaviour on morphisms of C and $\mathcal{D}$, we need the notion of distributive laws of PROPs.

Definition 2.10. A distributive law is a rewrite rule that distributes morphisms from the two different PROPs past each other:

$$\xrightarrow{f\in C}\xrightarrow{g\in\mathcal{D}} \quad\sim\quad \xrightarrow{g'\in\mathcal{D}}\xrightarrow{f'\in C}$$

If E is a collection of such rewrites, then $C +_E \mathcal{D}$ denotes the PROP presented by $(S_1 \sqcup S_2, E_1 \sqcup E_2 \sqcup E)$.

Note, this is not the traditional way in which distributive laws and their resulting categories are defined, but in the case where C and $\mathcal{D}$ admit presentations (which is the only case we encounter in this paper), this is in fact equivalent to the traditional definition [52].

2.2 Algebraic Geometry

In reviewing the basic algebraic geometry tools required for our purposes, we follow standard texts [20, 23, 37].

We denote by k an arbitrary field, and $\overline{k}$ its algebraic closure. Likewise we denote by $\mathbb{F}_q$ a finite field of size $q = p^n$ for some prime p, and $\overline{\mathbb{F}}_q$ its algebraic closure. The category of finitely generated commutative algebras over k is denoted $\mathsf{CAlg}_k^{\text{f.g.}}$.

2.2.1 Varieties and Polynomial Mappings.

Definition 2.11. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The **zero-set** of I is:

$$V(I) := \{\mathbf{a} \in \overline{k}^n \mid \forall f \in I, f(\mathbf{a}) = 0\} \tag{5}$$

An **affine variety** over k is any a zero-set of any ideal of polynomials.

For an intermediate field $k \subset k' \subset \overline{k}$, the k'-**rational locus** of a variety $V \subset \overline{k}^n$ is $V^{(k')} := V \cap (k')^n$; i.e. the set of points in V whose coordinates lie entirely in k'. When we say "a rational locus over k" without naming an intermediate field, we mean the k-rational locus of a variety over k.

Definition 2.12. Let S be any subset of $\overline{k}^n$. The set of k-polynomials vanishing on S is

$$I_k(S) := \{f \in k[x_1, \ldots, x_n] \mid \forall \mathbf{a} \in S, f(\mathbf{a}) = 0\}$$

It is easy to verify that this set of polynomials forms a radical ideal.

Definition 2.13. Let $V \subset \overline{k}^n$ and $W \subset \overline{k}^m$ be affine varieties over k. A function $\phi : V \to W$ is a k-**polynomial mapping** if there exists a polynomial tuple $f = (f_1, \ldots, f_m) \in (k[x_1, \ldots, x_n])^m$ such that

$$\phi(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$$

for all $(a_1, \ldots, a_n) \in V$. An **isomorphism of varieties** is a polynomial mapping σ which is invertible as a function, such that the inverse function σ^{-1} is itself a polynomial mapping.

The polynomial mappings from V to k forms a commutative algebra over k, called the **coordinate ring** of N, and denoted $k[V]$.

Proposition 2.14. *[20] Let V be an affine variety over k. Then*

$$k[V] \cong k[x_1, \ldots, x_n]/I_k(V).$$

Definition 2.15. (The Categories of Affine Varieties and Rational Loci) [20] For each fixed field k, the polynomial mappings between affine varieties over k forms a category AffVar_k. For each intermediate field $k \subset k' \subset \overline{k}$, there is a full subcategory $\mathsf{AffVar}_k^{(k')} \subset \mathsf{AffVar}_k$ consisting of affine varieties that are entirely k'-rational.

Proposition 2.16. *There is a fully faithful contravariant functor $k[-] : \mathsf{AffVar}_k^{op} \to \mathsf{CAlg}_k^{\text{f.g.}}$ sending an affine variety V to its coordinate ring $k[V]$.*

2.2.2 The Nullstellensatze.

Proposition 2.17 (Hilbert's Nullstellensatz)**.** *[37] Let k be an algebraically closed field, and $J \subset k[x_1, \ldots, x_n]$ an ideal. Then*

$$I_k(V(J)) = \sqrt{J} \tag{6}$$

Definition 2.18. A commutative algebra A over k is **reduced** if it has no nonzero nilpotents. The full subcategory of $\mathsf{CAlg}_k^{\text{f.g.}}$ consisting of reduced commutative algebras is denoted $\mathsf{CAlg}_k^{\text{f.g., red.}}$.

Proposition 2.19. *[23] The functor $(-)_{red} : \mathsf{CAlg}_k^{\text{f.g.}} \to \mathsf{CAlg}_k^{\text{f.g., red.}}$ sending $A \mapsto A/\mathrm{nil}\,A$ is the left-adjoint of the inclusion $\mathsf{CAlg}_k^{\text{f.g., red.}} \hookrightarrow \mathsf{CAlg}_k^{\text{f.g.}}$.*

Proposition 2.20. *[23] If k is an algebraically closed field, then the coordinate ring functor $k[-]$ gives an anti-equivalence of categories*

$$k[-] : \mathsf{AffVar}_k^{op} \simeq \mathsf{CAlg}_k^{\text{f.g., red.}}. \tag{7}$$

Denote its inverse functor (up to isomorphism) as

$$\mathrm{Spec} : \mathsf{CAlg}_k^{\text{f.g., red.}} \to \mathsf{AffVar}_k^{op} \tag{8}$$

We now turn our attention to the case of finite fields. Note: while affine varieties over algebraically closed fields are "rare" among the subsets of k^n, *any subset* of $\mathbb{F}_q^n$ is an affine variety over $\mathbb{F}_q$.

Proposition 2.21. *The category $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ of rational loci over $\mathbb{F}_q$ is equivalent to the category FinSet of finite sets and relations.*

Proof. It is well known [31, 54] that any subset of $\mathbb{F}_q^n$ is an affine variety, and any function between them is polynomial. $\square$

However our results are most easily read if we think in terms of polynomial constraints and morphisms, rather than subsets and functions. We retain the notation $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ as a reminder of this "attitude".

Proposition 2.22 (Finite Field Nullstellensatz). *Let $J \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be any ideal of polynomials over a finite field. Then*

$$I_{\mathbb{F}_q}(V^{(\mathbb{F}_q)}(J)) = J + \Gamma_q^n \tag{9}$$

where $\Gamma_q^n := (x_1^q - x_1, \ldots, x_n^q - x_n)$. [30]

Definition 2.23. For a finite field $\mathbb{F}_q$, a commutative algebra A over $\mathbb{F}_q$ is called q-**reduced**[1] if for every $f \in A$, $f^q = f$. The q-reduced algebras form a full subcategory $\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}} \subset \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}$.

Definition 2.24. For a finite field $\mathbb{F}_q$ and a finitely generated commutative algebra A over it, define its q-radical as the ideal generated as follows:

$$\Gamma_q(A) := (f^q - f : f \in A) \tag{10}$$

Remark 2.25. If $\{x_1, ..., x_n\}$ generate A over $\mathbb{F}_q$ then

$$\Gamma_q(A) = \Gamma_q^n = (x_1^q - x_1, \ldots, x_n^q - x_n). \tag{11}$$

Proposition 2.26. *The functor $(-)_{qred} : \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}} \to \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}}$ mapping $A \mapsto A/\Gamma_q(A)$ is left-adjoint to the inclusion.*

Proposition 2.27. *For a finite field $\mathbb{F}_q$, the coordinate ring functor $\mathbb{F}_q[-]$ restricted to the $\mathbb{F}_q$-rational loci defines an equivalence of categories*

$$\mathbb{F}_q[-] : \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)\,op} \simeq \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}} \tag{12}$$

Denote its inverse functor as Spec.

Proof. Because $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)} \simeq \mathsf{FinSet}$, so this is really just a non-binary version of the well known Stone duality between finite boolean algebras and finite sets [44]. The q-reduced commutative algebras over $\mathbb{F}_q$ correspond one-to-one with $\mathbb{F}_q$-valued functions out of finite sets, and $\mathbb{F}_q[-]$ sends a set to its algebra of $\mathbb{F}_q$-valued functions [54]. For a more algebraic perspective see also [34]. □

Notation. Denote the q-reduced free commutative algebras

$$\mathcal{R}_q^n := S_{\mathbb{F}_q}(n)/\Gamma_q^n, \tag{13}$$

and denote the full subcategory of $\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}$ consisting of such algebras as $\mathsf{Poly}_{\mathbb{F}_q}^{\text{qred.}}$, and F_q its inclusion functor.

3 The Polynomial Fragment

Consider the free-forgetful adjunction

$$\begin{tikzcd} \mathsf{Set} \arrow[r, bend left, "S_k"] \arrow[r, phantom, "\perp"] & \mathsf{CAlg}_k \arrow[l, bend left, "U"] \end{tikzcd}$$

On finite sets n, $S_k(n)$ is just the polynomial algebra $k[x_1, \ldots, x_n]$. Then let $T_k = U \circ S_k$ be the associated monad.

[1]This is our terminology. In finite field error correction literature this is just called "reduced" [30], but we need to avoid confusion with the aforementioned more standard notion of reduction from algebra.

Definition 3.1. Let Poly_k be the full subcategory of $\mathsf{CAlg}_k^{\text{f.g.}}$ given by the image of S_k restricted to finite sets. In other words, let Poly_k be the Kleisli category of T_k restricted to finite sets, corresponding to the polynomial algebras $k[x_1, \ldots, x_n]$.

Notation (Sharps and Flats). It is worth being careful about the equivalence between Poly_k and $\mathrm{Kl}\, T_k|_{fin}$, the Kleisli category of T_k restricted to finite objects. If $f \in (k[x_1, \ldots, x_n])^m$ is a tuple of polynomials, denote by $f^\#$ its unique extension to an algebra morphism $S_k(m) \to S_k(n)$. This acts on a polynomial $g(y_1, \ldots, y_m)$ by substituting y_j with $f_j(x_1, \ldots, x_n)$. Notice the contravariance implicit in this: algebra morphisms point and compose in the opposite direction than polynomials. Conversely, if $\varphi : S_k(m) \to S_k(n)$ is an algebra morphism, denote by $\varphi^\flat : m \to S_k(n)$ the corresponding tuple of polynomials defined by $\varphi_j^\flat = \varphi(x_j)$.

Recall from section 2.1 that for any finitary monad T, there is an equivalence $\mathrm{Kl}\, T|_{fin} \simeq \mathbb{L}_T^{op}$, where $\mathbb{L}_T$ denotes the Lawvere theory corresponding to T. In our case, the Lawvere theory is that of commutative algebras over k, which we denote $\mathbb{L}_{CAlg_k}$. Then:

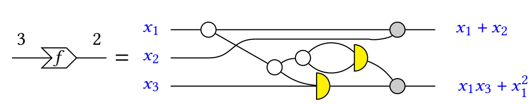
Proposition 3.2. *The generators and rewrite rules depicted in figure 2 form a presentation of the PROP $\mathbb{L}_{CAlg_k} \simeq \mathsf{Poly}_k^{op}$.*

Proof. This is the standard presentation of the Lawvere theory of commutative algebras over k, with the following interpretation for the diagrams: the white dots and are read as copying and its counit deleting, the grey dots and are read as adding and its unit zero, the yellow half-moons and are read as multiplication and its unit one, and the "squeeze" gadgets κ labelled by elements of k are read as the scaling operation by the field k on a k-commutative algebra. The rewrite rules of the Lawvere theory guarantee that each (finite variable) polynomial with coefficients in k can be expressed as a diagram in this language uniquely up to rewrites. □

Notation (Scalable Notation). We can now unambiguously introduce scalable notation for diagrams in $\mathbb{L}_{CAlg_k}$. For $n \in \mathbb{N}$ we define n-labelled wire and gates, as depicted in figure 3.

For every polynomial tuple $f \in (k[x_1, \ldots, x_n])^m$, we abbreviate the diagram (unique up to rewrites) that corresponds to $f^\#$ in $\mathbb{L}_{CAlg_k}$ as n f m.

For example, for the polynomial tuple $f = (x_1 + x_2,\ x_1x_3 + x_1^2) \in (k[x_1, x_2, x_3])^2$, we have



(14)

Notice that the contravariance between morphism composition and polynomial composition has been inherited by our diagrammatic language. Diagrammatically, everything is drawn in the direction of the Lawvere theory $\mathbb{L}_{CAlg_k}$. So n f m corresponds to a tuple of polynomials $(k[x_1, \ldots, x_n])^m$, which corresponds to a morphism $f^\# \in \mathsf{Poly}_k(m, n)$. The necessity for this will become clear in section 6 when we construct the language for spans of affine varieties.

Figure 2: The Theory $\mathbb{L}_{CAlg_K}$ of Commutative Algebras over k

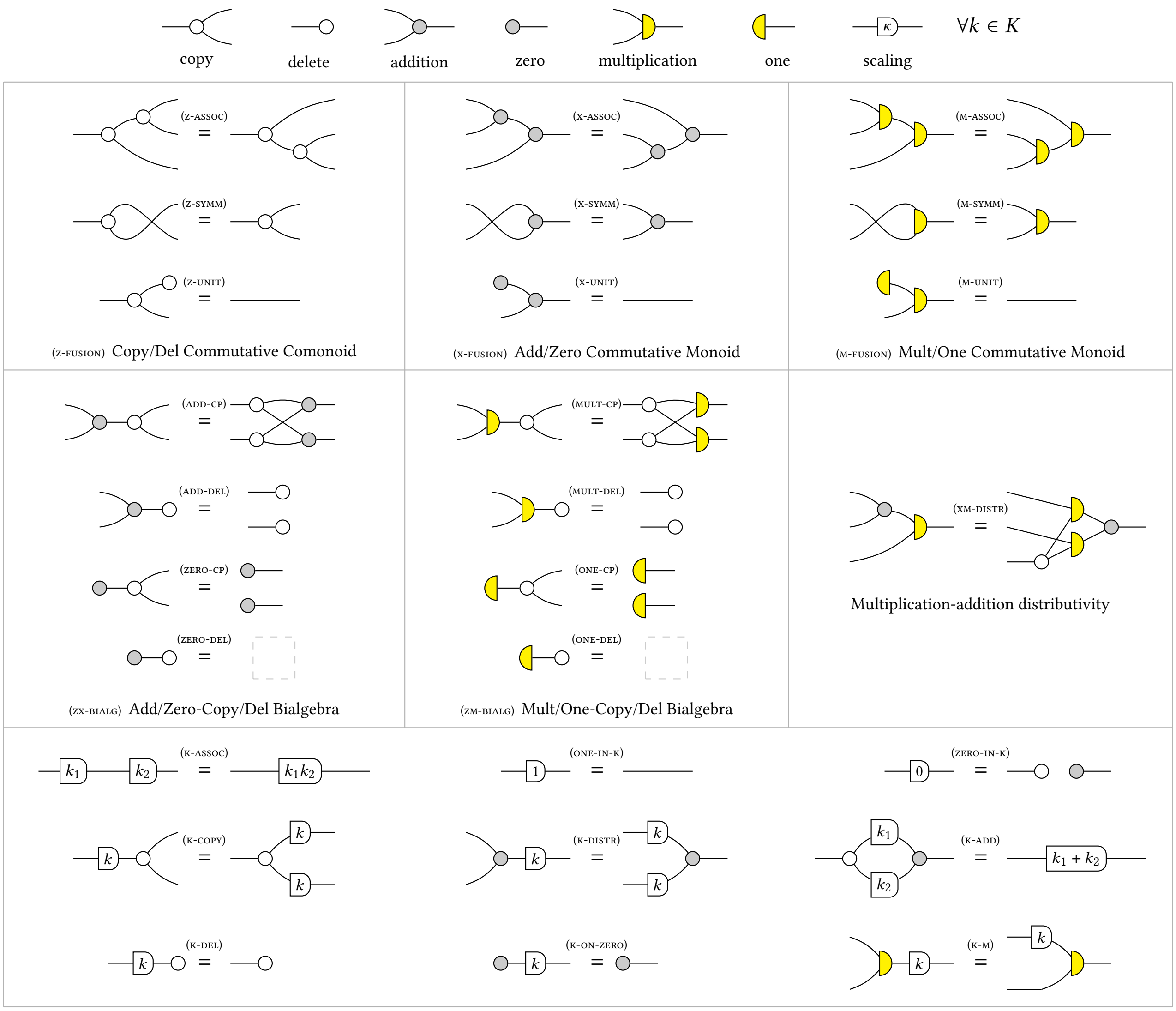
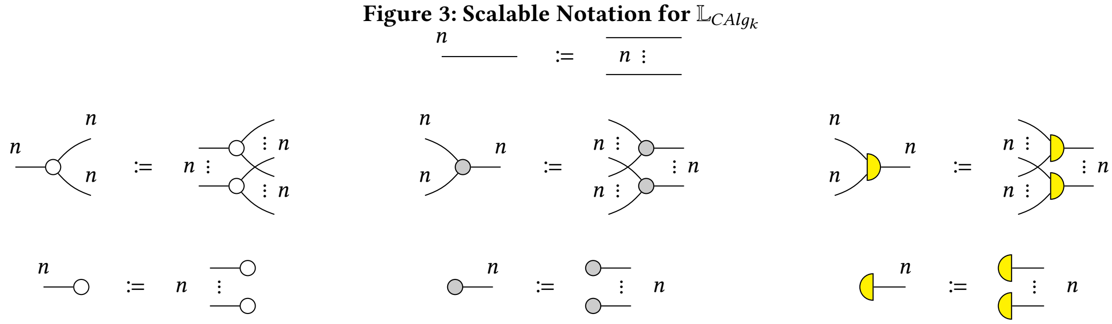


Figure 3: Scalable Notation for $\mathbb{L}_{CAlg_k}$



Proposition 3.3. *From the rewrite rules of $\mathbb{L}_{CAlg_k}$ it is possible to derive the rewrite rules about polynomials in the scalable notation, as depicted in figure 4.*

Proof. See appendix A. □

4 (Co)span Semantics

In this section we describe the target semantic categories of graphical commutative algebra and graphical algebraic geometry. We begin by recalling the definition of structured (co)spans, which is of particular importance here:

Definition 4.1. [5] Let $F : \mathcal{A} \to \mathcal{X}$ be a functor where $\mathcal{X}$ is a category with pullbacks. Define the bicategory of **structured spans** ${}_F\mathbf{Sp}(\mathcal{X})$: its objects are those of $\mathcal{A}$; its 1-cells are pairs of $\mathcal{X}$ morphisms of the form $FA \leftarrow S \to FB$ with $A, B \in \mathcal{A}$, which compose via pullback

$$\begin{tikzcd}
 & & S \times_{FB} T \arrow[dl] \arrow[dr] \arrow[dd, phantom, "\lrcorner" rotate=-45, very near start] & & \\
 & S \arrow[dl] \arrow[dr] & & T \arrow[dl] \arrow[dr] & \\
FA & & FB & & FC
\end{tikzcd}$$

and its 2-cells are commuting diagrams of the form

$$\begin{tikzcd}
 & S \arrow[dl] \arrow[dr] \arrow[dd] & \\
FA & & FB \\
 & S' \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Quotienting the categories of 1-cells of ${}_F\mathbf{Sp}(\mathcal{X})$ by the 2-isomorphisms, we obtain a 1-category ${}_F\,\mathrm{Span}(\mathcal{X})$, whose objects are those of $\mathcal{A}$, and morphisms are isomorphism classes of spans $FA \leftarrow S \to FB$.

For a functor $F : \mathcal{A} \to \mathcal{X}$ where $\mathcal{X}$ has pushouts, the bicategory of **structured cospans** ${}_F\mathbf{Csp}(\mathcal{X})$ and the 1-category ${}_F\,\mathrm{Cosp}(\mathcal{X})$ are defined dually to the above, with 1-cells of the form $FA \to S \leftarrow FB$ and composition given by pushout instead of pullback.

The following is an immediate well-known consequence of the dual nature of the definitions of structures cospans and spans:

Proposition 4.2. *If $F : \mathcal{A} \to \mathcal{X}$ is a functor and $\mathcal{X}$ has pullbacks, then $\mathcal{X}^{op}$ has pushouts, and there is an equivalence*

$$ {}_F\mathrm{Span}(\mathcal{X}) \simeq {}_{F^{op}}\,\mathrm{Cosp}(\mathcal{X}^{op}) \tag{15}$$

where $F^{op} : \mathcal{A}^{op} \to \mathcal{X}^{op}$ is the dual functor of F.

Definition 4.3. In the structured span construct, the category $\mathcal{A}$ embeds into ${}_F\,\mathrm{Span}(\mathcal{X})$ both covariantly by the graph embedding:

$$G_{\mathrm{Span}} : \quad \left(A \xrightarrow{f} B\right) \quad \mapsto \quad \left(FA = FA \xrightarrow{Ff} FB\right)$$

and contravariantly by the cograph embedding:

$$G^{op}_{\mathrm{Span}} : \quad \left(A \xrightarrow{f} B\right) \quad \mapsto \quad \left(FB \xleftarrow{Ff} FA = FA\right)$$

Similarly in the structured cospan construct, the category $\mathcal{A}$ embeds into ${}_F\,\mathrm{Cosp}(\mathcal{X})$ covariantly by the graph embedding:

$$G_{\mathrm{Cosp}} : \quad \left(A \xrightarrow{f} B\right) \quad \mapsto \quad \left(FA \xrightarrow{Ff} FB = FB\right)$$

and contravariantly by the cograph embedding:

$$G^{op}_{\mathrm{Cosp}} : \quad \left(A \xrightarrow{f} B\right) \quad \mapsto \quad \left(FB = FB \xleftarrow{Ff} FA\right)$$

The following are not new results, but are recalled here as we shall need it immediately.

Proposition 4.4. *For any field k, the category $\mathsf{CAlg}_k^{\text{f.g.}}$ of finitely-generated commutative algebras over k has pushouts.*

Proof. To construct the pushout: suppose $A = k[x_1, \ldots, x_n]/I_A$, $B = k[y_1, \ldots, y_m]/I_B$, $C = k[z_1, \ldots, z_r]/I_C$ with maps $A \xleftarrow{\phi} C \xrightarrow{\psi} B$. Then

$$A \otimes_C B = \frac{k[x_1, \ldots, x_n, y_1, \ldots, y_m]}{I_A + I_B + \sum_{i=1}^{r}(\phi(z_i) - \psi(z_i))} \tag{16}$$

Where, by a slight abuse of notation, I_A, I_B denote the images of I_A, I_B via the embeddings

$$k[x_1, \ldots, x_n] \hookrightarrow k[x_1, \ldots, x_n, y_1, \ldots, y_m] \hookleftarrow k[y_1, \ldots, y_m]$$

□

Corollary 4.5. *If k is either algebraically closed or finite, the category $\mathsf{AffVar}_k^{(k)}$ has pullbacks.*

Definition 4.6 (Semantic Category of Graphical Commutative Algebra)**.** Let $F : \mathsf{Poly}_k \hookrightarrow \mathsf{CAlg}_k^{\text{f.g.}}$ be the inclusion of the polynomial algebras into the finitely generated algebras. Then apply the structured cospans construction to obtain a category ${}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$. The objects of this category are polynomial algebras, and the morphisms are structured cospans of the form

$$S_k(n) \xrightarrow{f} A \xleftarrow{g} S_k(m) \tag{17}$$

where A is some finitely generated commutative algebra over k. Such a cospan is, in other words, a choice of n elements of A (corresponding to the left leg), and a choice of m elements of A (corresponding to the right leg). These cospans compose as usual by pushout.

Definition 4.7 (Semantic Category of Graphical Algebraic Geometry)**.** Let k be an algebraically closed field and $\mathbb{F}_q$ a finite field. Apply the structured span construction with respect to the inclusions of free spaces $k^n, \mathbb{F}_q^n$ into the respective categories of affine varieties to obtain categories ${}_G\,\mathrm{Span}(\mathsf{AffVar}_k)$ and ${}_{G_q}\,\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$. Morphisms in ${}_G\,\mathrm{Span}(\mathsf{AffVar}_k)$ are spans of polynomials maps $k^n \leftarrow V \to k^m$ where V is an affine variety.

Proposition 4.8. *The three semantic categories are PROPs.*

Proof. The objects of ${}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$ are the polynomial algebras $k[x_1, \ldots, x_n]$, the monoidal product on objects is $k[x_1, \ldots, x_n] \otimes k[y_1, \ldots, y_m] = k[x_1, \ldots, x_n, y_1, \ldots, y_m]$; and on morphisms by the tensor-product of algebra morphisms on both legs of the cospans.

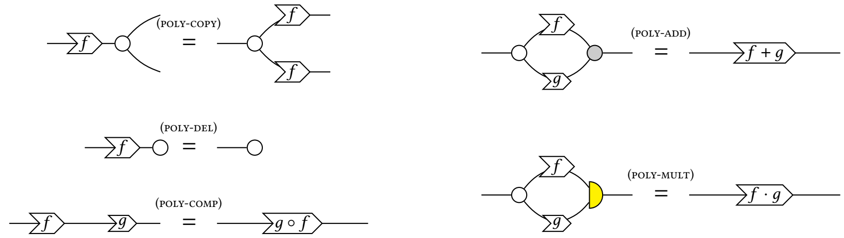
The braidings are given by the graphs of

$$\sigma : k[x_1, \ldots, x_n, y_1, \ldots, y_m] \to k[y_1, \ldots, y_m, x_1, \ldots, x_n] \tag{18}$$

The proofs for the other two categories are similar. □

The semantic categories for GCA and GAG are related, and we now explain this relation. The structured (co)span construction is "functorial":

Figure 4: Rules for Scalable Notation



Proposition 4.9. *[5] Given $F : \mathcal{A} \to \mathcal{X}$ and $F' : \mathcal{B} \to \mathcal{Y}$, with $\mathcal{X}, \mathcal{Y}$ both having pullbacks, if there is a commutative square of functors*

$$\begin{tikzcd} \mathcal{A} \arrow[r, "F"] \arrow[d, "\Phi"'] & \mathcal{X} \arrow[d, "\Psi"] \\ \mathcal{B} \arrow[r, "F'"'] & \mathcal{Y} \end{tikzcd}$$

and Ψ preserves pullbacks, then there is a functor

$$\mathrm{Span}(\Psi, \Phi) : {}_F\,\mathrm{Span}(\mathcal{X}) \to {}_{F'}\,\mathrm{Span}(\mathcal{Y}) \tag{19}$$

which sends the structured span $(FA_1 \xleftarrow{f} X \xrightarrow{g} FA_2)$ to a structured span in ${}_F\,\mathrm{Span}(\mathcal{Y})$ by hitting everything with Ψ. The dual statement is true for structured cospans.

Corollary 4.10. *In particular, in the situation of proposition 4.9, if Φ, Ψ are both equivalences of categories, then the induced functor ${}_F\,\mathrm{Span}(\mathcal{X}) \to {}_{F'}\,\mathrm{Span}(\mathcal{Y})$ is also an equivalence of categories.*

In particular, recall from proposition 2.26 that there are functors

$$\begin{aligned} (-)_{red} &: \mathsf{CAlg}_k^{\text{f.g.}} \to \mathsf{CAlg}_k^{\text{f.g., red.}} \\ (-)_{qred} &: \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}} \to \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}} \end{aligned} \tag{20}$$

each of which are left-adjoint to the inclusion in the opposite direction, and therefore they preserve pushouts. Moreover, they commute with the inclusions of the "free" algebras $F : \mathsf{Poly}_k \hookrightarrow \mathsf{CAlg}_k^{\text{f.g.}}$ and $F_q : \mathsf{Poly}_{\mathbb{F}_q}^{\text{qred.}} \hookrightarrow \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}$. The functoriality of the structured cospan construction (proposition 4.9) implies there are functors

$$\begin{aligned} {}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}}) &\xrightarrow{(-)_{red}} {}_F\,\mathrm{Cosp}\left(\mathsf{CAlg}_k^{\text{f.g., red.}}\right) \\ {}_F\,\mathrm{Cosp}(\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}) &\xrightarrow{(-)_{qred}} {}_{F_q}\,\mathrm{Cosp}\left(\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}}\right) \end{aligned} \tag{21}$$

Now recall that if k is algebraically closed, then there is an anti-equivalence (2.20)

$$\mathrm{Spec} : \mathsf{CAlg}_k^{\text{f.g., red.}} \simeq \mathsf{AffVar}_k^{op} \tag{22}$$

and if $\mathbb{F}_q$ is finite of size q, then there is an anti-equivalence (2.27)

$$\mathrm{Spec} : \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}} \simeq \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)^{op}} \tag{23}$$

Moreover, it is easy to check that these commute with the inclusions F, F_q, G, G_q in the obvious way. So using the duality between span and cospan (4.2) we obtain maps

$$\begin{aligned} {}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}}) &\xrightarrow{(-)_{red}} {}_F\,\mathrm{Cosp}\left(\mathsf{CAlg}_k^{\text{f.g., red.}}\right) \simeq {}_G\,\mathrm{Span}(\mathsf{AffVar}_k) \\ {}_F\,\mathrm{Cosp}(\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}) &\xrightarrow{(-)_{qred}} {}_{F_q}\,\mathrm{Cosp}\left(\mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}}\right) \simeq {}_{G_q}\,\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}) \end{aligned} \tag{24}$$

5 Graphical Commutative Algebra

We now work towards a diagrammatic presentation of the structured cospan category ${}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$. All lemmas, propositions, and theorems in this section are proven in appendix B, unless otherwise specified.

5.1 Defining the Calculus $\mathbb{L}_{\mathrm{Cosp}}$

Definition 5.1. Construct the PROP $\mathbb{L}_{\mathrm{Cosp}} = \mathbb{L}_{CAlg_k} +_E \mathbb{L}_{CAlg_k}^{op}$ where E is the set of rewrite rules displayed in figure 5. We supply this PROP with an intended semantic functor

$$[-] : \mathbb{L}_{\mathrm{Cosp}} \to_F \mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}}) \tag{25}$$

by mapping each generator in $\mathbb{L}_{CAlg_k}$ via the cograph embedding, and each generator in $\mathbb{L}_{CAlg_k}^{op}$ via the graph embedding.

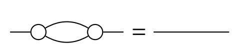
$$\begin{tikzcd} \mathbb{L}_{CAlg_k} \arrow[rr] \arrow[d] & & \mathsf{Poly}_k^{op} \arrow[dr, "G_{Csp}"] & \\ \mathbb{L}_{CAlg_k} + \mathbb{L}_{CAlg_k}^{op} \arrow[r, two heads] & \mathbb{L}_{CAlg_k} +_E \mathbb{L}_{CAlg_k}^{op} \arrow[rr, dashed, "{[-]}"] & & {}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}}) \\ \mathbb{L}_{CAlg_k}^{op} \arrow[rr] \arrow[u] & & \mathsf{Poly}_k \arrow[ur, "G_{Csp}^{op}"'] & \end{tikzcd}$$

We must first prove that the functor $[-]$ is well-defined, which is equivalent to the following statement:

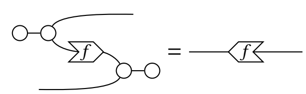
Proposition 5.2 (Cospan Soundness)**.** *Every rewrite rule in E is sound with respect to the intended semantic $[-]$.*

Once well-definedness has been established, we can now derive the following useful rewrite rules from the given rules:

Lemma 5.3. *The following are some useful derived rules of $\mathbb{L}_{\mathrm{Cosp}}$:*



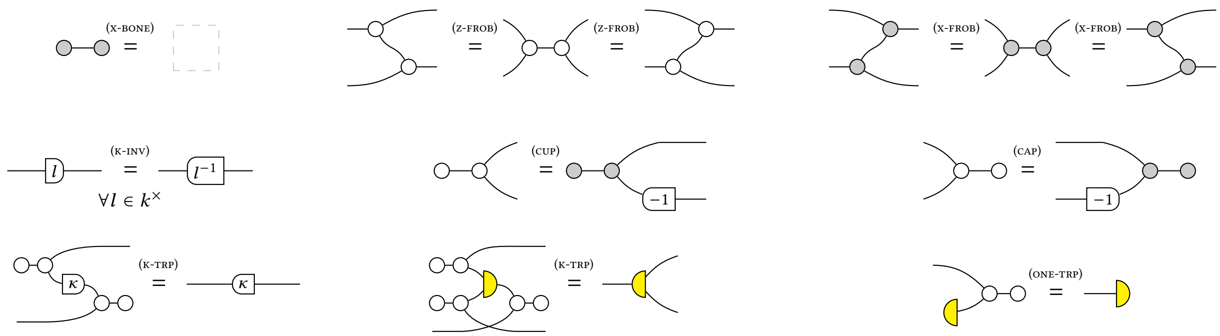
(special)



$\forall f \in (k[x_1, \ldots, x_n])^m$

(poly-trp)

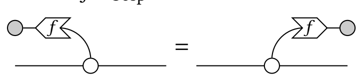
Figure 5: Additional Rewrite Rules for $\mathbb{L}_{\text{Cosp}}$

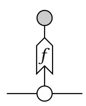


5.2 Universality and Completeness

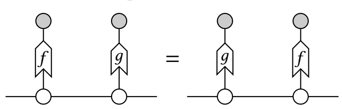
To consider the nature of the (essential) image of $[-]$ in ${}_F\,\mathsf{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$, we first prove the following sequence of lemmas in the language $\mathbb{L}_{\text{Cosp}}$, which will allow us to introduce an essential piece of syntactic sugar for summarizing a diagram.

Lemma 5.4. *For any $f \in k[x_1, \ldots, x_n]$, the following is deriveable from the rewrite rules of $\mathbb{L}_{\text{Cosp}}$:*

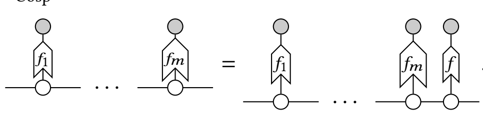


So we just speak of gadgets of the form 

Lemma 5.5. *For any $f, g \in k[x_1, \ldots, x_n]$, the following is deriveable from the rewrite rules of $\mathbb{L}_{\text{Cosp}}$:*

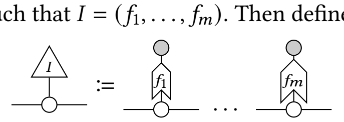


Lemma 5.6. *Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, and pick some f inside the ideal $(f_1, \ldots, f_m)$. Then the following is deriveable from the rewrite rules of $\mathbb{L}_{\text{Cosp}}$:*

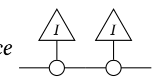
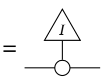
 (26)

Lemmas 5.5 and 5.6 mean that we can coherently define the following gadget:

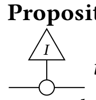
Definition 5.7. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Since $k[x_1, \ldots, x_n]$ is Noetherian [23], there exists a finite set of polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that $I = (f_1, \ldots, f_m)$. Then define

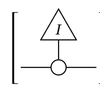
 (27)

Note that neither the choice of the basis $f_1, \ldots, f_m$, nor the ordering of them, matters in the definition, since any two such choices give diagrams which are rewriteable to each other per lemmas 5.5 and 5.6. For concreteness, we may always choose the reduced Grobner basis with respect to some chosen monomial ordering.

Corollary 5.8. *Idempotence*  =  *is provable in $\mathbb{L}_{\text{Cosp}}$.*

We now explain the semantics of these gadgets.

Proposition 5.9 (Quotient Gadgets). *The semantic of the gadget*  *is (any finite presentation of) the finitely generated commutative algebra defined by I. More precisely, if $I \subset k[x_1, \ldots, x_n]$ is any ideal, then*

 $= (S_k(n) \twoheadrightarrow S_k(n)/I \twoheadleftarrow S_k(n))$

where both legs are the canonical projections π_I against I.

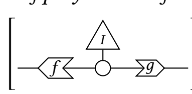
This is essentially what brings us from a language for Poly_k to a language that has full information about $\mathsf{CAlg}_k^{\text{f.g.}}$, which forces us to introduce the following notation:

Notation. If $A = S_k(n)/I$, and $f \in (k[x_1, \ldots, x_n])^m$, denote by $f_I^\# : S_k(m) \to A$ the algebra morphism one gets by passing to the quotient:

$$S_k(m) \xrightarrow{f^\#} S_k(n) \twoheadrightarrow S_k(n)/I = A \tag{28}$$

Or equivalently, the algebra morphism one gets by reducing f against I component-wise to obtain $f_I \in A^m$, and then taking its extension to an algebra morphism $f_I^\# : S_k(m) \to A$.

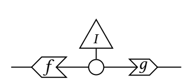
Proposition 5.10 (Cospan Universality). *For any ideal $I \subset k[x_1, \ldots, x_n]$ and tuples of polynomials $f \in (k[x_1, \ldots, x_n])^m$ and $g \in (k[x_1, \ldots, x_n])^{m'}$,*

 $= \left(S_k(m) \xrightarrow{f_I^\#} A \xleftarrow{g_I^\#} S_k(m')\right)$ (29)

where $A = S_k(n)/I$. Since every algebra morphism $S_k(m) \to A$ is equal to $f_I^\#$ for some f, so $[-] : \mathbb{L}_{\text{Cosp}} \to_F \mathsf{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$ is full.

It remains now to prove the completeness of the language $\mathbb{L}_{\text{Cosp}}$. We do this by reducing diagrams to a pseudo-normal form as follows:

Definition 5.11. A diagram D in $\mathbb{L}_{\text{Cosp}}$ is said to be in **cospan form** if it is draw as

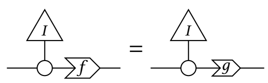
 (30)

for some ideal I and some polynomial tuples f, g.

Proposition 5.12 (Cospan Normal Form)**.** *Every diagram in $\mathbb{L}_{\text{Cosp}}$ can be rewritten into cospan form.*

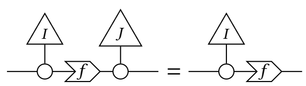
Thus, to show completeness of $\mathbb{L}_{\text{Cosp}}$, it suffices to show that, for any two diagrams in cospan form, if they have the same semantic in ${}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$, then they can be rewritten into each other. We do this via the following lemmas:

Lemma 5.13. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $f, g \in (k[x_1, \ldots, x_n])^m$ be any two polynomial tuples such that $f - g \in I^m$. That is, let f, g be such that $f_I^\# = g_I^\#$. Then the following diagram rewrite is derivable in $\mathbb{L}_{\text{Cosp}}$:*



(31)

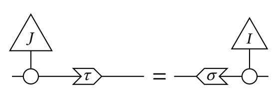
Lemma 5.14. *Suppose $I \subset S_k(n)$ and $J \subset S_k(m)$ are ideals of polynomials and $f \in (S_k(n))^m$. Suppose $f_I^\# : S_k(m) \to S_k(n)/I$ satisfies $J \subset \ker f_I^\#$. Then the following rewrite holds:*



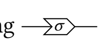
Lemma 5.15. *Suppose $I \subset S_k(n)$ and $J \subset S_k(m)$ are ideals, $\alpha : S_k(m)/J \to S_k(n)/I$ is an isomorphism of algebras, and $\sigma \in (k[x_1, \ldots, x_n])^m$, $\tau \in (k[y_1, \ldots, y_m])^n$ are a pair of polynomial tuples such that they represent α, α^{-1} respectively, i.e. such that the following commutes:*

$$\begin{tikzcd}
S_k(m) \arrow[r, two heads, "\pi_J"] \arrow[d, "\sigma^\#"'] & S_k(m)/J \arrow[d, shift left, "\alpha"] & S_k(m) \arrow[l, two heads, "\pi_J"'] \\
S_k(n) \arrow[r, two heads, "\pi_I"'] & S_k(n)/I \arrow[u, shift left, "\alpha^{-1}"] & S_k(n) \arrow[l, two heads, "\pi_I"] \arrow[u, "\tau^\#"']
\end{tikzcd}$$

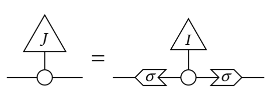
Then the following rewrite holds:



(32)

By composing  on the right to both sides of the equation in 5.15, we obtain:

Corollary 5.16. *If $\alpha : S_k(m)/J \to S_k(n)/I$ is an isomorphism of algebras, and $\sigma \in (k[x_1, \ldots, x_n])^m$ represents α as in lemma 5.15, then*



Lemmas 5.13, 5.14, and 5.15 suffice to show that any two diagrams in cospan normal form which have the same semantic in ${}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$ can be rewritten into each other. And therefore:

Proposition 5.17. *The functor $[-]$ is faithful. That is, $\mathbb{L}_{\text{Cosp}}$ is complete as a language for ${}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$.*

We have now completed the demonstration of our first main theorem:

Theorem 5.18. *The functor $[-] : \mathbb{L}_{\text{Cosp}} \to {}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$ is an isomorphism of PROPs. Thus $\mathbb{L}_{\text{Cosp}}$ is a sound, universal and complete language for ${}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$.*

Proof. Propositions 5.2, 5.10, and 5.17 together imply theorem 5.18. ◻

6 Graphical Algebraic Geometry

Our focus now turns from algebra to geometry. In this section k will always denote an algebraically closed field, and $\mathbb{F}_q$ will always denote a finite field of size q. All proofs are contained in appendix C unless otherwise specified.

Recall from equation 24 that there are two functors

$$\begin{gathered}
{}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}}) \xrightarrow{\mathrm{Spec}(-)_{red}} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k) \\
{}_F\,\mathrm{Cosp}(\mathrm{CAlg}_{\mathbb{F}_q}^{\text{f.g.}}) \xrightarrow{\mathrm{Spec}(-)_{qred}} {}_{G_q}\,\mathrm{Span}(\mathrm{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})
\end{gathered} \tag{33}$$

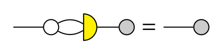
We now seek diagrammatic presentations for ${}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$ and ${}_{G_q}\,\mathrm{Span}(\mathrm{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$. Since we already have a presentation $\mathbb{L}_{\text{Cosp}} \cong_F \mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$, so we seek to find $\mathbb{L}_{\text{Span}_k}$ and $\mathbb{L}_{\text{Span}_q}$ that fit into the following commutative diagrams:

$$\begin{tikzcd}
\mathbb{L}_{\text{Cosp}} \arrow[r, "{[-]}"] \arrow[d, dashed, two heads] & {}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}}) \arrow[d, "\mathrm{Spec}(-)_{red}"] \\
\mathbb{L}_{\text{Span}_k} \arrow[r, dashed, "{[-]_k}"'] & {}_G\,\mathrm{Span}(\mathrm{AffVar}_k)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{L}_{\text{Cosp}} \arrow[r, "{[-]}"] \arrow[d, dashed, two heads] & {}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}}) \arrow[d, "\mathrm{Spec}(-)_{qred}"] \\
\mathbb{L}_{\text{Span}_q} \arrow[r, dashed, "{[-]_q}"'] & {}_{G_q}\,\mathrm{Span}(\mathrm{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})
\end{tikzcd}$$

such that $[-]_k$ and $[-]_q$ are both isomorphisms of PROPs.

6.1 GAG over Algebraically Closed Fields

Definition 6.1. Let $\mathbb{L}_{\text{Span}_k}$ be the quotient of $\mathbb{L}_{\text{Cosp}}$ defined by the following additional rewrite rule:



(red)

Proposition 6.2. *The PROP morphism*

$$\mathbb{L}_{\text{Cosp}} \xrightarrow{\mathrm{Spec}[-]_{red}} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k) \tag{34}$$

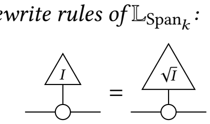
factors through $\mathbb{L}_{\text{Span}_k}$. In other words, rule (red) *is sound for affine varieties over an algebraically closed field.*

Thus we obtain a PROP morphism

$$\mathbb{L}_{\text{Span}_k} \xrightarrow{[-]_k} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k) \tag{35}$$

It remains to show that this morphism is faithful: in other words, that our rewrite rules are complete.

Lemma 6.3. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The following is deriveable from the rewrite rules of $\mathbb{L}_{\text{Span}_k}$:*



(36)

Proposition 6.4. *The semantic map $\mathbb{L}_{\text{Span}_k} \xrightarrow{[-]_k} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$ is faithful. In other words, $\mathbb{L}_{\text{Span}_k}$ is complete for ${}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$.*

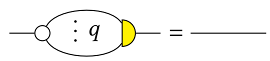
Since $[-]_k$ also inherits the fullness of $[-]$:

Theorem 6.5. *The semantic map $\mathbb{L}_{\text{Span}_k} \xrightarrow{[-]_k} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$ is an isomorphism of PROPs; $\mathbb{L}_{\text{Span}_k}$ is a universal, sound, and complete language for ${}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$.*

6.2 GAG over Finite Fields

The recipe for obtaining a language for spans of rational loci of affine varieties over finite fields is almost identical to the one used for spans of affine varieties over closed fields.

Definition 6.6. Let $\mathbb{L}_{\mathsf{Span}_q}$ be the quotient of $\mathbb{L}_{\mathsf{Cosp}}$ by the following additional rewrite rule:



(qred)

Proposition 6.7. *The PROP morphism*

$$\mathbb{L}_{\mathsf{Cosp}} \xrightarrow{\mathsf{Spec}[-]_{qred}} {}_{G_q}\,\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}) \tag{37}$$

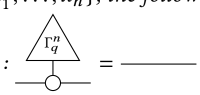
factors through $\mathbb{L}_{\mathsf{Span}_q}$. In other words, the rule qred is sound with respect to $\mathbb{F}_q$-rational loci.

Thus we obtain a PROP morphism

$$\mathbb{L}_{\mathsf{Span}_q} \xrightarrow{[-]_q} {}_{G_q}\,\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}) \tag{38}$$

Now to show that this morphism is faithful:

Lemma 6.8. *For $\Gamma_q^n = \{x_1^q, \ldots, x_n^q\}$, the following is deriveable from the rewrite rules of $\mathbb{L}_{\mathsf{Span}_q}$:*



Proposition 6.9. *The semantic map $[-]_q$ is faithful. In other words, the rules of $\mathbb{L}_{\mathsf{Span}_q}$ are complete.*

Theorem 6.10. *The semantic map $[-]_q$ is an isomorphism of PROPs.*

6.3 Matrix Semantics for GAG

Given a structured span of affine varieties over a field k (not necessarily algebraically closed) of the form $k^n \xleftarrow{\varphi} V \xrightarrow{\psi} k^m$ we can "repackage" the data of this structured span as an indexed family of affine varieties

$$V_{\mathbf{xy}} := \varphi^{-1}(\mathbf{x}) \cap \psi^{-1}(\mathbf{y}) \tag{39}$$

each of which is a subvariety of V.

In the particular case where $k = \mathbb{F}_q$ is a finite field, and V is an $\mathbb{F}_q$-rational locus, the family of affine varieties $V_{\mathbf{xy}}$ consists of finite sets, which we can view as entried in an $\mathbb{N}$-matrix:

Definition 6.11. Let $M_q : {}_{G_q}\,\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}) \to \mathsf{Mat}_{\mathbb{N}}$ be the functor which sends a structured span of $\mathbb{F}_q$-rational loci

$$\mathbb{F}_q^n \xleftarrow{\varphi} V \xrightarrow{\psi} \mathbb{F}_q^m \tag{40}$$

to the $q^n \times q^m$-matrix $M_q(\xleftarrow{\varphi}\xrightarrow{\psi})$ with entries

$$M_q(\xleftarrow{\varphi}\xrightarrow{\psi})_{\mathbf{xy}} = |\varphi^{-1}(\mathbf{x}) \cap \psi^{-1}(\mathbf{y})|. \tag{41}$$

The following is immediate (proofs are given in C.2):

Proposition 6.12. *The functor M_q is well-defined and fully faithful.*

Since $\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)} \simeq \mathsf{FinSet}$, this is just a restriction of the equivalence, well-known in folklore, between $\mathsf{Span}(\mathsf{FinSet}) \simeq \mathsf{Mat}_{\mathbb{N}}$ in disguise.

But since we already know that $\mathbb{L}_{\mathsf{Span}_q}$ is a sound, universal, and complete language for ${}_{G_q}\,\mathsf{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$ from section 6.2, so:

Corollary 6.13. *The diagrammatic language $\mathbb{L}_{\mathsf{Span}_q}$ serves as a sound, universal, and complete language for a full subcategory of $\mathsf{Mat}_{\mathbb{N}}$ consisting of the objects q^n with $n \in \mathbb{N}$.*

We use $[\![-]\!]_q : \mathbb{L}_{\mathsf{Span}_q} \to \mathsf{Mat}_{\mathbb{N}}$ to denote this new semantic.

7 From GAG to Counting CSP

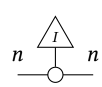
We now briefly illustrate the direct connection between GAG and CSP. Recall that a constraint satisfaction problem over a domain D and a constraint language Γ (typically a set of finite arity relations over D) is a pair $\langle X, C\rangle$, where:

- X is a set of variables $x_1, \ldots, x_n$,
- $C = \{C_1, \ldots, C_m\}$ is a set of constraints, each of which is a pair $C_j = \langle s_j, g_j\rangle$ where $s_j \subset X$ is the scope of the constraint, and $g_j \in \Gamma$ is the content of the constraint.

An assignment $\sigma : X \to D$ is said to satisfy the CSP if for every j, the tuple $(\sigma(x_i))_{i\in s_j}$ is in the relation g_j. The problem of determing whether there exists an assignment σ that satisfies $\langle X, C\rangle$ is called the decision problem $\mathsf{CSP}(\Gamma)$; while the problem of counting the number of assignments that satisfy $\langle X, C\rangle$ is called the counting problem $\#\mathsf{CSP}(\Gamma)$.

Now suppose that our domain of values is a finite field $\mathbb{F}_q$, and our constraint language Γ consists of polynomial maps $g : \mathbb{F}_q^n \to \mathbb{F}_q$, read as the requirement $g = 0$. Of course, every finite-arity relation over $\mathbb{F}_q$ can be expressed as an affine variety, and therefore our Γ is just the set of all relations over D. The finite field GAG gives an easy representation of instances of $\#\mathsf{CSP}(\Gamma)$ in the following way:

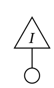
Proposition 7.1. *Let $\langle X, C\rangle$ be a CSP instance over the domain $\mathbb{F}_q$, with set of variables $X = \{x_1, \ldots, x_n\}$, and polynomial constraints $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$. Let I be the ideal generated by $g_1, \ldots, g_m$. Then the span semantic of the ideal gadget is*



$$\overset{[-]_q}{\mapsto} \left(\mathbb{F}_q^n \longleftrightarrow V(I)^{\mathbb{F}_q} \hookrightarrow \mathbb{F}_q^n\right) \tag{42}$$

where, recall, $V(I)^{\mathbb{F}_q} := \{\mathbf{x} \in \mathbb{F}_q^n : g_1(\mathbf{x}) = \cdots = g_j(\mathbf{x}) = 0\}$. In other words, it is the set of assignments satisfying $\langle X, C\rangle$.

The same diagram with no wires on either side has the following matrix semantic:



$$\overset{[\![-]\!]_q}{\mapsto} \left|V(I)^{(\mathbb{F}_q)}\right| \tag{43}$$

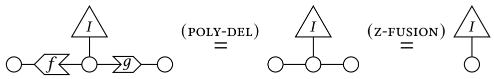
In other words, it is the number of assignments that satisfy $\langle X, C\rangle$.

Theorem 7.2. *The problem of rewriting arbitrary GAG diagrams into each other is #P-hard.*

Proof. This is a direct consequence of equation 43 in proposition 7.1, which shows that $\#\mathsf{CSP}(\Gamma)$ reduces to rewriting between a subset of diagrams in GAG, and $\#\mathsf{CSP}(\Gamma)$ is #P-complete [41]. □

Remark 7.3. In the case $q = 2$, polynomial constraints are equivalent to boolean constraints, and so $\#\mathsf{CSP}(\Gamma)$ is #SAT.

Remark 7.4. Conversely, since every diagram in GAG can be rewritten into cospan form, so every *closed* diagram (a diagram without input or output wires) can be rewritten into:



(44)

So determining the semantic of an arbitrary *closed* diagram in GAG is equivalent to $\#\mathrm{CSP}(\Gamma)$.

8 From GAG to Qudit ZH Calculus

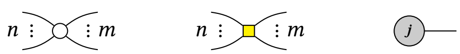
The ZH calculus is a graphical language for quantum computation, and it has a natural correspondence with the Toffoli-Hadamard gate set. In this section, we elucidate the connection between algebraic geometry and the ZH calculus. We review the Galois-Qudit ZH calculus introduced in [28] and show that the ZH calculus can be obtained as a fairly minimal extension of finite-field GAG: adding a single state and one scalar suffices to recover the ZH calculus in arbitrary dimension.

8.1 Qudit ZH Calculus

Here we give a brief overview of the qudit ZH Calculus as introduced in [28].

Definition 8.1. [45] A Galois-Qudit is a quantum system represented by a Hilbert space of dimension $q = p^t$ for some prime p and some natural number t, with a computational basis labelled as $|j\rangle$ with $j \in \mathbb{F}_q$.

For a finite field $\mathbb{F}_q$, the **Galois-Qudit ZH Calculus** over $\mathbb{F}_q$ is the free[2] dagger-PROP generated by three families of generators:

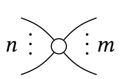


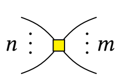
Z spider H spider j-state

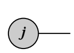
We will denote this free dagger-PROP as ZH. It admits a semantics functor to the PROP $q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]}$. A morphism from n to m in $q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]}$ is a matrix of the form $q^{\frac{k}{2}}A$, where A is a $q^m \times q^n$ matrix with entries in the ring $\mathbb{Z}[\omega]$, ω is a primitive pth root of 1, and k is an integer.

$$\mathsf{ZH} \xrightarrow{[\![-]\!]_{\mathsf{ZH}}} q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]} \tag{45}$$

This functor is full [28] and is defined on the generators as follows:


$$\mapsto \quad \sum_{i \in \mathbb{F}_q} |i\rangle^{\otimes m}\langle i|^{\otimes n}$$


$$\mapsto \quad \frac{1}{\sqrt{q}} \sum_{\substack{j_1,\dots,j_m \in \mathbb{F}_q \\ i_1,\dots,i_n \in \mathbb{F}_q}} \omega^{\mathrm{tr}(j_1 \dots j_m i_1 \dots i_n)} |j_1\rangle \dots |j_m\rangle\langle i_1| \dots \langle i_n|$$


$$\mapsto \quad \sqrt{q}|j\rangle \quad j \in \mathbb{F}_q$$

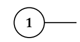
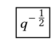
where $\mathrm{tr}(x) = x^p + \cdots + x^{p^t}$ is the field trace polynomial, which maps $\mathbb{F}_q \to \mathbb{F}_p$ linearly over $\mathbb{F}_p$.

[2] No complete set of rewrite rules are known for the qudit ZH. For the sake of full generality, we work with the free dagger-PROP generated by the ZH generators.

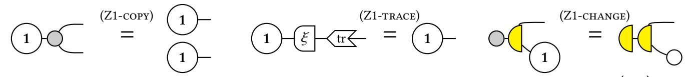
8.2 ZH Calculus as an Extension of GAG

We now extend the language $\mathbb{L}_{\mathsf{Span}_q}$ for finite field GAG to cover the entirety of the Galois-Qudit ZH Calculus over $\mathbb{F}_q$.

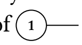
Definition 8.2. Define $\mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q}$ to be the PROP generated by $\mathbb{L}_{\mathsf{Span}_q}$ together with the following additional generators

  (46)

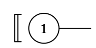
and the following additional rewrite rules

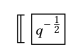


(47)

Where tr is the field trace polynomial and ξ is any element of $\mathbb{F}_q$ with $\mathrm{tr}\,\xi = 1$. Here, we think of  as a state in the Fourier basis as we define below.

Definition 8.3. We define the semantic functor $[\![-]\!]^{\mathsf{Fourier}}_q : \mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q} \to q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]}$. For each generator of $\mathbb{L}_{\mathsf{Span}_q}$, we set $[\![-]\!]^{\mathsf{Fourier}}_q$ to be the composition of $[\![-]\!]_q$ with the canonical inclusion $\mathrm{Mat}_{\mathbb{N}} \hookrightarrow q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]}$. For the additional generators, we define:


$$\Big[\!\Big[\ \cdot\ \Big]\!\Big]^{\mathsf{Fourier}}_q = \sum_{i \in \mathbb{F}_q} \omega^{\mathrm{tr}(i)}|i\rangle \tag{48}$$


$$\Big[\!\Big[\ \cdot\ \Big]\!\Big]^{\mathsf{Fourier}}_q = q^{-\frac{1}{2}} \tag{49}$$

This forces the following to commute:

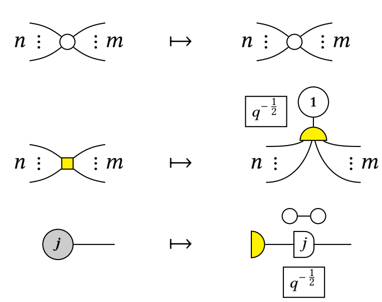
$$\begin{tikzcd}
\mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q} \arrow[r, "{[\![-]\!]^{\mathsf{Fourier}}_q}"] & q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]} \\
\mathbb{L}_{\mathsf{Span}_q} \arrow[u, hook] \arrow[r, "{[\![-]\!]_q}"'] & \mathrm{Mat}_{\mathbb{N}} \arrow[u, hook]
\end{tikzcd}$$

Moreover:

Proposition 8.4. *The rewrite rules in equation* (47) *are sound with respect to the semantics* $[\![-]\!]^{\mathsf{Fourier}}_q$.

The dagger-PROP $\mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q}$ covers the entirety of the Galois-Qudit ZH Calculus. To see this, we describe how its generators can be constructed in $\mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q}$ and show that the semantics agree.

Definition 8.5. We have the functor $\iota_{\mathsf{ZH}} : \mathsf{ZH} \to \mathbb{L}^{\mathsf{Fourier}}_{\mathsf{Span}_q}$ defined on the generators as follows:

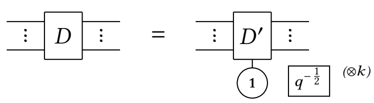


Proposition 8.6. *The functor ι_{ZH} is consistent with the semantics of the ZH Calculus. In other words, the following diagram commutes:*

$$\begin{tikzcd} \mathbb{L}^{\text{Fourier}}_{\text{Span}_q} \arrow[r, "{[\![-]\!]^{\text{Fourier}}_q}"] & q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]} \\ \mathsf{ZH} \arrow[u, "\iota_{\mathsf{ZH}}"] \arrow[ur, "{[\![-]\!]_{\mathsf{ZH}}}"'] & \end{tikzcd}$$

For the remainder of this paper we will use $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$ as a working notion of a Galois-Qudit ZH calculus *with rewrite rules* – we will show that the rewrite rules of $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$ forms a complete set of rules for ZH. Now, we show just how minimal an extension $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$ is over $\mathbb{L}_{\text{Span}_q}$:

Proposition 8.7. *For any diagram D in $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$, there exists $k \in \mathbb{N}$ and a diagram D' containing only the generators of $\mathbb{L}_{\text{Span}_q}$ such that*


(50)

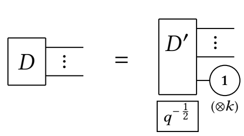
This shows that just a single copy of the state in the fourier basis is sufficient to extend the expressive power of finite-field GAG to cover the entirety of the Galois-Qudit ZH Calculus. Using this, we can compute amplitudes in the ZH calculus using finite-field GAG. Computing an amplitude in the ZH calculus corresponds to evaluating the semantics of a scalar diagram. We have the following result.

Theorem 8.8. *Let D be a scalar diagram in the ZH calculus over $\mathbb{F}_q$. The scalar $[\![D]\!]_{\mathsf{ZH}}$ can be computed using exactly q queries to an oracle O that evaluates the semantics of scalar diagrams in $\mathbb{L}_{\text{Span}_q}$.*

9 Catalyzing Qudit ZH Completeness

Theorem 9.1 (Completeness of Galois-Qudit ZH). *If D_1, D_2 are diagrams in the Galois-Qudit ZH Calculus over $\mathbb{F}_q$, and $[\![D_1]\!]_{\mathsf{ZH}} = [\![D_2]\!]_{\mathsf{ZH}}$, then D_1 can be rewritten into D_2 using the rewrite rules of $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$.*

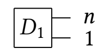
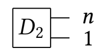
The first thing to notice is that to prove theorem 9.1, it suffices to prove it for states (diagrams without inputs) because any diagram, composed with cups, can be turned into a state, and vice-versa. Notice also that proposition 8.7 implies that a state in the ZH calculus can be rewritten into the form


(51)

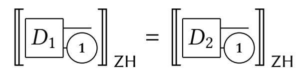
where D' is a diagram in the language $\mathbb{L}_{\text{Span}_q}$.

Our proof uses a catalysis-style argument [47]. We have a larger language (the Galois-qudit ZH) which extends a smaller language (the language $\mathbb{L}_{\text{Span}_q}$ of finite field GAG), in such a way that any diagram in ZH can be rewritten as a diagram in $\mathbb{L}_{\text{Span}_q}$, with some gadgets attached. Catalysis is about reducing the ZH semantic equality of D_1, D_2 to some form semantic equality statement between diagrams of $\mathbb{L}_{\text{Span}_q}$, involving subdiagrams of D_1, D_2. This allows us to leverage our knowledge that $\mathbb{L}_{\text{Span}_q}$ is complete for $\mathrm{Mat}_{\mathbb{N}}$ semantics, to derive the desired rewrites for D_1 and D_2 in ZH. In our case, the catalysis reduction is as follows:

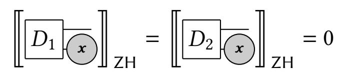
Proposition 9.2. *If*

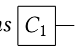
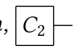
 *and* 

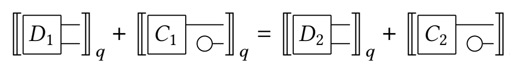
are diagrams in $\mathbb{L}_{\text{Span}_q}$, such that


(52)

and satisfying the following restriction condition: for all $x \in \mathbb{F}_q$ except for those lying on one line $\xi\mathbb{F}_p$ where ξ is some fixed element of field trace 1,

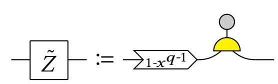

(53)

Then there exist diagrams  *n,*  *n in $\mathbb{L}_{\text{Span}_q}$ such that*

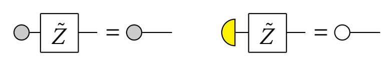

(54)

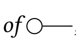
Notice that a semantic equality in ZH results not in an exact semantic equality in graphical algebraic geometry, but in an equality of sums. Luckily graphical algebraic geometry supplies the necessary gadgets for diagrammatically computing sums. This involves constructing so-called controlled-states for various diagrams in $\mathbb{L}_{\text{Span}_q}$, and then using those to construct sums.

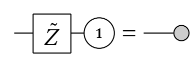
Lemma 9.3. *Let $\tilde{Z}$ be the following diagram in $\mathbb{L}_{\text{Span}_q}$:*

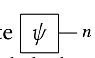

(55)

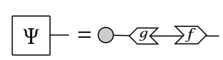
Then the following rewrites hold in $\mathbb{L}_{\text{Span}_q}$:

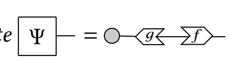
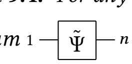

(56)

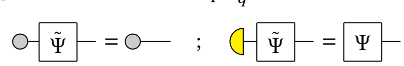
meaning that $\tilde{Z}$ serves as a controlled version of *; and moreover the following rewrite holds in $\mathbb{L}^{\text{Fourier}}_{\text{Span}_q}$:*


(57)

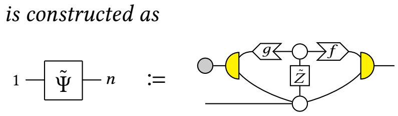
Now for any state  in $\mathbb{L}_{\text{Span}_q}$, recalling the (co)span normal form of graphical algebraic geometry (see (30)), ψ can be rewritten into the form


(58)

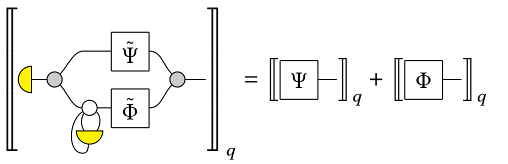
Lemma 9.4. *For any state*  *in $\mathbb{L}_{\text{Span}_q}$, there is a diagram*  *(the so-called* controlled state *of ψ) such that the following are rewriteable in $\mathbb{L}_{\text{Span}_q}$:*


(59)

Explicitly, $\tilde{\psi}$ is constructed as


(60)

Proposition 9.5. *For any states* $\boxed{\psi}\!-\!n$, $\boxed{\Phi}\!-\!n$ *in* $\mathbb{L}_{\mathrm{Span}_q}$, *let* $\tilde{\psi}, \tilde{\phi}$ *be their corresponding controlled states as defined in* (60). *Then the following diagram has the sum of* ψ *and* ϕ *as its semantics:*

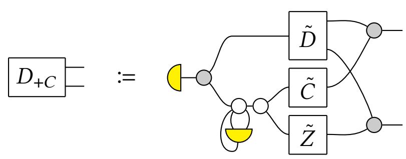

(61)

Now we return to the particular form of sums occurring in equation (70). Recall that in that sum, the second terms involve the factor ○—. Notice that

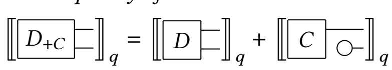
$$[\![\circ\!-\!(1)]\!]_q = \sum_{\theta \in \mathbb{F}_p} \omega^\theta = 0 \tag{62}$$

And so we might ask: are the rewrites of $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$ enough to detect that a sum of the form in equation (70) would lose its second term when plugged together with a —(1)? It turns out that this work is done by equation (57), which yields the following stronger form of proposition 9.5

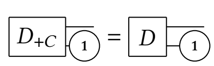
Proposition 9.6. *For diagrams* $\boxed{D}\!=\!n$, $\boxed{C}\!-\!n$ *in* $\mathbb{L}_{\mathrm{Span}_q}$, *letting*


(63)

where $\tilde{D}, \tilde{C}, \tilde{Z}$ *are the corresponding controlled diagrams, then the following semantic equality of sums holds:*

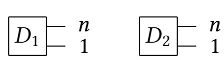

(64)

and moreover, the following rewrite holds in the language $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$*:*

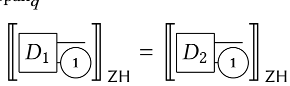

(65)

Which yields a catalysis argument for the completeness of the Galois-Qudit ZH Calculus up to global scalars:

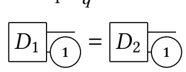
Proposition 9.7. *If*



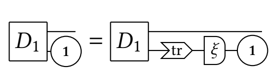
are diagrams in $\mathbb{L}_{\mathrm{Span}_q}$ *such that*


(66)

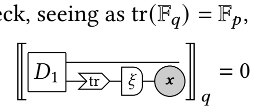
then the following holds in $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$*:*


(67)

Proof of proposition 9.7. First, since using rule (Z1-TRACE) we can rewrite

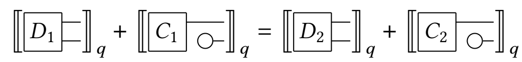

(68)

and it is easy to check, seeing as $\mathrm{tr}(\mathbb{F}_q) = \mathbb{F}_p$, that

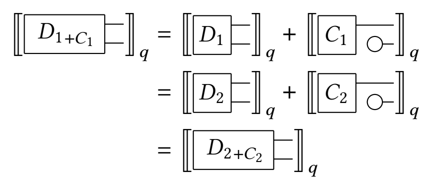

(69)

for any $x \notin \xi\mathbb{F}_p$. So, without loss of generality we may assume that D_1 satisfies the restriction condition (53). Similarly, the condition also holds for D_2.

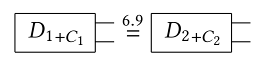
Proposition 9.2 then tells us that there exist diagrams $\boxed{C_1}\!-$, $\boxed{C_2}\!-$ in $\mathbb{L}_{\mathrm{Span}_q}$ such that


(70)

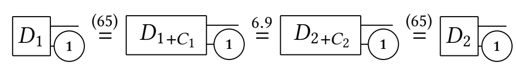
Then constructing D_{1+C_1}, D_{2+C_2} as in Proposition 9.6, we obtain diagrams in $\mathbb{L}_{\mathrm{Span}_q}$ such that


(71)

So by the completeness of graphical algebraic geometry (Proposition 6.9) we have rewrites in $\mathbb{L}_{\mathrm{Span}_q}$:


(72)

But then by the rewrite (65) given in proposition 9.6, we have rewrites


(73)

□

10 Conclusion and Future Directions

We have introduced a family of diagrammatic languages, which we refer to collectively as graphical algebraic geometry (GAG). This family of languages extends the existing literature on graphical linear algebra (GLA) by introducing the nonlinear multiplication operator. We construct three examples of languages within this family, and show that they are sound, universal, and complete, for their respective semantics in (co)spans of commutative algebras and affine varieties.

We showed that closed diagrams in GAG correspond exactly to counting constraint satisfaction problems, thereby showing that rewriting GAG diagrams into each other is #P-hard. We show also that GAG forms the nonlinear classical "backbone" of the Galois-qudit ZH calculus. Indeed, we show that all quantum processes in the qudit ZH calculus can be represented by consuming a single Fourier basis state, up to a finite number of scalars, meaning that a GAG oracle would be able to simulate the ZH processes with a constant number of queries. These connections serve to illustrate the potential versatility of GAG.

There are several directions of future work. On the theoretic side, there is an open question of constructing graphical algebraic geometry over $\mathbb{R}$. Indeed, for a real-closed field, one would be able to express inequality constraints of the form $g(x) \geq 0$ using the generators of GAG; but finding a complete set of rewrite rules for such languages may prove difficult, and will involve the Positivstellensatze. Such a language would have exciting applications in the verification of hybrid systems, where the safety space is often given as a semialgebraic set in $\mathbb{R}^n$, and dynamics are given by polynomial mappings [60]. On the practical side, there are two obvious directions. The first is to explore the connection between GAG and CSP: in particular, are their existing computational techniques that can optimize GAG rewriting, or bound the complexity of rewriting between diagrams of a certain class? The second is to use the characterization of ZH as an extension of GAG to “grok” quantum algebraic geometry codes, in the same way graphical linear algebra has been used to “grok” CSS codes [46].

References

[1] Amir Ali Ahmadi, Georgina Hall, Ameesh Makadia, and Vikas Sindhwani. 2017. Geometry of 3D Environments and Sum of Squares Polynomials. doi:10.48550/arXiv.1611.07369 arXiv:1611.07369 [math].

[2] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman. 2001. Asymptotically Good Quantum Codes. *Physical Review A* 63, 3 (Feb. 2001), 032311. doi:10.1103/PhysRevA.63.032311 arXiv:quant-ph/0006061.

[3] Miriam Backens and Aleks Kissinger. 2019. ZH: A Complete Graphical Calculus for Quantum Computations Involving Classical Non-linearity. *Electronic Proceedings in Theoretical Computer Science* 287 (Jan. 2019), 23–42. doi:10.4204/EPTCS.287.2

[4] Miriam Backens, Aleks Kissinger, Hector Miller-Bakewell, John van de Wetering, and Sal Wolffs. 2023. Completeness of the ZH-calculus. *Compositionality* 5 (July 2023), 5. doi:10.32408/compositionality-5-5 arXiv:2103.06610 [quant-ph].

[5] John C. Baez and Kenny Courser. 2020. Structured Cospans. doi:10.48550/arXiv.1911.04630 arXiv:1911.04630 [math].

[6] John C. Baez and Jason Erbele. 2015. Categories in Control. doi:10.48550/arXiv.1405.6881 arXiv:1405.6881 [math].

[7] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. Scalable, transparent, and post-quantum secure computational integrity. https://eprint.iacr.org/2018/046 Publication info: Preprint. MINOR revision..

[8] Elwyn R. Berlekamp. 1968. *Algebraic coding theory* (1st ed ed.). McGraw-Hill, New York.

[9] Filippo Bonchi, Robin Piedeleu, Pawel Sobocinski, and Fabio Zanasi. 2019. Graphical Affine Algebra. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, Vancouver, BC, Canada, 1–12. doi:10.1109/LICS.2019.8785877

[10] Filippo Bonchi, Pawel Sobocinski, and Fabio Zanasi. 2014. Interacting Bialgebras Are Frobenius. In *Foundations of Software Science and Computation Structures*. Springer, Berlin, Heidelberg, 351–365. doi:10.1007/978-3-642-54830-7-23 ISSN: 1611-3349.

[11] Filippo Bonchi, Pawel Sobocinski, and Fabio Zanasi. 2015. Full Abstraction for Signal Flow Graphs. In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL ’15)*. Association for Computing Machinery, New York, NY, USA, 515–526. doi:10.1145/2676726.2676993

[12] Filippo Bonchi, Pawel Sobocinski, and Fabio Zanasi. 2017. Interacting Hopf Algebras. *Journal of Pure and Applied Algebra* 221, 1 (Jan. 2017), 144–184. doi:10.1016/j.jpaa.2016.06.002 arXiv:1403.7048 [cs].

[13] Eugenia Cheng. 2020. Distributive laws for Lawvere theories. *Compositionality* 2 (May 2020), 1. doi:10.32408/compositionality-2-1 arXiv:1112.3076 [math].

[14] Bob Coecke and Ross Duncan. 2008. Interacting Quantum Observables. In *Automata, Languages and Programming (Lecture Notes in Computer Science)*, Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz (Eds.). Springer, Berlin, Heidelberg, 298–310. doi:10.1007/978-3-540-70583-3_25

[15] Bob Coecke and Aleks Kissinger. 2017. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning* (1 ed.). Cambridge University Press. doi:10.1017/9781316219317

[16] Valerie Coffman, Joydip Kundu, and William K. Wootters. 1999. Distributed Entanglement. doi:10.1103/PhysRevA.61.052306 arXiv:quant-ph/9907047.

[17] Cole Comfort. 2021. Distributive Laws, Spans and the ZX-Calculus. doi:10.48550/arXiv.2102.04386 arXiv:2102.04386 [math].

[18] Cole Comfort. 2021. The ZX&-calculus: A complete graphical calculus for classical circuits using spiders. *Electronic Proceedings in Theoretical Computer Science* 340 (Sept. 2021), 60–90. doi:10.4204/EPTCS.340.4 arXiv:2004.05287 [cs].

[19] Cole Comfort and Aleks Kissinger. 2022. A Graphical Calculus for Lagrangian Relations. *Electronic Proceedings in Theoretical Computer Science* 372 (Nov. 2022), 338–351. doi:10.4204/EPTCS.372.24 arXiv:2105.06244 [cs].

[20] David Cox, John Little, and Donal OSHEA. 2007. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra* (third edition ed.). Springer Nature, New York, NY. doi:10.1007/978-0-387-35651-8 ISSN: 0172-6056.

[21] David A. Cox, John Little, and Donal O’Shea. 2015. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer International Publishing, Cham. doi:10.1007/978-3-319-16721-3

[22] Niel de Beaudrap and Dominic Horsman. 2020. The ZX Calculus Is a Language for Surface Code Lattice Surgery. *Quantum* 4 (Jan. 2020), 218. doi:10.22331/q-2020-01-09-218

[23] David Eisenbud. 1995. *Commutative Algebra: with a View Toward Algebraic Geometry* (1st ed. 1995. ed.). Springer New York, New York, NY. doi:10.1007/978-1-4612-5350-1

[24] Brendan Fong, Paolo Rapisarda, and Paweł Sobociński. 2016. A categorical approach to open and interconnected dynamical systems. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*. 495–504. doi:10.1145/2933575.2934556 arXiv:1510.05076 [eess].

[25] Markus Frembs. 2024. An algebraic characterisation of Kochen-Specker contextuality. doi:10.48550/arXiv.2408.16764 arXiv:2408.16764 [quant-ph].

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

[27] Carlos Galindo and Fernando Hernando. 2015. Quantum codes from affine variety codes and their subfield-subcodes. *Designs, Codes and Cryptography* 76, 1 (July 2015), 89–100. doi:10.1007/s10623-014-0016-8 arXiv:1403.4060 [cs].

[28] Dichuan Gao. 2024. The Qudit ZH Calculus for Arbitrary Finite Fields: Universality and Application. doi:10.48550/arXiv.2406.02219 arXiv:2406.02219 [quant-ph].

[29] Masoud Gharahi. 2024. Classifying Entanglement by Algebraic Geometry. *International Journal of Quantum Information* 22, 03 (April 2024), 2350047. doi:10.1142/S0219749923500478 arXiv:2408.12265 [quant-ph].

[30] Sudhir Ghorpade. 2019. A note on Nullstellensatz over finite fields. In *Contemporary Mathematics*, Shrikrishna Dani, Surender Jain, Jugal Verma, and Meenakshi Wasadikar (Eds.). Vol. 738. American Mathematical Society, Providence, Rhode Island, 23–32. doi:10.1090/conm/738/14876

[31] D. G. Glynn and J. W. P. Hirschfeld. 1995. On the classification of geometric codes by polynomial functions. *Designs, Codes and Cryptography* 6, 3 (Nov. 1995), 189–204. doi:10.1007/BF01388474

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

[33] Jens Groth. 2016. On the Size of Pairing-Based Non-interactive Arguments. In *Advances in Cryptology – EUROCRYPT 2016*, Marc Fischlin and Jean-Sébastien Coron (Eds.). Springer, Berlin, Heidelberg, 305–326. doi:10.1007/978-3-662-49896-5_11

[34] A. Grothendieck. 1960. *Eléments de géométrie algébrique*. Presses Universitaires de Frane, Paris.

[35] V. Guruswami and M. Sudan. 1999. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory* 45, 6 (Sept. 1999), 1757–1767. doi:10.1109/18.782097

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

[37] Robin Hartshorne. 1977. *Algebraic Geometry*. Graduate Texts in Mathematics, Vol. 52. Springer New York, New York, NY. doi:10.1007/978-1-4757-3849-0

[38] Helmut Hasse. 1936. Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. 1936, 175 (Jan. 1936), 55–62. doi:10.1515/crll.1936.175.55

[39] David Hilbert. 1890. Ueber die Theorie der algebraischen Formen. *Math. Ann.* 36, 4 (Dec. 1890), 473–534. doi:10.1007/BF01208503

[40] T. Hoholdt and R. Pellikaan. 1995. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory* 41, 6 (Nov. 1995), 1589–1614. doi:10.1109/18.476214

[41] Mark Jerrum. 2017. Counting Constraint Satisfaction Problems. In *Dagstuhl Follow-Ups*, Andrei Krokhin and Stanislav Zivny (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 27 pages, 647864 bytes. doi:10.4230/DFU.VOL7.15301.205 Artwork Size: 27 pages, 647864 bytes.

[42] Lingfei Jin. 2014. Quantum Stabilizer Codes from Maximal Curves. *IEEE Transactions on Information Theory* 60, 1 (Jan. 2014), 313–316. doi:10.1109/TIT.2013.2287694 arXiv:1311.2705 [cs].

[43] Lingfei Jin and Chaoping Xing. 2013. Euclidean and Hermitian Self-orthogonal Algebraic Geometry Codes and Their Application to Quantum Codes. doi:10.48550/arXiv.1308.3575 arXiv:1308.3575 [cs].

[44] P. T. Johnstone. 1982. *Stone spaces*. University Press, Cambridge.

[45] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. 2005. Nonbinary stabilizer codes over finite fields. doi:10.48550/arXiv.quant-ph/0508070 arXiv:quant-ph/0508070.

[46] Aleks Kissinger. 2022. Phase-free ZX diagrams are CSS codes (...or how to graphically grok the surface code). doi:10.48550/arXiv.2204.14038 arXiv:2204.14038 [quant-ph].

[47] Aleks Kissinger, Neil J. Ross, and John van de Wetering. 2024. Catalysing Completeness and Universality. doi:10.48550/arXiv.2404.09915 arXiv:2404.09915 [quant-ph].

[48] Aleks Kissinger and John van de Wetering. 2020. Reducing T-count with the ZX-calculus. *Physical Review A* 102, 2 (Aug. 2020), 022406. arXiv:1903.10477 doi:10.1103/PhysRevA.102.022406

[49] Alexander Kissinger and John van de Wetering. 2024. *Picturing Quantum Software*.

[50] Tuomas Laakkonen, Konstantinos Meichanetzidis, and John van de Wetering. 2023. Picturing Counting Reductions with the ZH-Calculus. *Electronic Proceedings in Theoretical Computer Science* 384 (Aug. 2023), 89–113. doi:10.4204/EPTCS.384.6 arXiv:2304.02524 [cs].

[51] Tuomas Laakkonen, Konstantinos Meichanetzidis, and John van de Wetering. 2024. A Graphical #SAT Algorithm for Formulae with Small Clause Density. *Electronic Proceedings in Theoretical Computer Science* 406 (Aug. 2024), 137–161. doi:10.4204/EPTCS.406.7 arXiv:2212.08048 [cs].

[52] Stephen Lack. 2004. Composing PROPs. *Theory and Applications of Categories [electronic only]* 13 (2004), 147–163. http://eudml.org/doc/124613

[53] J. M. Landsberg and Laurent Manivel. 2003. On the ideals of secant varieties of Segre varieties. doi:10.48550/arXiv.math/0311388 arXiv:math/0311388.

[54] Rudolf Lidl. 1997. *Finite fields* (second edition. ed.). University Press, Cambridge.

[55] Saunders MacLane. 1965. Categorical algebra. *Bull. Amer. Math. Soc.* 71, 1 (Jan. 1965), 40–106. https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society/volume-71/issue-1/Categorical-algebra/bams/1183526392.full Publisher: American Mathematical Society.

[56] Ryutaroh Matsumoto. 2002. Algebraic geometric construction of a quantum stabilizer code. *IEEE Transactions on Information Theory* 48, 7 (July 2002), 2122–2124. doi:10.1109/TIT.2002.1013156 arXiv:quant-ph/0107129.

[57] R. Matsumoto. 2002. Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes. *IEEE Transactions on Information Theory* 48, 7 (July 2002), 2122–2124. doi:10.1109/TIT.2002.1013156

[58] Akimasa Miyake. 2003. Classification of multipartite entangled states by multidimensional determinants. *Physical Review A* 67, 1 (Jan. 2003), 012108. doi:10.1103/PhysRevA.67.012108 arXiv:quant-ph/0206111.

[59] Boldizsár Poór, Razin A. Shaikh, and Quanlong Wang. 2025. ZX-calculus Is Complete for Finite-Dimensional Hilbert Spaces. *Electronic Proceedings in Theoretical Computer Science* 426 (Aug. 2025), 127–158. doi:10.4204/eptcs.426.5

[60] Stephen Prajna and Ali Jadbabaie. 2004. Safety Verification of Hybrid Systems Using Barrier Certificates. In *Hybrid Systems: Computation and Control*, Rajeev Alur and George J. Pappas (Eds.). Springer, Berlin, Heidelberg, 477–492. doi:10.1007/978-3-540-24743-2_32

[61] I. S. Reed and 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 (June 1960), 5. doi:10.1137/0108018 Num Pages: 5 Place: Philadelphia, United States Publisher: Society for Industrial and Applied Mathematics.

[62] Patrick Roy, John van de Wetering, and Lia Yeh. 2023. The Qudit ZH-Calculus: Generalised Toffoli+Hadamard and Universality. *Electronic Proceedings in Theoretical Computer Science* 384 (Aug. 2023), 142–170. doi:10.4204/EPTCS.384.9 arXiv:2307.10095 [quant-ph].

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

[64] Shaska. 2008. Quantum codes from algebraic curves with automorphisms. *Condensed Matter Physics* 11, 2 (June 2008), 383. doi:10.5488/CMP.11.2.383

[65] Edward Tsang. 1993. *Foundations of constraint satisfaction.* Academic Press Limited, London, England ;.

[66] M. A. Tsfasman, S. G. Vlădutx, and Th. Zink. 1982. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten* 109, 1 (Jan. 1982), 21–28. doi:10.1002/mana.19821090103

[67] S. G. Vlâdut and V. G. Drinfel'd. 1983. Number of points of an algebraic curve. *Functional Analysis and Its Applications* 17, 1 (Jan. 1983), 53–54. doi:10.1007/BF01083182 Company: Springer Distributor: Springer Institution: Springer Label: Springer Number: 1 Publisher: Kluwer Academic Publishers-Plenum Publishers.

[68] André Weil. 1949. Numbers of solutions of equations in finite fields. *Bulletin (new series) of the American Mathematical Society* 55, 5 (1949), 497–508. doi:10.1090/S0002-9904-1949-09219-4

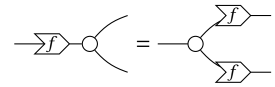
[69] Adam Wills, Min-Hsiu Hsieh, and Hayata Yamasaki. 2024. Constant-Overhead Magic State Distillation. doi:10.48550/arXiv.2408.07764 arXiv:2408.07764 [quant-ph].

[70] Fabio Zanasi. 2018. Interacting Hopf Algebras: the theory of linear systems. doi:10.48550/arXiv.1805.03032 arXiv:1805.03032 [math].

A Derived Rules for Scalable Notation in $\mathbb{L}_{CAlg_k}$

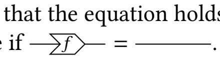
Proposition 3.3. *From the rewrite rules of $\mathbb{L}_{CAlg_k}$ it is possible to derive the rewrite rules about polynomials in the scalable notation, as depicted in figure 4.*

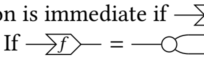
Proof. We begin by proving that rewrite rule (poly-copy)is derivable in $\mathbb{L}_{CAlg_k}$, that is,

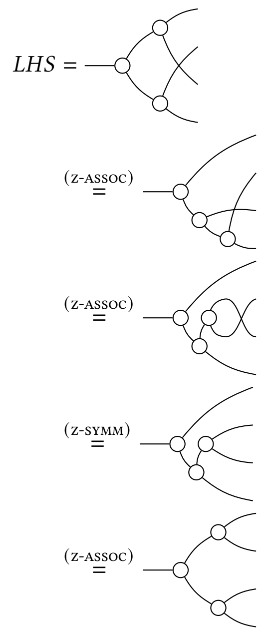


(74)

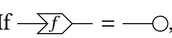
Since by theorem 3.2 the polynomials are in correspondence with diagrams in $\mathbb{L}_{CAlg_k}$, so we may prove this proposition by structural induction on diagrams.

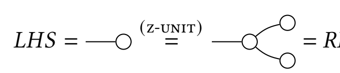
First we check that the equation holds the generators. The equation is immediate if .

If , then we have:

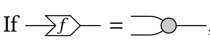


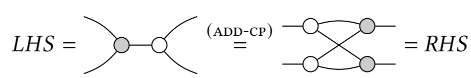
(75)

If , then we have (recalling that the spider with legs labelled by 0 is the empty diagram):

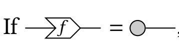


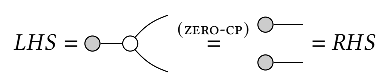
(76)

If , then we have:

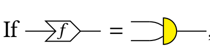


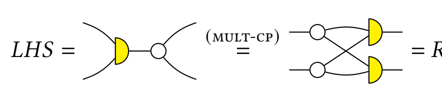
(77)

If , then we have:

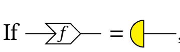


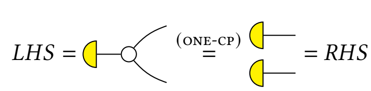
(78)

If , then we have:



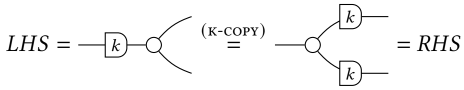
(79)

If , then we have:



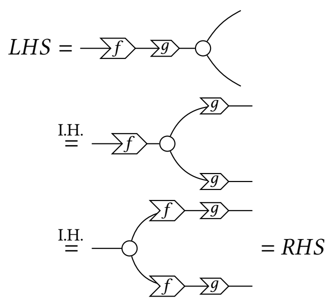
(80)

If ⟶ f ⟶ = ⟶ κ ⟶, then we have:

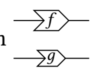


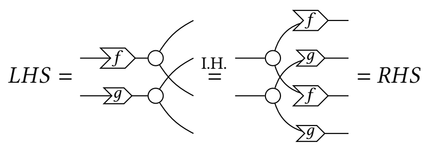
(81)

Thus the proposition holds for all the generators of $\mathbb{L}_{CAlg_k}$. Now for the inductive step: suppose the proposition holds for n ⟶ f ⟶ m and n' ⟶ g ⟶ m'. Then, in the case $m = n'$, consider the diagram ⟶ f ⟶ g ⟶. we have



(82)

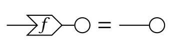
Finally, for the diagram  we have



(83)

Here, I.H. denotes the inductive hypothesis. This completes the induction.

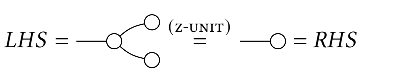
We next prove that rule (POLY-DEL)is deriveable in $\mathbb{L}_{CAlg_k}$, that is,



(84)

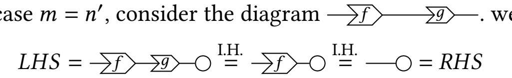
We again use structural induction on the diagrams of $\mathbb{L}_{CAlg_k}$. The equation is tautological if either ⟶ f ⟶ = ——— or ⟶ f ⟶ = ——○ (recalling that the spider with legs labelled by 0 is the empty diagram).

If ⟶ f ⟶ = ——○⊂, we have

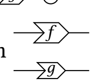


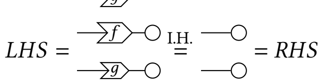
(85)

If ⟶ f ⟶ = or or or or ⟶ κ ⟶, the desired proposition is just a straightforward application of axioms (ADD-DEL), (ZERO-DEL), (MULT-DEL), (ONE-DEL), (K-DEL)respectively. So the proposition holds for all generators of $\mathbb{L}_{CAlg_k}$. Now for the inductive step: suppose the proposition holds for n ⟶ f ⟶ m and n' ⟶ g ⟶ m'. Then, in the case $m = n'$, consider the diagram ⟶ f ⟶ g ⟶. we have



(86)

Finally, for the diagram  we have



(87)

This completes the induction.

Finally, the rules (POLY-ADD), (POLY-MULT), and (POLY-COMP)are direct consequences of the fact that $\mathbb{L}_{CAlg_k}$ is the Lawvere theory of commutative algebras over k. ◻

B Proofs about $\mathbb{L}_{\mathrm{Cosp}}$

B.1 Proofs about Soundness

Proposition 5.2 (Cospan Soundness)**.** *Every rewrite rule in E is sound with respect to the intended semantic* $[\![-]\!]$.

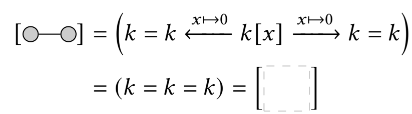
Proof. First to prove (K-INV): for $l \in k^{\times}$,

$$\begin{aligned}
[\![-\boxed{l}-]\!] &= \left(k[x] = k[x] \xleftarrow{y \mapsto lx} k[y]\right) \\
&= \left(k[x] \xrightarrow{x \mapsto l^{-1}y} k[y] = k[y]\right) \\
&= [\![-\boxed{l^{-1}}-]\!]
\end{aligned} \tag{88}$$

where the second equality is the span isomorphism

$$\begin{tikzcd}
 & k[x] \arrow[dd, "l^{-1}y"] & \\
k[x] \arrow[ur, equal] \arrow[dr, "l^{-1}y"'] & & k[y] \arrow[ul, "lx"'] \arrow[dl, equal] \\
 & k[y] &
\end{tikzcd}$$

Next to prove (X-BONE):

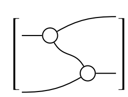


(89)

here the second equality is the pushout

$$\begin{tikzcd}
 & k & \\
k \arrow[ur, equal] & & k \arrow[ul, equal] \\
 & k[x] \arrow[ul, "x\mapsto 0"] \arrow[ur, "x\mapsto 0"'] &
\end{tikzcd}$$

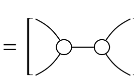
Next to prove(Z-FROB):



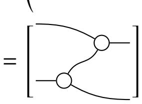
$$= \left(k[x_1, x_2] \xleftarrow{\substack{x_1 \leftarrow\!\shortmid y_1 \\ x_1 \leftarrow\!\shortmid y_2 \\ x_2 \leftarrow\!\shortmid y_3}} k[y_1, y_2, y_3] \xrightarrow{\substack{y_1 \mapsto z_1 \\ y_2 \mapsto z_2 \\ y_3 \mapsto z_2}} k[z_1, z_2] \right)$$

$$= \left(k[x_1, x_2] \to \frac{k[x_1, x_2, z_1, z_2]}{(x_1 - z_1, x_1 - z_2, x_2 - z_2)} \leftarrow k[z_1, z_2] \right) \tag{90}$$

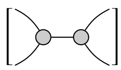
$$= \left(k[x_1, x_2] \xrightarrow{\substack{x_1 \mapsto y \\ x_2 \mapsto y}} k[y] \xleftarrow{\substack{y \leftarrow\!\shortmid z_1 \\ y \leftarrow\!\shortmid z_2}} k[z_1, z_2] \right) =$$



$$= \left(k[x_1, x_2] \xleftarrow{\substack{x_1 \leftarrow\!\shortmid y_1 \\ x_2 \leftarrow\!\shortmid y_2 \\ x_2 \leftarrow\!\shortmid y_3}} k[y_1, y_2, y_3] \xrightarrow{\substack{y_1 \mapsto z_1 \\ y_2 \mapsto z_1 \\ y_3 \mapsto z_2}} k[z_1, z_2] \right)$$

$=$ 

Next for the soundness of (x-frob): first, by a pushout we obtain that



$$= \left(k[x_1,x_2] \xleftarrow{x_1+x_2 \mapsfrom y} k[y] \xrightarrow{y\mapsto z_1+z_2} k[z_1,z_2]\right) \qquad (91)$$
$$= \left(k[x_1,x_2] \to \frac{k[x_1,x_2,z_1,z_2]}{(x_1+x_2-z_1-z_2)} \leftarrow k[z_1,z_2]\right)$$

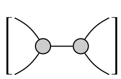
Now consider the apex of the cospan in the final line of 91. We can parametrize it in two ways:

$$\begin{tikzcd}
 & k[u_1,u_2,u_3] & \\
k[x_1,x_2] \arrow[ur, "\substack{x_1\mapsto u_1+u_2 \\ x_2\mapsto u_3}"] \arrow[r] \arrow[dr, "\substack{x_1\mapsto v_1 \\ x_2\mapsto v_2+v_3}"'] & \frac{k[x_1,x_2,z_1,z_2]}{(x_1+x_2-z_1-z_2)} \arrow[u, "\alpha"] \arrow[d, "\beta"'] & k[z_1,z_2] \arrow[ul, "\substack{z_1\mapsto u_1 \\ z_2\mapsto u_2+u_3}"'] \arrow[l] \arrow[dl, "\substack{z_1\mapsto v_1+v_2 \\ z_2\mapsto v_3}"] \\
 & k[v_1,v_2,v_3] &
\end{tikzcd}$$

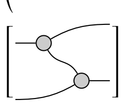
where α, β are the obvious maps that make the above diagram commute:

$$\alpha : \begin{array}{l} x_1 \mapsto u_1+u_2 \\ x_2 \mapsto u_3 \\ z_1 \mapsto u_1 \\ z_2 \mapsto u_2+u_3 \end{array} \qquad \beta : \begin{array}{l} x_1 \mapsto v_1 \\ x_2 \mapsto v_2+v_3 \\ z_1 \mapsto v_1+v_2 \\ z_2 \mapsto v_3 \end{array} \qquad (92)$$

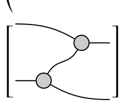
Which are both isomorphisms of algebras. This gives:



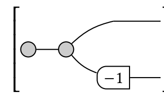
$$= \left(k[x_1,x_2] \to \frac{k[x_1,x_2,z_1,z_2]}{(x_1+x_2-z_1-z_2)} \leftarrow k[z_1,z_2]\right)$$
$$= \left(k[x_1,x_2] \xrightarrow{\substack{x_1\mapsto u_1+u_2 \\ x_2\mapsto u_3}} k[u_1,u_2,u_3] \xleftarrow{\substack{u_1 \mapsfrom z_1 \\ u_2+u_3 \mapsfrom z_2}} k[z_1,z_2]\right)$$

$=$  $\qquad (93)$

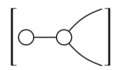
$$= \left(k[x_1,x_2] \xrightarrow{\substack{x_1\mapsto v_1 \\ x_2\mapsto v_2+v_3}} k[v_1,v_2,v_3] \xleftarrow{\substack{v_1+v_2 \mapsfrom z_1 \\ v_3 \mapsfrom z_2}} k[z_1,z_2]\right)$$

$=$ 

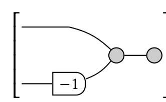
Now for the soundness of (cup):

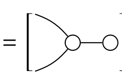


$$= \left(k \xleftarrow{0 \mapsfrom x} k[x] \xrightarrow{x\mapsto y_1-y_2} k[y_1,y_2]\right)$$
$$= \left(k \to \frac{k[y_1,y_2]}{(y_1-y_2)} \leftarrow k[y_1,y_2]\right) \qquad (94)$$
$$= \left(k \to k[x] \xleftarrow{\substack{x \mapsfrom y_1 \\ x \mapsfrom y_2}} k[y_1,y_2]\right)$$

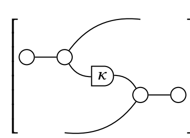
$=$ 

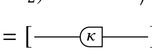
The proof for the soundness of (cap)is almost identical:



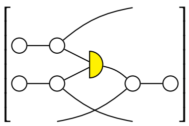
$$= \left(k[x_1,x_2] \xleftarrow{x_1-x_2 \mapsfrom y} k[y] \xrightarrow{y\mapsto 0} k\right)$$
$$= \left(k[x_1,x_2] \to \frac{k[x_1,x_2]}{(x_1-x_2)} \leftarrow k\right) \qquad (95)$$
$$= \left(k[x_1,x_2] \xrightarrow{\substack{x_1\mapsto y \\ x_2\mapsto y}} k[y] \leftarrow k\right) =$$ 

Now for the soundness of (κ-trp):



$$= \left(k[x_2] \to k\begin{bmatrix}x_1 \\ x_2\end{bmatrix} \xleftarrow{\substack{x_1 \mapsfrom y_1 \\ \kappa x_1 \mapsfrom y_2 \\ x_2 \mapsfrom y_3}} k\begin{bmatrix}y_1 \\ y_2 \\ y_3\end{bmatrix} \xrightarrow{\substack{y_1\mapsto z_1 \\ y_2\mapsto z_2 \\ y_3\mapsto z_2}} k\begin{bmatrix}z_1 \\ z_2\end{bmatrix} \leftarrow k[z_1]\right) \qquad (96)$$
$$= \left(k[x_2] \to \frac{k[x_1,x_2,z_1,z_2]}{(x_1-z_1, \kappa x_1 - z_2, x_2 - z_2)} \leftarrow k[z_1]\right)$$
$$= \left(k[x_2] \xrightarrow{x_2\mapsto \kappa z_1} k[z_1] \leftarrow k[z_1]\right) =$$ 

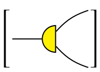
For the soundness of (K-TRP):



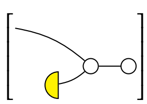
$$= \left(k[x_3] \to k\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \xleftarrow{\substack{x_1 \mapsfrom y_1 \\ x_1x_2 \mapsfrom y_2 \\ x_3 \mapsfrom y_3 \\ x_2 \mapsfrom y_4}} k\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} \xrightarrow{\substack{y_1 \mapsto z_1 \\ y_2 \mapsto z_2 \\ y_3 \mapsto z_2 \\ y_4 \mapsto z_3}} k\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \leftarrow k\begin{bmatrix} z_1 \\ z_3 \end{bmatrix} \right) \tag{97}$$

$$= \left(k[x_3] \to \frac{k[x_1, x_2, x_3, z_1, z_2, z_3]}{(x_1 - z_1, x_1x_2 - z_2, x_3 - z_2, x_2 - z_3)} \leftarrow k\begin{bmatrix} z_1 \\ z_3 \end{bmatrix} \right)$$

$$= \left(k[x_3] \xrightarrow{x_3 \mapsto z_1 z_3} k[z_1, z_3] \leftarrow k[z_1, z_3] \right)$$

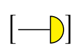
= 

For the soundness of (ONE-TRP):



$$= \left(k[x] \xleftarrow{\substack{x \mapsfrom y_1 \\ 1 \mapsfrom y_2}} k[y_1, y_2] \xrightarrow{\substack{y_1 \mapsto z \\ y_2 \mapsto z}} k[z] \leftarrow k \right) \tag{98}$$

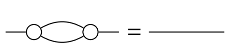
$$= \left(k[x] \to \frac{k[x, z]}{(x - z, 1 - z)} \leftarrow k \right)$$

$$= \left(k[x] \xrightarrow{x \mapsto 1} k \leftarrow k \right) =$$ 

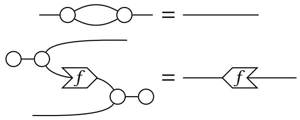
This completes the proof that every rewrite rule contained in figure 5 are sound with respect to the semantics functor $[-] : \mathbb{L}_{\text{Cosp}} \to_F \text{Cosp}(\text{CAlg}_k^{\text{f.g.}})$. □

B.2 Proofs of Derived Rules

Lemma 5.3. *The following are some useful derived rules of* $\mathbb{L}_{\text{Cosp}}$*:*



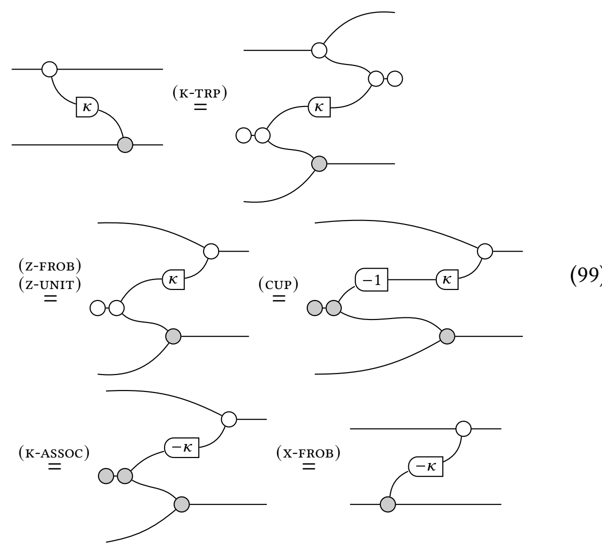
(special)



$\forall f \in (k[x_1, \ldots, x_n])^m$

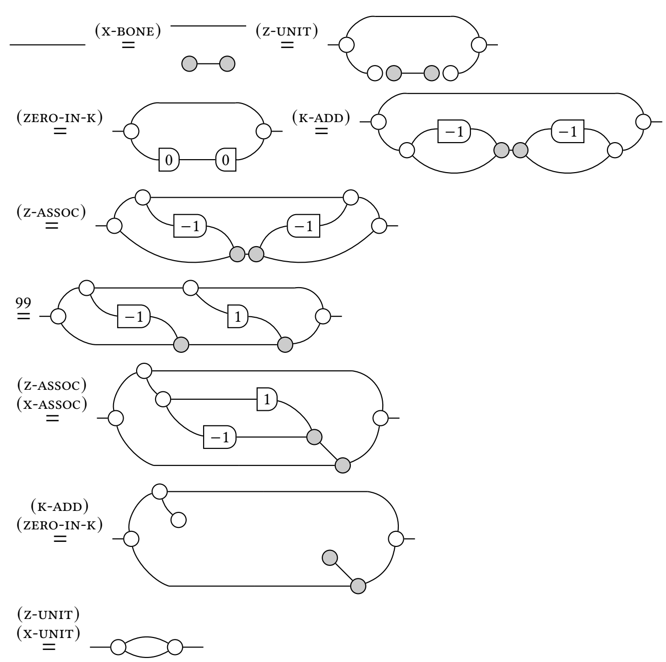
(poly-trp)

Proof. First we show how to derive special. The reasoning in this proof is almost identical to the reasoning in the proofs contained in appendix A.2.2 of [70]. We first make the following derivation: for any $\kappa \in k$,



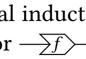
(99)

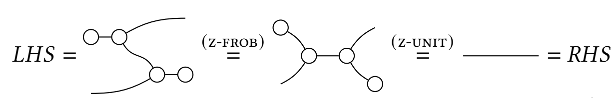
and with this we can make the desired derivation:



(100)

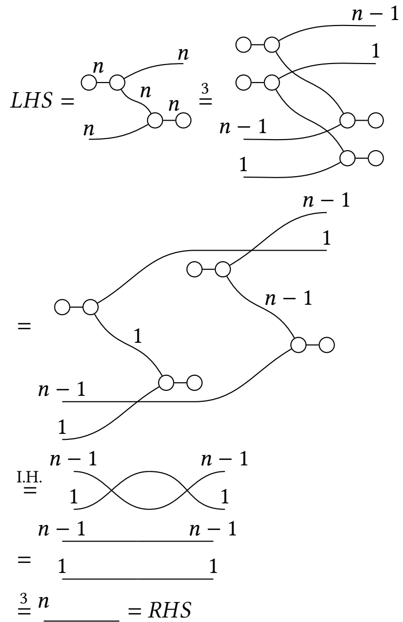
as required.

Next we show how to derive poly-trp by structural induction on $\mathbb{L}_{CAlg_k}$. First we show that the proposition holds for  = n ______. When $n = 1$ this is easily derived as:



(101)

whereas for $n > 1$ we can induct on n:

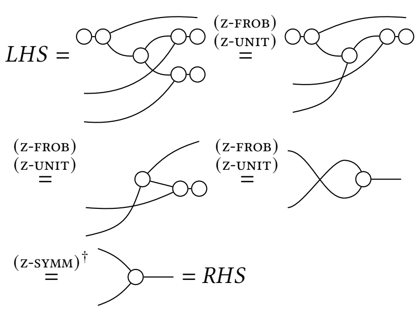


(102)

where the equality labelled "I.H." is an application of the inductive hypothesis.

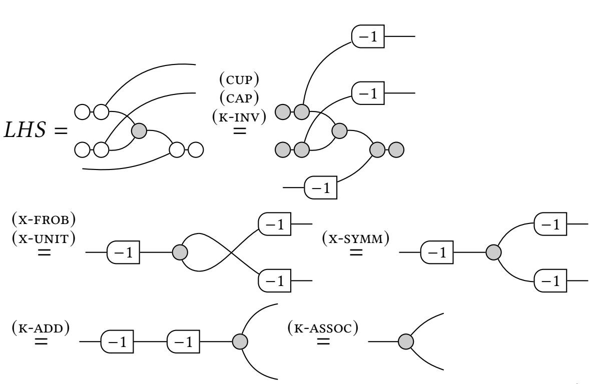
We then check that the proposition holds for f ranging over every generator of $\mathbb{L}_{CAlg_k}$.

If f = , then



(103)

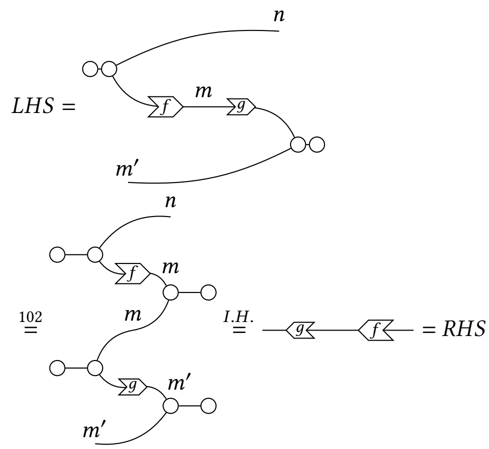
If f = , the derivation is similar:



(104)

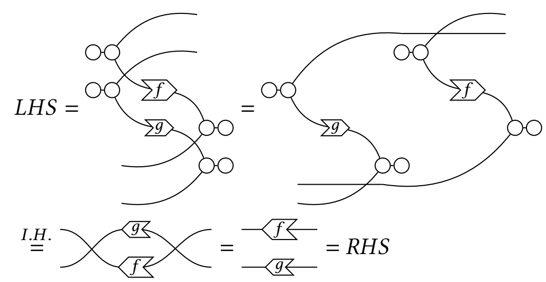
For f = or , the proposition is a straightforward application of their respective (co)unitality laws (z-unit) and (x-unit). Finally, for f = , , or κ, the proposition is verbatim identical to the laws (k-trp), (one-trp), or (k-trp) respectively.

Now for the inductive step: suppose the proposition holds for $n \xrightarrow{f} m$ and $n' \xrightarrow{g} m'$. Then, in the case $m = n'$, consider the diagram $\xrightarrow{f}\xrightarrow{g}$. we have



(105)

And for the diagram f over g, we have



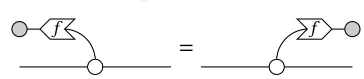
(106)

Where the second equality follows from the naturality of the braidings, and the fourth equality follows from both the naturality and the involutivity of the braidings. This completes the structural induction and proof. □

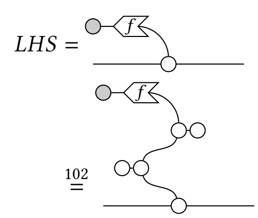
B.3 Proofs about Ideal Gadgets

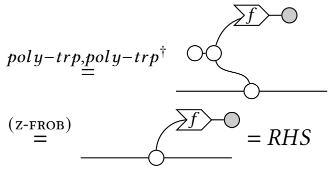
In this appendix we prove that the following lemmas hold in $\mathbb{L}_{\mathrm{Cosp}}$.

Lemma 5.4. *For any $f \in k[x_1, \dots, x_n]$, the following is deriveable from the rewrite rules of $\mathbb{L}_{\mathrm{Cosp}}$:*



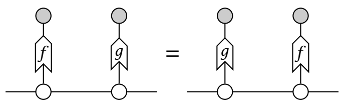
Proof.



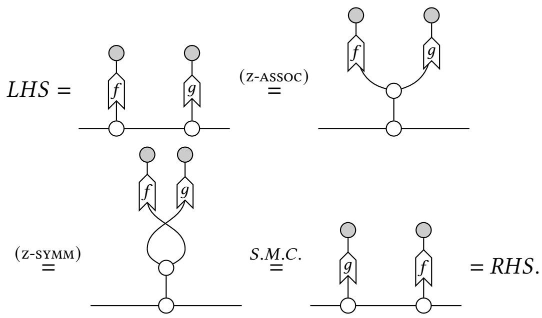


□

Lemma 5.5. *For any $f, g \in k[x_1, \ldots, x_n]$, the following is deriveable from the rewrite rules of $\mathbb{L}_{\mathrm{Cosp}}$:*



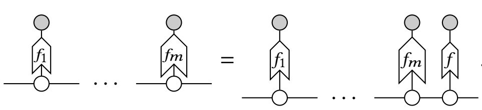
Proof.



(107)

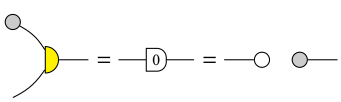
Here the equality labelled S.M.C. follows from the naturality of the braidings in a symmetric monoidal category. □

Lemma 5.6. *Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, and pick some f inside the ideal $(f_1, \ldots, f_m)$. Then the following is deriveable from the rewrite rules of $\mathbb{L}_{\mathrm{Cosp}}$:*



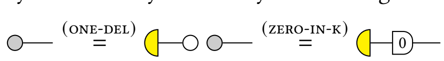
(26)

Proof. First, by the completeness of $\mathbb{L}_{CAlg_k}$, we know that the following equation is deriveable:

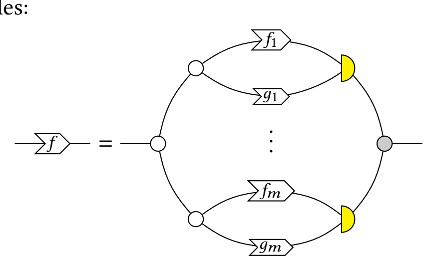


(108)

Note, the second equality here is verbatim rule (zero-in-k); while the first equality can be easily derived by substituting

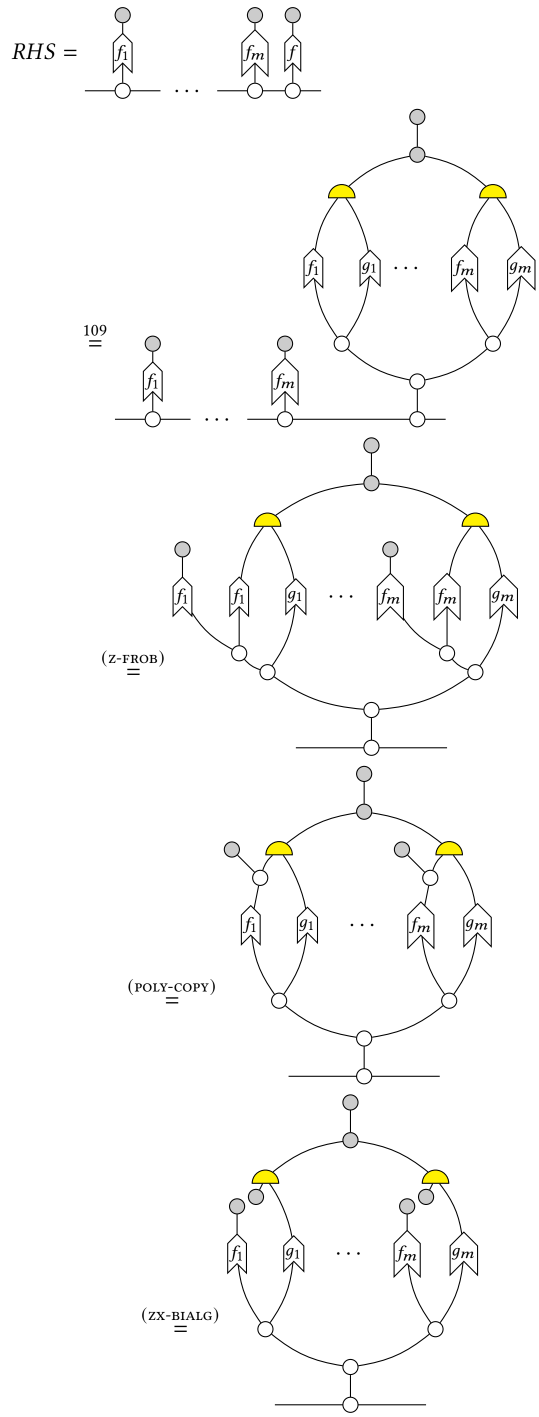


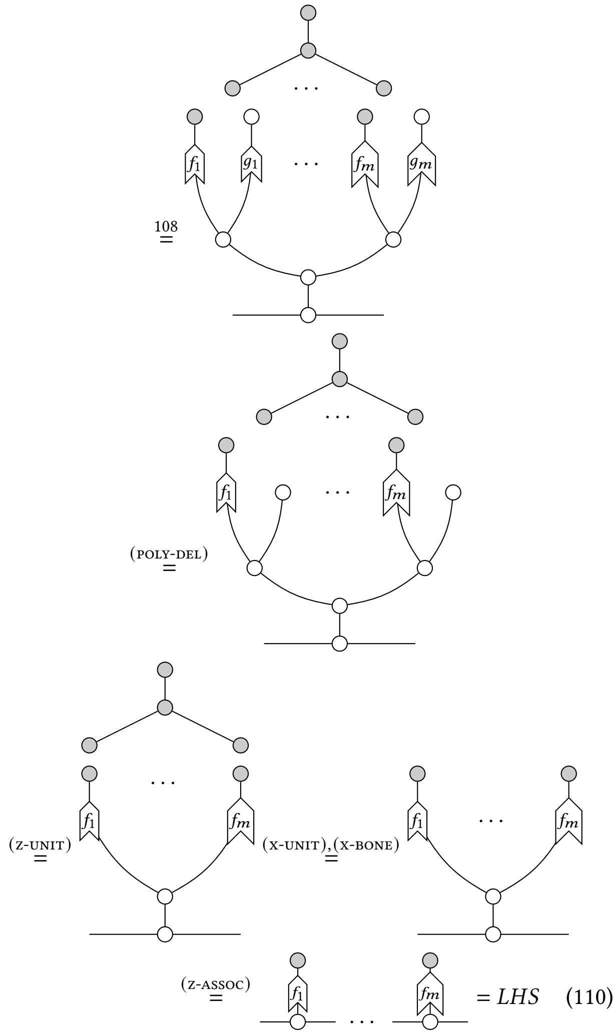
Now, since $f \in (f_1, \ldots, f_m)$, so there exist polynomials $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$ such that $f = g_1 f_1 + \cdots + g_m f_m$. Then by the completeness of $\mathbb{L}_{CAlg_k}$, we know that the following is deriveable by its rewrite rules:



(109)

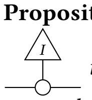
Thus we can rewrite the right-hand-side of (26) as follows:

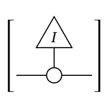




(110)

□

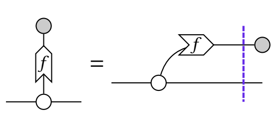
Proposition 5.9 (Quotient Gadgets). *The semantic of the gadget*  *is (any finite presentation of) the finitely generated commutative algebra defined by I. More precisely, if $I \subset k[x_1, \ldots, x_n]$ is any ideal, then*



$$= (S_k(n) \twoheadrightarrow S_k(n)/I \twoheadleftarrow S_k(n))$$

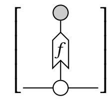
where both legs are the canonical projections π_I against I.

Proof. We first show this for the case where I is a principal ideal: say $I = (f)$. We view the gadget as a composition of two diagrams like so:



(111)

Note that the left-half is a diagram in $\mathbb{L}_{CAlg_k}$, while the right-half is a diagram in $\mathbb{L}^{op}_{CAlg_k}$. So

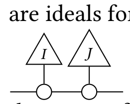


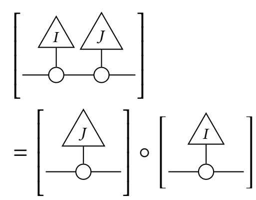
$$= \left(k[x_1, \ldots, x_n] \xleftarrow[x_j \leftarrow\!\shortmid y_j]{f(\mathbf{x}) \leftarrow\!\shortmid y_0} k[y_0, \ldots, y_n] \xrightarrow[y_j \mapsto z_j]{y_0 \mapsto 0} k[z_1, \ldots, z_n]\right)$$

$$= \left(k[x_1, \ldots, x_n] \rightarrow \frac{k[x_1, \ldots, x_n, z_1, \ldots, z_n]}{(f(\mathbf{x}), x_j - z_j)} \leftarrow k[z_1, \ldots, z_n]\right)$$

$$= \left(k[x_1, \ldots, x_n] \rightarrow \frac{k[x_1, \ldots, x_n]}{(f(\mathbf{x}))} \leftarrow k[x_1, \ldots, x_n]\right) \quad (112)$$

where, in the derivation 112, the index j is always quantified universally over $1, \ldots, n$.

Now we perform the inductive step: suppose that $I, J \subset k[x_1, \ldots, x_n]$ are ideals for which the proposition holds. Then the composition  is the gadget corresponding to the ideal generated by the union of the elements in I and J (since we have taken a union of the generators). In other words it is the gadget corresponding to $I + J$. We compute:



$$= \left(k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix} \twoheadrightarrow k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}/I \twoheadleftarrow k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix} \twoheadrightarrow k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}/J \twoheadleftarrow k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}\right)$$

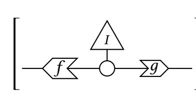
$$= \left(k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix} \twoheadrightarrow \frac{k[x_1, \ldots, x_n]}{I + J} \twoheadleftarrow k\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}\right)$$

(113)

Recall that, since $k[x_1, \ldots, x_n]$ is a Noetherian ring, every ideal is a finite sum of principal ideals. This completes the induction and the proof. □

B.4 Proofs about Universality and Completeness

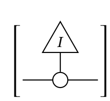
Proposition 5.10 (Cospan Universality). *For any ideal $I \subset k[x_1, \ldots, x_n]$ and tuples of polynomials $f \in (k[x_1, \ldots, x_n])^m$ and $g \in (k[x_1, \ldots, x_n])^{m'}$,*



$$= \left(S_k(m) \xrightarrow{f_I^\#} A \xleftarrow{g_I^\#} S_k(m')\right) \qquad (29)$$

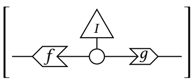
where $A = S_k(n)/I$. Since every algebra morphism $S_k(m) \rightarrow A$ is equal to $f_I^\#$ for some f, so $[-] : \mathbb{L}_{\mathrm{Cosp}} \rightarrow_F \mathrm{Cosp}(\mathrm{CAlg}_k^{\mathrm{f.g.}})$ is full.

Proof. Recall from proposition 5.9 that the semantic of the quotient gadget in the middle of the diagram on the left-hand-side is



$$= (S_k(n) \twoheadrightarrow S_k(n)/I \twoheadleftarrow S_k(n)) \qquad (114)$$

Thus we have



$$= \left(S_k(m) \xrightarrow{f^\#} S_k(n) \twoheadrightarrow S_k(n)/I \twoheadleftarrow S_k(n) \xleftarrow{g^\#} S_k(m')\right) \quad (115)$$

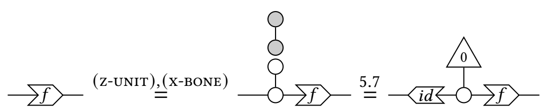
$$= \left(S_k(m) \xrightarrow{f^\#_I} A \xleftarrow{g^\#_I} S_k(m')\right)$$

as required. □

Proposition 5.12 (Cospan Normal Form)**.** *Every diagram in $\mathbb{L}_{\mathrm{Cosp}}$ can be rewritten into cospan form.*

Proof. We prove by structural induction. First we show that every generator of $\mathbb{L}_{\mathrm{Cosp}}$ can be rewritten into cospan form. By †-symmetry, we only need to show this for the generators coming from $\mathbb{L}_{CAlg_k}$.

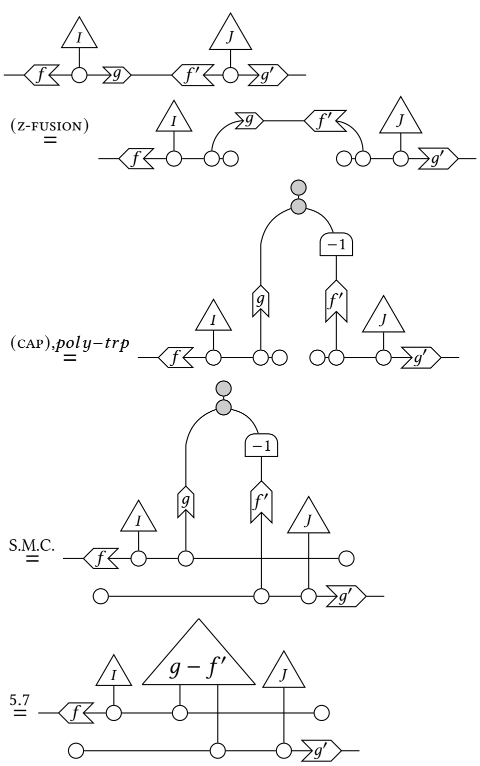
But this is immediate: for any f $\in \mathbb{L}_{CAlg_k}$, we may rewrite it as



(116)

Thus all the generators of $\mathbb{L}_{\mathrm{Cosp}}$ can be rewritten into cospan form. It remains now to show that compositions and monoidal products of cospan form diagrams can be rewritten into cospan form.

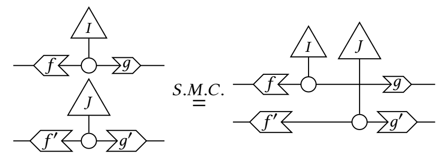
Take any pair of composable diagrams in cospan form. Their composition can be rewritten thus:



(117)

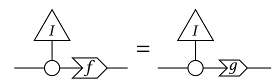
Where the equality labelled "S.M.C." is an application of the coherence axioms of symmetric monoidal categories. Note that this corresponds precisely to the pushout operation taken in the composition of cospans.

Finally, take any pair of arbitrary diagrams in cospan form. Their monoidal product can be rewritten as:



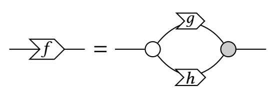
which is again in cospan form. Thus by induction all diagrams in $\mathbb{L}_{\mathrm{Cosp}}$ can be rewritten into cospan form. □

Lemma 5.13. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $f, g \in (k[x_1, \ldots, x_n])^m$ be any two polynomial tuples such that $f - g \in I^m$. That is, let f, g be such that $f^\#_I = g^\#_I$. Then the following diagram rewrite is derivable in $\mathbb{L}_{\mathrm{Cosp}}$:*



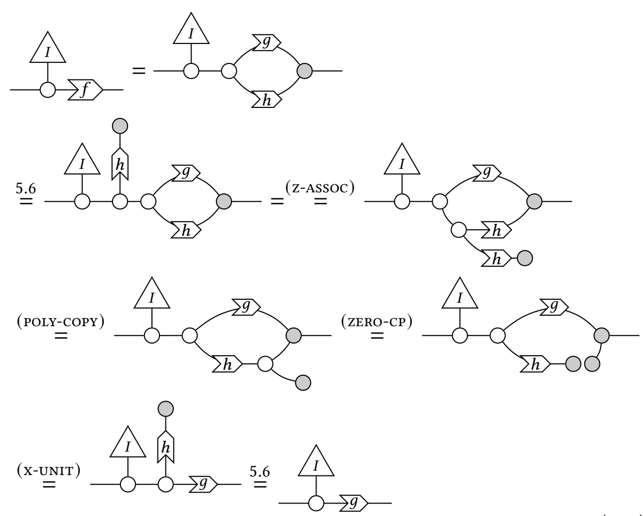
(31)

Proof. Suppose $h = f - g \in I^m$. By Proposition 3.2



(118)

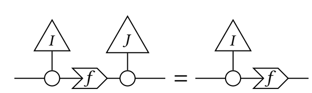
is a rewrite in $\mathbb{L}_{CAlg_k}$. So we compute:



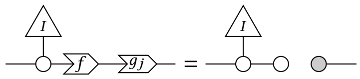
(119)

□

Lemma 5.14. *Suppose $I \subset S_k(n)$ and $J \subset S_k(m)$ are ideals of polynomials and $f \in (S_k(n))^m$. Suppose $f^\#_I : S_k(m) \to S_k(n)/I$ satisfies $J \subset \ker f^\#_I$. Then the following rewrite holds:*

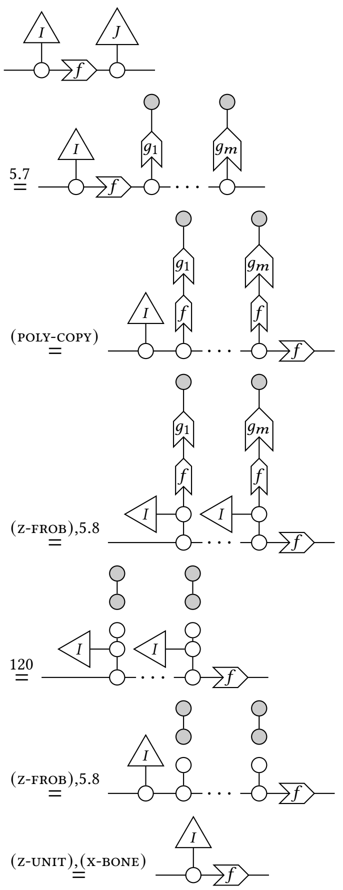


Proof. Suppose $g_1, \ldots, g_m$ is a basis $J = (g_1, \ldots, g_m)$. Then for each g_j, we have $f^\#_I(g_j) = 0$. Using the definition of the #, we have in other words $(g_j \circ f)^\#_I = 0$. So $g_j \circ f \in I$. Thus by lemma 5.13, we have a rewrite



(120)

So we can derive:



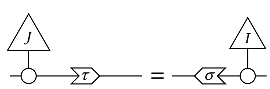
(121)

□

Lemma 5.15. *Suppose $I \subset S_k(n)$ and $J \subset S_k(m)$ are ideals, $\alpha : S_k(m)/J \to S_k(n)/I$ is an isomorphism of algebras, and $\sigma \in (k[x_1, \ldots, x_n])^m$, $\tau \in (k[y_1, \ldots, y_m])^n$ are a pair of polynomial tuples such that they represent α, α^{-1} respectively, i.e. such that the following commutes:*

$$\begin{tikzcd} S_k(m) \arrow[r, two heads, "\pi_J"] \arrow[d, "\sigma^\#"'] & S_k(m)/J \arrow[d, shift left, "\alpha"] & S_k(m) \arrow[l, two heads, "\pi_J"'] \\ S_k(n) \arrow[r, two heads, "\pi_I"'] & S_k(n)/I \arrow[u, shift left, "\alpha^{-1}"] & S_k(n) \arrow[l, two heads, "\pi_I"] \arrow[u, "\tau^\#"'] \end{tikzcd}$$

Then the following rewrite holds:



(32)

Proof. We know that

$$\pi_I \circ \sigma^\# = \alpha \circ \pi_J$$
$$\pi_J \circ \tau^\# = \alpha^{-1} \circ \pi_I \tag{122}$$

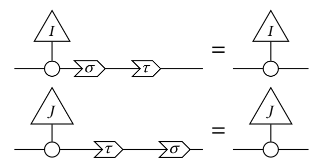
from which we can easily derive that

$$\pi_I \circ \sigma^\# \circ \tau^\# = \pi_I$$
$$\pi_J \circ \tau^\# \circ \sigma^\# = \pi_J \tag{123}$$

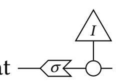
which is to say,

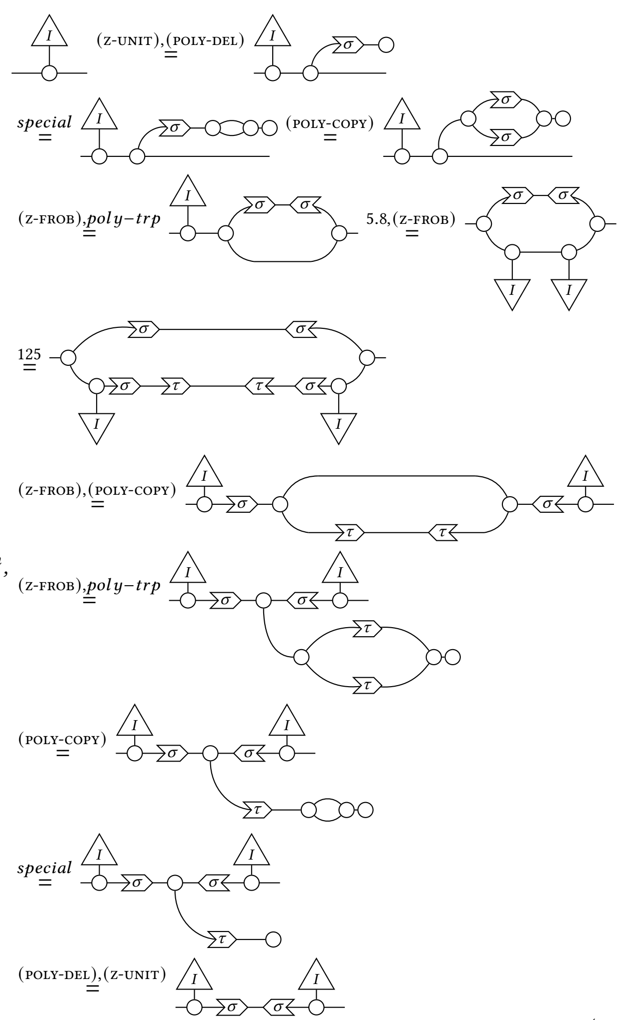
$$(\tau \circ \sigma)^\#_I = (id)^\#_I$$
$$(\sigma \circ \tau)^\#_J = (id)^\#_J \tag{124}$$

So by lemma 5.13, the following are deriveable in $\mathbb{L}_{\mathrm{Cosp}}$:



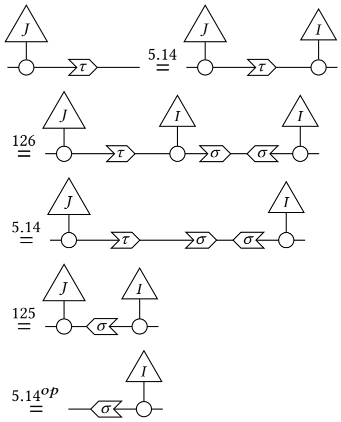
(125)

Now we can show that  is the left inverse of σ:



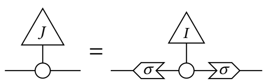
(126)

And consequently we have the rewrite we need:

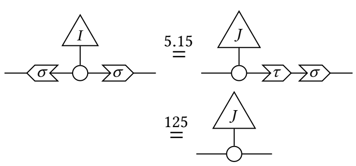


$\square$

Corollary 5.16. *If $\alpha : S_k(m)/J \to S_k(n)/I$ is an isomorphism of algebras, and $\sigma \in (k[x_1, \ldots, x_n])^m$ represents α as in lemma 5.15, then*



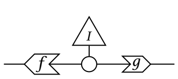
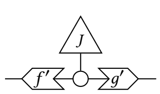
Proof.


(127)

$\square$

Proposition 5.17. *The functor $[-]$ is faithful. That is, $\mathbb{L}_{\mathsf{Cosp}}$ is complete as a language for ${}_F\,\mathsf{Cosp}(\mathsf{CAlg}_k^{\mathrm{f.g.}})$.*

Proof. This is in other words to say that our rewrite rules are complete. By proposition 5.12 any diagram in $\mathbb{L}_{\mathsf{Cosp}}$ can be rewritten into cospan form. So it suffices to prove that, whenever two diagrams in cospan form are mapped to isomorphic cospans by $[-]$, then they are rewriteable into each other. Pick any two diagrams in cospan form

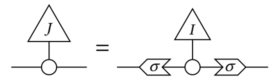
 and 

with the same wire types on both ends. Suppose there exists a cospan isomorphism

$$\begin{tikzcd} & S_k(u)/I & \\ k^n \arrow[ur, "f_I^\#"] \arrow[dr, "f_J'^\#"'] & & k^m \arrow[ul, "g_I^\#"'] \arrow[dl, "g_J'^\#"] \\ & S_k(v)/J \arrow[uu, "\alpha"] & \end{tikzcd} \tag{128}$$

between their images under the semantics functor.

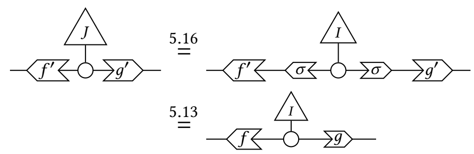
Since $\alpha : S_k(v)/J \to S_k(u)/I$ is an isomorphism, so corollary 5.16 gives a rewrite



where σ is some tuple of polynomials such that $\sigma_I^\# = \alpha \circ \pi_J$ (say, pick $\sigma = (\alpha \circ \pi_J)_I^\flat$). Moreover, since diagram 128 commutes, so

$$f_I^\# = \alpha \circ f_J'^\# = \alpha \circ \pi_J \circ f'^\# = \sigma_I^\# \circ f'^\# = (f' \circ \sigma)_I^\# \tag{129}$$

and similarly we may derive $g_I^\# = (g' \circ \sigma)_I^\#$. So we have the following rewrites:


(130)

$\square$

C Proofs about $\mathbb{L}_{\mathsf{Span}_k}$ and $\mathbb{L}_{\mathsf{Span}_q}$

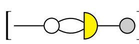
C.1 Proofs about $\mathbb{L}_{\mathsf{Span}_k}$

Proposition 6.2. *The PROP morphism*

$$\mathbb{L}_{\mathsf{Cosp}} \xrightarrow{\mathrm{Spec}[-]_{red}}{}_G\, \mathsf{Span}(\mathsf{AffVar}_k) \tag{34}$$

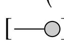
factors through $\mathbb{L}_{\mathsf{Span}_k}$. In other words, rule (red) *is sound for affine varieties over an algebraically closed field.*

Proof. We compute directly:

Spec []$_{red}$ $= \mathrm{Spec}\left(k[x] \xleftarrow{x^2} k[y] \xrightarrow{0} k\right)_{red}$

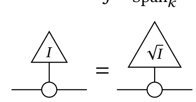
$$\overset{pushout}{=} \mathrm{Spec}\left(k[x] \to k[x]/(x^2) \leftarrow k\right)_{red} \tag{131}$$

$$\overset{reduce}{=} \mathrm{Spec}\left(k[x] \xrightarrow{0} k = k\right)$$

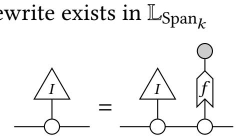
= Spec []$_{red}$

Thus rule red is sound with respect to the map $\mathrm{Spec}[-]_{red}$, and so the map factors through $\mathbb{L}_{\mathsf{Span}_k}$. $\square$

Lemma 6.3. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The following is deriveable from the rewrite rules of $\mathbb{L}_{\mathsf{Span}_k}$:*

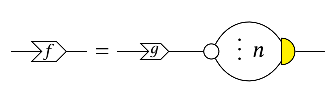

(36)

Proof. Since $\sqrt{I}$ will have a finite basis, so it suffices to prove that the following rewrite exists in $\mathbb{L}_{\mathsf{Span}_k}$

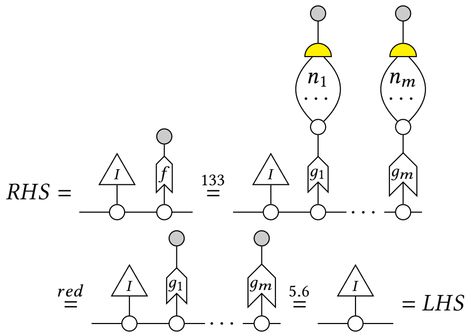

(132)

for any $f \in \sqrt{I}$.

Since $f \in \sqrt{I}$, so there exists some $g \in I$ and some $n \in \mathbb{N}$ such that $g^n = f$. Thus by the completeness of $\mathbb{L}_{CAlg_k}$ alone, the following is deriveable:


(133)

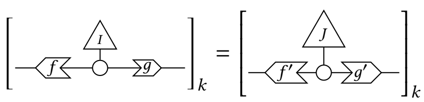
So we have



∎

Proposition 6.4. *The semantic map* $\mathbb{L}_{\mathrm{Span}_k} \xrightarrow{[-]_k} {}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$ *is faithful. In other words,* $\mathbb{L}_{\mathrm{Span}_k}$ *is complete for* ${}_G\,\mathrm{Span}(\mathrm{AffVar}_k)$.

Proof. Pick any ideals $I \subset S_k(u)$ and $J \subset S_k(v)$, and any tuples of polynomials $f \in (k[x_1,\ldots,x_n])^u$, $f' \in (k[x_1,\ldots,x_n])^v$, $g \in (k[y_1,\ldots,y_m])^u$, and $g' \in (k[y_1,\ldots,y_m])^n$. Suppose that the following diagrams are sent to the same semantic by $[-]_k$:

 (134)

that is, there is a span isomorphism of varieties

$$\begin{aligned}&\mathrm{Spec}\left(S_k(n) \xrightarrow{f_I^\#} S_k(u)/I \xleftarrow{g_I^\#} S_k(m)\right)_{red}\\ &= \mathrm{Spec}\left(S_k(n) \xrightarrow{f_J'^\#} S_k(v)/J \xleftarrow{g_J'^\#} S_k(m)\right)_{red}\end{aligned} \tag{135}$$

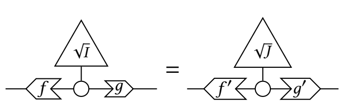
Since $\mathrm{Spec} : \mathrm{CAlg}_k^{\text{f.g., red.}} \to \mathrm{AffVar}_k^{op}$ is an equivalence of categories (Proposition 2.20), so this means

$$\begin{aligned}&\left(S_k(n) \xrightarrow{f_I^\#} S_k(u)/I \xleftarrow{g_I^\#} S_k(m)\right)_{red}\\ &= \left(S_k(n) \xrightarrow{f_J'^\#} S_k(v)/J \xleftarrow{g_J'^\#} S_k(m)\right)_{red}\end{aligned} \tag{136}$$

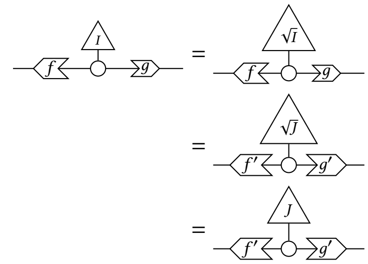
which is to say, there is an isomorphism of cospans of algebras

$$\begin{aligned}&\left(S_k(n) \xrightarrow{f_{\sqrt{I}}^\#} S_k(u)/\sqrt{I} \xleftarrow{g_{\sqrt{I}}^\#} S_k(m)\right)\\ &= \left(S_k(n) \xrightarrow{f_{\sqrt{J}}'^\#} S_k(v)/\sqrt{J} \xleftarrow{g_{\sqrt{J}}'^\#} S_k(m)\right)\end{aligned} \tag{137}$$

Thus, by the completeness of $\mathbb{L}_{\mathrm{Cosp}}$ for ${}_F\,\mathrm{Cosp}(\mathrm{CAlg}_k^{\text{f.g.}})$ (Proposition 5.17), the following rewrite exists under just the rules of $\mathbb{L}_{\mathrm{Cosp}}$:

 (138)

Thus with lemma 6.3 we obtain the series of rewrites

 (139)

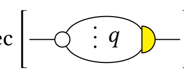
∎

Proposition 6.7. *The PROP morphism*

$$\mathbb{L}_{\mathrm{Cosp}} \xrightarrow{\mathrm{Spec}[-]_{qred}} {}_{G_q}\,\mathrm{Span}(\mathrm{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}) \tag{37}$$

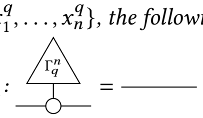
factors through $\mathbb{L}_{\mathrm{Span}_q}$*. In other words, the rule qred is sound with respect to* $\mathbb{F}_q$*-rational loci.*

Proof. We compute directly:

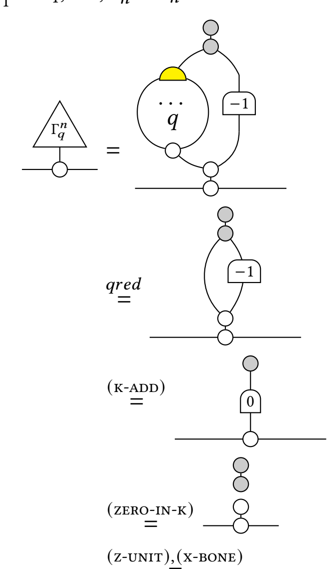
Spec  $_{qred}$

$$\begin{aligned}&= \mathrm{Spec}\left(k[x] = k[x] \xleftarrow{x^q} k[y]\right)_{qred}\\ &= \mathrm{Spec}\left(k[x]/(x^q - x) = k[x]/(x_q - x) \xleftarrow{x} k[y]/(y^q - y)\right)\\ &= \mathrm{Spec}\left(k[x]/(x^q - x) = k[x]/(x_q - x) = k[x]/(x^q - x)\right)\\ &= \mathrm{Spec}\left(k[x] = k[x] = k[x]\right)_{qred}\\ &= \mathrm{Spec}\,[\,\rule{2em}{0.4pt}\,]_{qred}\end{aligned} \tag{140}$$

∎

Lemma 6.8. *For* $\Gamma_q^n = \{x_1^q,\ldots,x_n^q\}$*, the following is deriveable from the rewrite rules of* $\mathbb{L}_{\mathrm{Span}_q}$*:* 

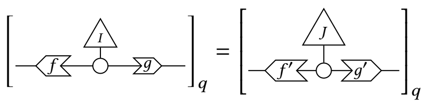
Proof. Recall from 2.25 that $\Gamma_q^n \subset k[x_1,\ldots,x_n]$ is the ideal generated by $x_1^q - x_1,\ldots,x_n^q - x_n$. Thus

 (141)

□

Proposition 6.9. *The semantic map $[-]_q$ is faithful. In other words, the rules of $\mathbb{L}_{\mathrm{Span}_q}$ are complete.*

Proof. For ideals $I \subset S_k(u)$ and $J \subset S_k(v)$, and tuples of polynomials $f \in (k[x_1, \ldots, x_n])^u$, $f' \in (k[x_1, \ldots, x_n])^v$, $g \in (k[y_1, \ldots, y_m])^u$, and $g' \in (k[y_1, \ldots, y_m])^n$. Suppose that the following diagrams are sent to the same semantic by $[-]_q$:



(142)

that is, there is a span isomorphism of varieties

$$\begin{aligned}&\mathrm{Spec}\left(S_{\mathbb{F}_q}(n) \xrightarrow{f_I^\#} S_{\mathbb{F}_q}(u)/I \xleftarrow{g_I^\#} S_{\mathbb{F}_q}(m)\right)_{qred}\\ &= \mathrm{Spec}\left(S_{\mathbb{F}_q}(n) \xrightarrow{f_J'^\#} S_{\mathbb{F}_q}(v)/J \xleftarrow{g_J'^\#} S_{\mathbb{F}_q}(m)\right)_{qred}\end{aligned} \tag{143}$$

Since $\mathrm{Spec} : \mathsf{CAlg}_{\mathbb{F}_q}^{\text{f.g., qred.}} \to \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)^{op}}$ is an equivalence of categories (Proposition 2.27), so this means

$$\begin{aligned}&\left(S_{\mathbb{F}_q}(n) \xrightarrow{f_I^\#} S_{\mathbb{F}_q}(u)/I \xleftarrow{g_I^\#} S_{\mathbb{F}_q}(m)\right)_{qred}\\ &= \left(S_{\mathbb{F}_q}(n) \xrightarrow{f_J'^\#} S_{\mathbb{F}_q}(v)/J \xleftarrow{g_J'^\#} S_{\mathbb{F}_q}(m)\right)_{qred}\end{aligned} \tag{144}$$

which is to say, there is an isomorphism of cospans of algebras

$$\begin{aligned}&\left(\frac{S_{\mathbb{F}_q}(n)}{\Gamma_q^n} \xrightarrow{(f_I^\#)_{qred}} \frac{S_{\mathbb{F}_q}(u)}{I + \Gamma_q^u} \xleftarrow{(g_I^\#)_{qred}} \frac{S_{\mathbb{F}_q}(m)}{\Gamma_q^m}\right)\\ &= \left(\frac{S_{\mathbb{F}_q}(n)}{\Gamma_q^n} \xrightarrow{(f_J'^\#)_{qred}} \frac{S_{\mathbb{F}_q}(v)}{J + \Gamma_q^v} \xleftarrow{(g_J'^\#)_{qred}} \frac{S_{\mathbb{F}_q}(m)}{\Gamma_q^m}\right)\end{aligned} \tag{145}$$

Composing both sides of the equation with projections maps we obtain isomorphisms of cospans

$$\begin{aligned}&\left(S_{\mathbb{F}_q}(n) \twoheadrightarrow \frac{S_{\mathbb{F}_q}(n)}{\Gamma_q^n} \xrightarrow{(f_I^\#)_{qred}} \frac{S_{\mathbb{F}_q}(u)}{I + \Gamma_q^u} \xleftarrow{(g_I^\#)_{qred}} \frac{S_{\mathbb{F}_q}(m)}{\Gamma_q^m} \twoheadleftarrow S_{\mathbb{F}_q}(m)\right)\\ &= \left(S_{\mathbb{F}_q}(n) \twoheadrightarrow \frac{S_{\mathbb{F}_q}(n)}{\Gamma_q^n} \xrightarrow{(f_J'^\#)_{qred}} \frac{S_{\mathbb{F}_q}(v)}{J + \Gamma_q^v} \xleftarrow{(g_J'^\#)_{qred}} \frac{S_{\mathbb{F}_q}(m)}{\Gamma_q^m} \twoheadleftarrow S_{\mathbb{F}_q}(m)\right)\end{aligned} \tag{146}$$

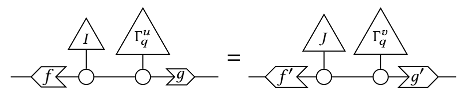
Now recall, that for an algebra morphism $\varphi : A \to B$, the morphism $\varphi_{qred} : A/\Gamma_q(A) \to B/\Gamma_q(B)$ is the unique morphism making the following commute:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, two heads] & B \arrow[d, two heads] \\ A/\Gamma_q(A) \arrow[r, "\varphi_{qred}"'] & B/\Gamma_q(B) \end{tikzcd}$$

so in particular, equation 146 becomes

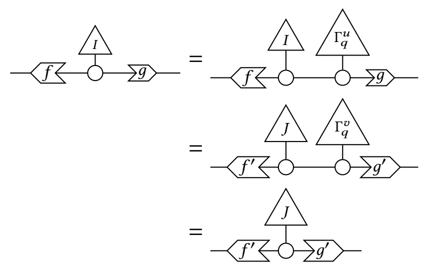
$$\begin{aligned}&\left(S_{\mathbb{F}_q}(n) \xrightarrow{f_{I+\Gamma_q^u}^\#} \frac{S_{\mathbb{F}_q}(u)}{I + \Gamma_q^u} \xleftarrow{g_{I+\Gamma_q^u}^\#} S_{\mathbb{F}_q}(m)\right)\\ &= \left(S_{\mathbb{F}_q}(n) \xrightarrow{f_{J+\Gamma_q^v}'^\#} \frac{S_{\mathbb{F}_q}(v)}{J + \Gamma_q^v} \xleftarrow{g_{J+\Gamma_q^v}'^\#} S_{\mathbb{F}_q}(m)\right)\end{aligned} \tag{147}$$

Thus by the completeness of $\mathbb{L}_{\mathrm{Cosp}}$ for ${}_F\,\mathrm{Cosp}(\mathsf{CAlg}_k^{\text{f.g.}})$, the following rewrite can be derived from just the rewrite rules of $\mathbb{L}_{\mathrm{Cosp}}$:



(148)

Thus, with lemma 6.8, we obtain the following series of rewrites:



(149)

Thus any two diagrams with the same semantic under $[-]_q$ are rewriteable into each other with the rules of $\mathbb{L}_{\mathrm{Span}_q}$. So $[-]_q$ is faithful. □

C.2 Proofs about $\mathrm{Mat}_{\mathbb{N}}$ semantics for $\mathbb{L}_{\mathrm{Span}_q}$

Proposition 6.12. *The functor M_q is well-defined and fully faithful.*

Proof. First consider the identity span $\mathbb{F}_q^n \xleftarrow{id} \mathbb{F}_q^n \xrightarrow{id} \mathbb{F}_q^n$. For each pair $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, it is clear that

$$M_q\left(\xleftarrow{id}\xrightarrow{id}\right)_{\mathbf{xy}} = \delta_{\mathbf{x},\mathbf{y}} \tag{150}$$

and so $M_q\left(\xleftarrow{id}\xrightarrow{id}\right)$ is the identity matrix.

Next suppose we have a composition of two structured spans of rational loci over $\mathbb{F}_q$:

$$\begin{tikzcd}[column sep=small] & & & V \times_{\psi,\phi'} W \arrow[dl, "\pi_V"'] \arrow[dr, "\pi_W"] & & & \\ & & V \arrow[dll, "\phi"'] \arrow[dr, "\psi"] & & W \arrow[dl, "\phi'"'] \arrow[drr, "\psi'"] & & \\ \mathbb{F}_q^n & & & \mathbb{F}_q^m & & & \mathbb{F}_q^{n'} \end{tikzcd}$$

The set of points in the pullback $V \underset{\psi,\psi'}{\times} W$ is the set of pairs $(\mathbf{v},\mathbf{w}) \in V \times W$ such that $\psi\mathbf{v} = \psi'\mathbf{w}$. So we compute, for $\mathbf{x} \in \mathbb{F}_q^n, \mathbf{z} \in \mathbb{F}_q^{n'}$:

$$\begin{aligned} & M\left(\xleftarrow{\phi}\xrightarrow{\psi}\xleftarrow{\phi'}\xrightarrow{\psi'}\right)_{\mathbf{xz}} \\ &= \left|\{(\mathbf{v},\mathbf{w}) \in V \times W : \psi\mathbf{v} = \phi'\mathbf{w}, \phi\mathbf{v} = \mathbf{x}, \psi'\mathbf{w} = \mathbf{z}\}\right| \\ &= \left|\bigcup_{\mathbf{y}\in\mathbb{F}_q^m}\left\{(\mathbf{v},\mathbf{w}) \in V \times W : {\phi\mathbf{v}=\mathbf{x} \atop \psi\mathbf{v}=\mathbf{y}}, {\phi'\mathbf{w}=\mathbf{y} \atop \psi'\mathbf{w}=\mathbf{z}}\right\}\right| \\ &= \sum_{\mathbf{y}\in\mathbb{F}_q^m}\left|\left\{\mathbf{v} \in V : {\phi\mathbf{v}=\mathbf{x} \atop \psi\mathbf{v}=\mathbf{y}}\right\} \times \left\{\mathbf{w} \in W : {\phi'\mathbf{w}=\mathbf{y} \atop \psi'\mathbf{w}=\mathbf{z}}\right\}\right| \\ &= \sum_{\mathbf{y}\in\mathbb{F}_q^m} M_q\left(\xleftarrow{\phi}\xrightarrow{\psi}\right)_{\mathbf{xy}} M_q\left(\xleftarrow{\phi'}\xrightarrow{\psi'}\right)_{\mathbf{yz}} \end{aligned} \tag{151}$$

and therefore,

$$M\left(\xleftarrow{\phi}\xrightarrow{\psi}\xleftarrow{\phi'}\xrightarrow{\psi'}\right) = M_q\left(\xleftarrow{\phi}\xrightarrow{\psi}\right) M_q\left(\xleftarrow{\phi'}\xrightarrow{\psi'}\right) \tag{152}$$

As required.

We now prove fullness and faithfulness separately. □

Lemma C.1. *The functor M_q is full.*

Proof. It's clear that the objects in the image of M_q are q^n, with $n \in \mathbb{N}$. Let A be an $\mathbb{N}$-matrix of dimensions $q^n \times q^m$, which we interpret as a function $A : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{N}$. Pick a number $N \in \mathbb{N}$ such that

$$q^N > \max_{\substack{\mathbf{x}\in\mathbb{F}_q^n \\ \mathbf{y}\in\mathbb{F}_q^m}} A_{\mathbf{xy}} \tag{153}$$

Then for $\mathbf{x} \in \mathbb{F}_q^n, \mathbf{y} \in \mathbb{F}_q^m$, we can find some subset $V_{\mathbf{xy}} \subset \mathbb{F}_q^N$ such that $|V_{\mathbf{xy}}| = A_{\mathbf{xy}}$. Then consider the set $V \subset \mathbb{F}_q^n \times \mathbb{F}_q^m \times \mathbb{F}_q^N$ defined by

$$V = \bigcup_{\substack{\mathbf{x}\in\mathbb{F}_q^n \\ \mathbf{y}\in\mathbb{F}_q^m}} \{\mathbf{x}\} \times \{\mathbf{y}\} \times V_{\mathbf{xy}} \tag{154}$$

Since every subset of affine spaces over $\mathbb{F}_q$ is an affine variety (this is a well-known elementary fact, see for example [31, 54]), so V is an affine variety. Then consider the structured span

$$\mathbb{F}_q^n \xleftarrow{\pi_x} V \xrightarrow{\pi_y} \mathbb{F}_q^m \tag{155}$$

where π_x, π_y are the restrictions of the projection maps

$$\mathbb{F}_q^n \leftarrow \mathbb{F}_q^n \times \mathbb{F}_q^m \times \mathbb{F}_q^N \to \mathbb{F}_q^m. \tag{156}$$

This is a morphism in ${}_{G_q}\,\mathrm{Span}(\mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)})$, and

$$M_q\left(\xleftarrow{\pi_x}\xrightarrow{\pi_y}\right)_{\mathbf{xy}} = |V_{\mathbf{xy}}| = A_{\mathbf{xy}} \tag{157}$$

Thus A is in the image of M_q. □

Lemma C.2. *The functor M_q is faithful.*

Proof. Suppose two structured spans of rational loci over $\mathbb{F}_q$ which are mapped by M_q to the same $\mathbb{N}$-matrix:

$$M_q\left(\mathbb{F}_q^n \xleftarrow{\phi} V \xrightarrow{\psi} \mathbb{F}_q^m\right) = M_q\left(\mathbb{F}_q^n \xleftarrow{\phi'} W \xrightarrow{\psi'} \mathbb{F}_q^m\right) \tag{158}$$

Then for each pair $\mathbf{x} \in \mathbb{F}_q^n, \mathbf{y} \in \mathbb{F}_q^m$, there exists some set-theoretic bijection

$$\sigma_{\mathbf{xy}} : \phi^{-1}(\mathbf{x}) \cap \psi^{-1}(\mathbf{y}) \to \phi'^{-1}(\mathbf{x}) \cap \psi'^{-1}(\mathbf{y}) \tag{159}$$

These bijections can be glued into

$$\begin{aligned} \sigma : & V \to W \\ & \mathbf{v} \mapsto \sigma_{\phi\mathbf{v},\psi\mathbf{v}}(\mathbf{v}) \end{aligned} \tag{160}$$

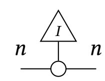
Since every function between rational loci over $\mathbb{F}_q$ is a polynomial mapping [31], so σ is a polynomial mapping. Moreover, by construction the following commutes:

$$\begin{tikzcd} & V \arrow[dl, "\phi"'] \arrow[dr, "\psi"] \arrow[dd, "\sigma"] & \\ \mathbb{F}_q^n & & \mathbb{F}_q^m \\ & W \arrow[ul, "\phi'"] \arrow[ur, "\psi'"'] & \end{tikzcd}$$

and therefore σ is a structured span isomorphism. □

D Proof of GAG as CSP

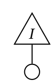
Proposition 7.1. *Let $\langle X, C\rangle$ be a CSP instance over the domain $\mathbb{F}_q$, with set of variables $X = \{x_1,\ldots,x_n\}$, and polynomial constraints $g_1,\ldots,g_m \in k[x_1,\ldots,x_n]$. Let I be the ideal generated by $g_1,\ldots,g_m$. Then the span semantic of the ideal gadget is*



$$\overset{[-]_q}{\mapsto} \left(\mathbb{F}_q^n \hookleftarrow V(I)^{\mathbb{F}_q} \hookrightarrow \mathbb{F}_q^n\right) \tag{42}$$

where, recall, $V(I)^{\mathbb{F}_q} := \{\mathbf{x} \in \mathbb{F}_q^n : g_1(\mathbf{x}) = \cdots = g_j(\mathbf{x}) = 0\}$. In other words, it is the set of assignments satisfying $\langle X, C\rangle$.

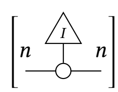
The same diagram with no wires on either side has the following matrix semantic:



$$\overset{[\![-]\!]_q}{\mapsto} \left|V(I)^{(\mathbb{F}_q)}\right| \tag{43}$$

In other words, it is the number of assignments that satisfy $\langle X, C\rangle$.

Proof. We know from proposition 5.9 that the *cospan semantic* of the ideal gadget is



$$= (S_k(n) \twoheadrightarrow S_k(n)/I \twoheadleftarrow S_k(n)) \tag{161}$$

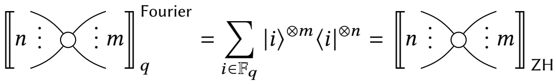
Hitting the cospan of algebras with the functor $\mathrm{Spec}(-)_{\mathrm{qred}} : \mathsf{CAlg}_{\mathbb{F}_q}^{\mathrm{f.g.}} \to \mathsf{AffVar}_{\mathbb{F}_q}^{(\mathbb{F}_q)}$ yields equation 42. Then equation 43 follows immediately by composing on both left and right legs with the projection $\mathbb{F}_q^n \xrightarrow{!} *$ where $*$ is the singleton. □

E Proofs about ZH calculus as an extension of GAG

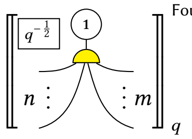
Proposition 8.6. *The functor ι_{ZH} is consistent with the semantics of the ZH Calculus. In other words, the following diagram commutes:*

$$\begin{tikzcd} \mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q} \arrow[r, "{[\![-]\!]_q^{\mathrm{Fourier}}}"] & q^{\frac{*}{2}}\,\mathrm{Mat}_{\mathbb{Z}[\omega]} \\ \mathrm{ZH} \arrow[u, "\iota_{\mathrm{ZH}}"] \arrow[ur, "{[\![-]\!]_{\mathrm{ZH}}}"'] & \end{tikzcd}$$

Proof. We check that the image of each generator of ZH under ι_{ZH} is mapped to the same matrix as under $\llbracket - \rrbracket_{\mathsf{ZH}}$.
Z-spider:



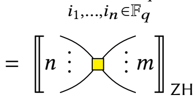
H-spider:



(162)

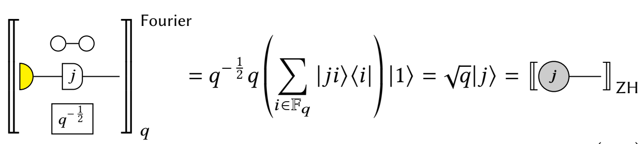
$$= \frac{1}{\sqrt{q}} \left(\sum_{\substack{j_1,\dots,j_m \in \mathbb{F}_q \\ i_1,\dots,i_n \in \mathbb{F}_q}} |j_1\rangle \dots |j_m\rangle\langle i_1| \dots \langle i_n| \otimes \langle j_1 \dots j_m i_1 \dots i_n| \right) \left(\sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(k)} |k\rangle \right) \tag{163}$$

$$= \frac{1}{\sqrt{q}} \sum_{\substack{j_1,\dots,j_m \in \mathbb{F}_q \\ i_1,\dots,i_n \in \mathbb{F}_q}} \omega^{\mathrm{tr}(j_1 \dots j_m i_1 \dots i_n)} |j_1\rangle \dots |j_m\rangle\langle i_1| \dots \langle i_n| \tag{164}$$



(165)

X-basis state:



(166)

□

Proposition 8.4. *The rewrite rules in equation* (47) *are sound with respect to the semantics* $\llbracket - \rrbracket_q^{\mathrm{Fourier}}$.

Proof. First we check the (Z1-copy)rule:

$$\llbracket L.H.S. \rrbracket_q^{\mathrm{Fourier}} = \left(\sum_{j,k \in \mathbb{F}_q} |j\rangle|k\rangle\langle j+k| \right) \left(\sum_{i \in \mathbb{F}_q} \omega^{\mathrm{tr}(i)} |i\rangle \right) \tag{167}$$

$$= \sum_{j,k \in \mathbb{F}_q} \omega^{\mathrm{tr}(j+k)} |j\rangle|k\rangle \tag{168}$$

$$= \left(\sum_{j \in \mathbb{F}_q} \omega^{\mathrm{tr}(j)} |j\rangle \right) \otimes \left(\sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(k)} |k\rangle \right) \tag{169}$$

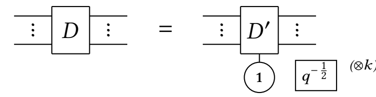
$$= \llbracket R.H.S. \rrbracket_q^{\mathrm{Fourier}} \tag{170}$$

Next we check the (Z1-del)rule:

$$\llbracket L.H.S. \rrbracket_q^{\mathrm{Fourier}} = \langle 0| \left(\sum_{i \in \mathbb{F}_q} \omega^{\mathrm{tr}(i)} |i\rangle \right) = \omega^{\mathrm{tr}(0)} = 1 = \llbracket R.H.S. \rrbracket_q^{\mathrm{Fourier}} \tag{171}$$

□

Proposition 8.7. *For any diagram D in $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$, there exists $k \in \mathbb{N}$ and a diagram D' containing only the generators of $\mathbb{L}_{\mathrm{Span}_q}$ such that*

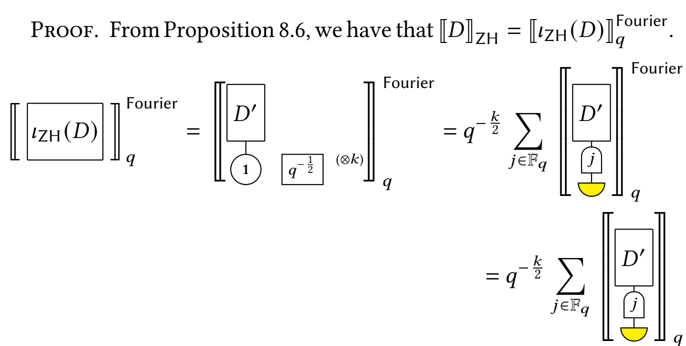


(50)

Proof. For all $\boxed{q^{-\frac{1}{2}}}$ in D, we can pull them out to the front of the diagram using the monoidal structure. Then we only need to consider the instances of the (1)— generator. This holds trivially if the diagram D contains a single instance of the (1)—. If there are two or more instances, we can use the (Z1-copy)rule to merge multiple instances into one. When there are no instances of (1)—, we can use the (Z1-del)rule in reverse to introduce one copy. □

Theorem 8.8. *Let D be a scalar diagram in the ZH calculus over $\mathbb{F}_q$. The scalar $\llbracket D \rrbracket_{\mathsf{ZH}}$ can be computed using exactly q queries to an oracle O that evaluates the semantics of scalar diagrams in $\mathbb{L}_{\mathrm{Span}_q}$.*

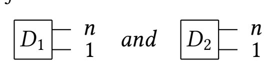
Proof. From Proposition 8.6, we have that $\llbracket D \rrbracket_{\mathsf{ZH}} = \llbracket \iota_{\mathsf{ZH}}(D) \rrbracket_q^{\mathrm{Fourier}}$.



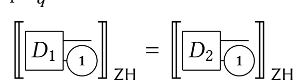
Thus, we can compute $\llbracket D \rrbracket_{\mathsf{ZH}}$ using q queries to the oracle O that computes $\llbracket - \rrbracket_q$ on scalar diagrams in $\mathbb{L}_{\mathrm{Span}_q}$. □

F Proofs about ZH completeness

Proposition 9.2. *If*

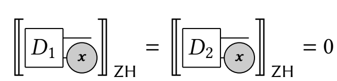


are diagrams in $\mathbb{L}_{\mathrm{Span}_q}$, such that



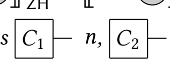
(52)

and satisfying the following restriction condition: for all $x \in \mathbb{F}_q$ except for those lying on one line $\xi\mathbb{F}_p$ where ξ is some fixed element of field trace 1,

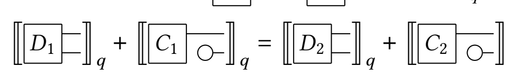


(53)

Then there exist diagrams

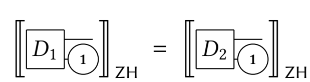


in $\mathbb{L}_{\mathrm{Span}_q}$ such that

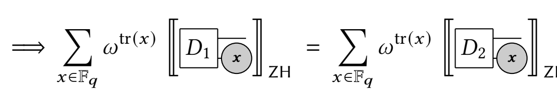


(54)

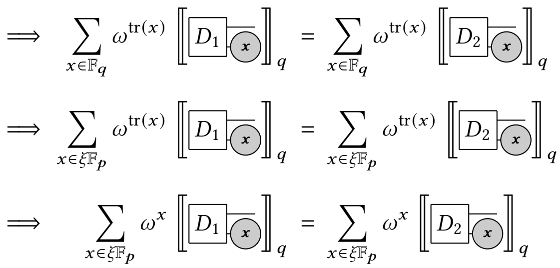
Proof.



(172)



(173)

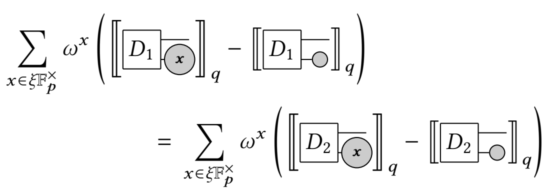


(174)

(175)

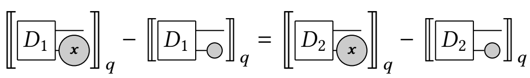
(176)

Using the fact that $\omega^0 = -\sum_{x\in\xi\mathbb{F}_p^\times}\omega^x$, we can rewrite the above as



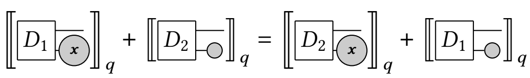
(177)

where $\xi\mathbb{F}_p^\times$ denotes the nonzero elements of $\xi\mathbb{F}_p$. Recall that the semantics $[\![-]\!]_q$ is a matrix with entries in $\mathbb{N}$, so the above is a linear combination of the $\{\omega^x\}_{x\in\xi\mathbb{F}_p^\times}$ with coefficients in $\mathbb{Z}$. Since $\{\omega^x\}_{x\in\xi\mathbb{F}_p^\times}$ are linearly independent over $\mathbb{Z}$, we have that for all $x\in\xi\mathbb{F}_p^\times$,



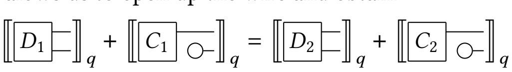
(178)

But note that the above holds trivially for $x=0$. So moving terms around, we have that for all $x\in\xi\mathbb{F}_p$,

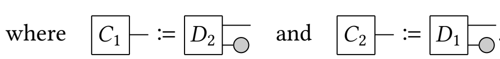


(179)

This alows us to open up the wire and obtain



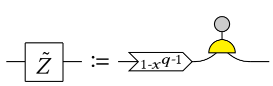
(180)



(181)

□

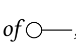
Lemma 9.3. *Let $\tilde{Z}$ be the following diagram in $\mathbb{L}_{\mathrm{Span}_q}$:*

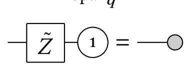


(55)

Then the following rewrites hold in $\mathbb{L}_{\mathrm{Span}_q}$:

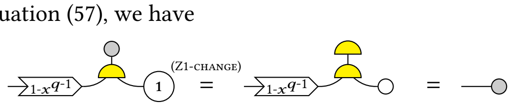
(56)

meaning that $\tilde{Z}$ serves as a controlled version of *; and moreover the following rewrite holds in $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$:*

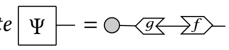
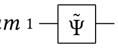


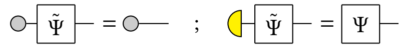
(57)

Proof. Equation (56) follows from the completeness of $\mathbb{L}_{\mathrm{Span}_q}$. For equation (57), we have



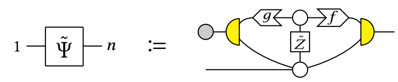
where the last equality follows from the completeness of $\mathbb{L}_{\mathrm{Span}_q}$. □

Lemma 9.4. *For any state*  *in $\mathbb{L}_{\mathrm{Span}_q}$, there is a diagram*  *(the so-called* controlled state *of ψ) such that the following are rewriteable in $\mathbb{L}_{\mathrm{Span}_q}$:*



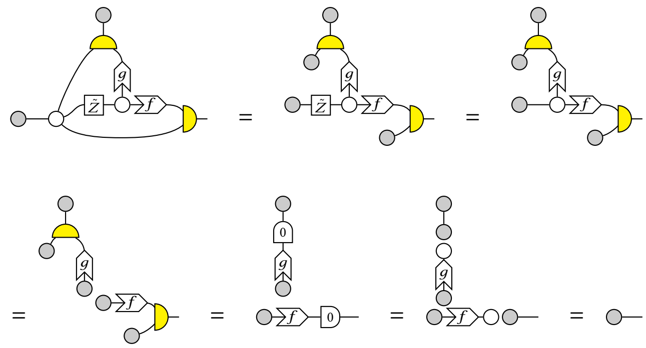
(59)

Explicitly, $\tilde{\psi}$ is constructed as

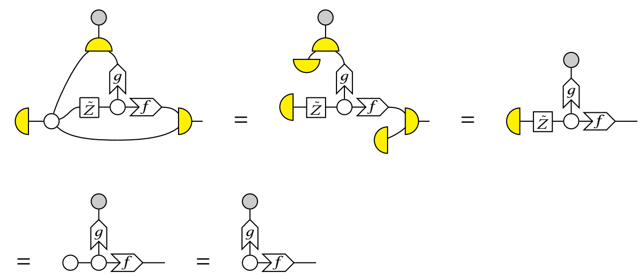


(60)

Proof. First, we verify by plugging in $|0\rangle$:

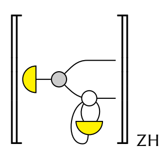


Next, we verify by plugging in $|1\rangle$:



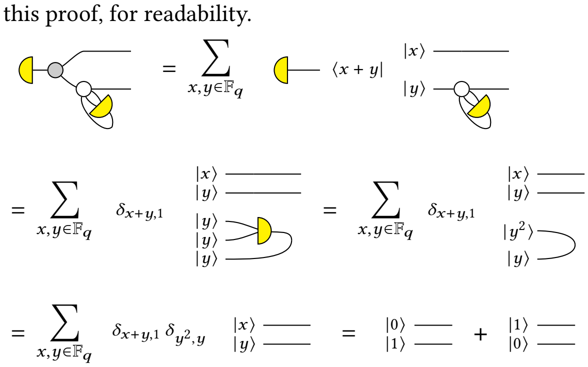
□

Lemma F.1.



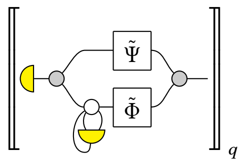
$$= \quad |01\rangle + |10\rangle \tag{182}$$

Proof. We will omit the semantics brackets $[\![-]\!]_{\mathrm{ZH}}$ for the rest of this proof, for readability.



□

Proposition 9.5. *For any states* $\boxed{\psi}-n$, $\boxed{\Phi}-n$ *in* $\mathbb{L}_{\mathrm{Span}_q}$, *let* $\tilde{\psi}, \tilde{\phi}$ *be their corresponding controlled states as defined in (60). Then the following diagram has the sum of* ψ *and* ϕ *as its semantics:*

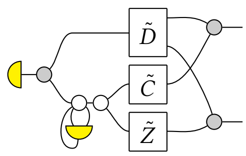


$$= \left[\!\left[\boxed{\Psi}- \right]\!\right]_q + \left[\!\left[\boxed{\Phi}- \right]\!\right]_q \tag{61}$$

Proof. This follows from the definition of controlled states (Lemma 9.4) and Lemma F.1. □

Proposition 9.6. *For diagrams* $\boxed{D}\,n$, $\boxed{C}-n$ *in* $\mathbb{L}_{\mathrm{Span}_q}$, *letting*

$\boxed{D_{+C}} :=$



(63)

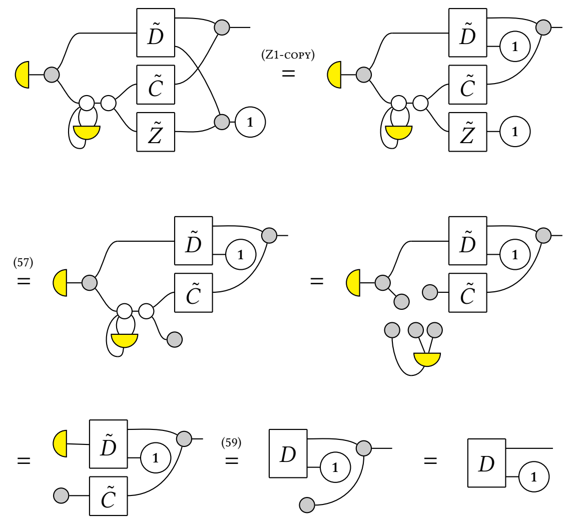
where $\tilde{D}, \tilde{C}, \tilde{Z}$ *are the corresponding controlled diagrams, then the following semantic equality of sums holds:*

$$\left[\!\left[\boxed{D_{+C}} \right]\!\right]_q = \left[\!\left[\boxed{D} \right]\!\right]_q + \left[\!\left[\boxed{C} \circ\!- \right]\!\right]_q \tag{64}$$

and moreover, the following rewrite holds in the language $\mathbb{L}^{\mathrm{Fourier}}_{\mathrm{Span}_q}$:

$$\boxed{D_{+C}}\!-\!(1) = \boxed{D}\!-\!(1) \tag{65}$$

Proof. Equation (64) follows from Proposition 9.5. Next, we prove equation (65).



□