Invariants of structures

Charlotte Aten
University of Colorado Boulder

The New York City Category Theory Seminar

2024 December 4

Introduction

- Example: Graphs
- Example: Associativity
- Background story: Bourbaki's structures
- Thesis results
- Structures
- Isomorphism invariant polynomials

Example: Graphs

- Fix a universe
$$A := \{a_1, \ldots, a_n\}.$$
- For each pair $\{a_i, a_j\} \in \binom{A}{2}$, we have a variable x_{ij}.
- Given a graph $\mathbf{G} = (A, f \subset \binom{A}{2})$, we can evaluate x_{ij} on $\mathbf{G}$ by
$$x_{ij}(\mathbf{G}) = \begin{cases} 1 & \text{when } \{a_i, a_j\} \in f \\ 0 & \text{otherwise} \end{cases}.$$

Example: Graphs

- That is, x_{ij} acts as the indicator function of the pair $\{a_i, a_j\}$.
- We can form monomials, such as

$$y = x_{12}x_{23}x_{31}.$$

- The natural notion of action inherited from the x_{ij} gives us

$$y(\mathbf{G}) = \begin{cases} 1 & \text{when } \{a_1, a_2, a_3\} \text{ is a clique in } \mathbf{G} \\ 0 & \text{otherwise} \end{cases}.$$

Example: Graphs

- This property is not invariant under permutations of the names of our vertices.
- A more well-behaved property is that of having a triangle.

Example: Graphs

- This corresponds to the polynomial

$$p = \sum_{\{a_i, a_j, a_k\} \in \binom{A}{3}} x_{ij} x_{jk} x_{ki}.$$

- This time we have

$$p(\mathbf{G}) = \# \text{ of triangles in } \mathbf{G}.$$

Example: Graphs

- I claim that every property of finite structures can be computed by evaluating at such polynomials.

Example: Associativity

- Fix a universe
$$A := \{a_1, \ldots, a_n\}.$$
- For each triple $(a_i, a_j, a_k) \in A^3$, we have a variable x_{ijk}.
- Given a ternary relational structure $\mathbf{A} = (A, f \subset A^3)$, we can evaluate x_{ijj} on $\mathbf{A}$ by
$$x_{ijk}(\mathbf{A}) = \begin{cases} 1 & \text{when } (a_i, a_j, a_k) \in f \\ 0 & \text{otherwise} \end{cases}.$$

Example: Associativity

- If $\mathbf{A} = (A, f)$ is a magma in the sense that f is the graph of a binary operation $A^2 \to A$ with $(a_i, a_j, a_k) \in f$ meaning that $f(a_i, a_j) = a_k$, then we can express associativity in terms of polynomials in the x_{ijk}.
- We have that

$$f(f(a_i, a_j), a_k) = a_\ell = f(a_i, f(a_j, a_k))$$

when there is exactly one witness to both

$$(\exists a_s)((a_i, a_j, a_s) \in f \wedge (a_s, a_k, a_\ell) \in f)$$

and

$$(\exists a_s)((a_i, a_s, a_\ell) \in f \wedge (a_j, a_k, a_s) \in f).$$

Example: Associativity

- These terms correspond to

$$\sum_{s=1}^{n} x_{ijs} x_{sk\ell}$$

and

$$\sum_{s=1}^{n} x_{is\ell} x_{jks},$$

respectively.

Example: Associativity

- This means that associativity corresponds to having

$$\sum_{i,j,k,\ell=1}^{n}\left(\sum_{s=1}^{n}(x_{ijs}x_{sk\ell}-x_{is\ell}x_{jks})\right)^2(\mathbf{A})=0.$$

Example: Associativity

- We can decompose this polynomial as

$$\sum_{i=j=k=\ell}\left(\sum_{s=1}^{n}(x_{ijs}x_{sk\ell}-x_{is\ell}x_{jks})\right)^2+$$

$$\sum_{i=j=k\neq\ell}\left(\sum_{s=1}^{n}(x_{ijs}x_{sk\ell}-x_{is\ell}x_{jks})\right)^2+$$

$$\sum_{i=j=\ell\neq k}\left(\sum_{s=1}^{n}(x_{ijs}x_{sk\ell}-x_{is\ell}x_{jks})\right)^2+$$

$$\cdots$$

Example: Associativity

- The first term

$$\sum_{i=j=k=\ell} \left(\sum_{s=1}^{n} (x_{ijs}x_{sk\ell} - x_{is\ell}x_{jks}) \right)^2 = \sum_{i=1}^{n} \left(\sum_{s=1}^{n} (x_{iis}x_{sii} - x_{isi}x_{iis}) \right)^2$$

is counting the number of times that $a_i(a_i a_i) = a_i(a_i a_i) = a_i$ fails to occur.

Background story: Bourbaki's structures

- In writing the textbook series *les Éléments de mathématique*, Bourbaki had sought to lay out in the first text of the series, *Theory of Sets* a systematic description of mathematical structures as they would appear throughout the rest of the series.

Background story: Bourbaki's structures

- Basically, they said that a *structure* was a set, say A, equipped with an indexed family $\{f_i\}_{i \in I}$ of *relations* f_i where each f_i was a subset of a set which could be constructed from A by taking Cartesian products and powersets finitely many times.
- For example, a relation on A might be a subset of

$$A \times \mathrm{Sb}(\mathrm{Sb}(A) \times A^{57}) \times \mathrm{Sb}(\mathrm{Sb}(\mathrm{Sb}(A))).$$

Background story: Bourbaki's structures

- Bourbaki defined what we would now call morphisms of these structures and proved several results about them, all of which we would now consider to belong to category theory.
- Once Eilenberg and Mac Lane had established category theory Grothendieck and then Cartier were asked to produce a category theory component for the *Éléments*, although if either did their contribution never made it into the texts.

Background story: Bourbaki's structures

- Discussions in «La Tribu» during the 1950s seem to indicate that Bourbaki felt much of the *Éléments* would have to be rewritten in order to accommodate the new notions from category theory.
- It appeared to be difficult to synthesize the structural and categorical viewpoints together, so the consensus became that this task was not worth the effort.

Thesis results

- In my thesis I presented one possible categorification of Bourbaki's concept of structure.
- The main result in this case is a generalization of a result of Hilbert on symmetric polynomials to the setting of finite structures.
- This generalization has the perhaps surprising implication that any first-order property of a finite structure $\mathbf{A}$ can be checked by counting the number of small substructures $\mathbf{B} \hookrightarrow \mathbf{A}$, where «small» is a function of the logical complexity of the first-order property.

Thesis results

- As Bourbaki imagined, the setup for this is a little involved and is relegated to an appendix.
- That appendix also contains a Yoneda-style embedding theorem which shows that categories of structures built from a set A may always be viewed as having basic relations of the form A^n as in model theory.

Structures

- Given an index category $\mathscr{I}$ and categories $\mathscr{C}$ and $\mathscr{D}$ we refer to a functor $\rho\colon \mathscr{I} \to \mathbf{Fun}(\mathscr{C}, \mathscr{D})$ as a *presignature*.
- In our examples before, $\mathscr{I}$ was the trivial category with one object and $\mathscr{C} = \mathscr{D} = \mathbf{Set}$.
- For graphs $\rho(\star)$ is the functor $A \mapsto \binom{A}{2}$.
- For ternary relational structures (like magmas) $\rho(\star)$ is the functor $A \mapsto A^3$.

Structures

- To each presignature we associate an *extractor*

$$\rho\_ : \mathscr{C} \to \mathbf{Fun}(\mathscr{I}, \mathscr{D}).$$

- The *extraction* of ρ at an object A of $\mathscr{C}$ is a functor

$$\rho_A : \mathscr{I} \to \mathscr{D}.$$

- A *signature* is a presignature which supports taking images in a certain sense.

Structures

Definition (Signature)

Given a presignature $\rho\colon \mathscr{I} \to \mathbf{Fun}(\mathscr{C}, \mathscr{D})$ we say that ρ is a $(\mathscr{C}, \mathscr{D})$-*signature* on the index category $\mathscr{I}$ when given any monomorphism $F\colon U \hookrightarrow \rho_A$ in $\mathbf{Fun}(\mathscr{I}, \mathscr{D})$ and any morphism $h\colon A \to B$ in $\mathscr{C}$ we have that $\mathrm{Im}(\rho_h \circ F)$ exists in $\mathbf{Fun}(\mathscr{I}, \mathscr{D})$.

- If $\mathscr{D}$ has all images and $\mathscr{I}$ is discrete then any presignature as above is a signature.

Structures

Definition (Structure)

Given a $(\mathscr{C}, \mathscr{D})$-signature ρ on an index category $\mathscr{I}$ and $A \in \mathrm{Ob}(\mathscr{C})$ we refer to a subobject $\mathbf{A}$ of ρ_A in the category $\mathbf{Fun}(\mathscr{I}, \mathscr{D})$ as a $(\mathscr{C}, \mathscr{D})$-*structure* of signature ρ on A (or as a ρ-*structure* when we want to emphasize the signature).

Structures

- Given a structure $\mathbf{A}$ on an object A of signature $\rho\colon \mathscr{I} \to \mathbf{Fun}(\mathscr{C}, \mathscr{D})$ and $N \in \mathrm{Ob}(\mathscr{I})$ we refer to the class of morphisms
$$\mathbf{A}_N := \{ F_N \mid F \in \mathbf{A} \}$$
in $\mathscr{D}$ as the *relation* of $\mathbf{A}$ at N.
- Morphisms of $\mathscr{I}$ similarly give us *relators* between relations.

Structures

- Let $\mathbf{A}$ be a structure on an object A of signature ρ and let $\mathbf{B}$ be a structure on an object B of signature ρ.
- We say that a morphism $h\colon A \to B$ is a *morphism* from $\mathbf{A}$ to $\mathbf{B}$ when $h(\mathbf{A}) \leq \mathbf{B}$ as subobjects of ρ_B.
- There is a category $\mathbf{Struct}^{\rho}$ of structures with a given signature.

Structures

Definition (Finite signature)

We say that a signature $\rho\colon \mathscr{I} \to \mathbf{Fun}(\mathbf{Set}, \mathbf{Set})$ is *finite* when $\mathscr{I}$ has finitely many objects and finitely many morphisms and for each $N \in \mathrm{Ob}(\mathscr{I})$ and each finite set A we have that $\rho_A(N)$ is finite.

Definition (Finite structure)

We say that a structure of finite signature ρ on a finite set is a *finite structure*.

Isomorphism invariant polynomials

- We denote by Struct_A^ρ the collection of all structures of the same signature on the set A, which we call a *kinship class*.
- The class Struct^ρ of all structures with signature ρ is likewise called a *similarity class*.

Isomorphism invariant polynomials

Definition (Substructure)

Given a structure $\mathbf{A}$ of signature ρ we refer to a subobject of $\mathbf{A}$ in $\mathbf{Struct}^{\rho}$ as a *substructure* of $\mathbf{A}$.

Isomorphism invariant polynomials

- Given a set of variables X the symmetric group Σ_X of permutations of X acts on the corresponding polynomial algebra $\mathbf{R}[X]$ for some unital commutative ring $\mathbf{R}$.
- The polynomials invariant under this action are the *symmetric polynomials*, which themselves form an $\mathbf{R}$-algebra.
- A classical result of Hilbert is that certain very simple *elementary symmetric polynomials* generate this algebra of all symmetric polynomials.

Isomorphism invariant polynomials

Definition (Variables X_A^ρ)

Given a finite signature ρ on an index category $\mathscr{I}$ and a finite set A we define

$$X_A^\rho := \bigcup_{N \in \mathrm{Ob}(\mathscr{I})} \{ x_{N,a} \mid a \in \rho_A(N) \} .$$

Isomorphism invariant polynomials

Definition (Monomial $y_{\mathbf{A}}$)

Given a finite signature ρ on an index category $\mathscr{I}$, a finite set A, and a structure $\mathbf{A} := (A, F) \in \mathrm{Struct}^{\rho}_{A}$ we define

$$y_{\mathbf{A}} := \prod_{N \in \mathrm{Ob}(\mathscr{I})} \prod_{a \in F(N)} x_{N,a}.$$

Isomorphism invariant polynomials

Definition ((ρ, A) polynomial algebra)

Given a commutative ring $\mathbf{R}$, a finite signature ρ, and a finite set A we define the (ρ, A) *polynomial algebra* over $\mathbf{R}$ to be the subalgebra of $\mathbf{R}[X_A^\rho]$ which is generated by Y_A^ρ. We denote this algebra by $\mathbf{Pol}_A^\rho(\mathbf{R})$.

Isomorphism invariant polynomials

Definition (Action υ)

We define a group action $\upsilon\colon \Sigma_A \to \mathbf{Aut}(\mathbf{R}[X_A^\rho])$ by setting $(\upsilon(\sigma))(x_{N,a}) := x_{N,(\rho_\sigma(N))(a)}$ and extending.

Definition (Symmetric polynomial)

A polynomial $p \in \mathrm{Pol}_A^\rho(\mathbf{R})$ is called *symmetric* when for every $\sigma \in \Sigma_A$ we have that $(\upsilon(\sigma))(p) = p$.

Isomorphism invariant polynomials

Definition (Action ζ)

We define a group action $\zeta\colon \Sigma_A \to \Sigma_{\mathrm{Struct}_A^\rho}$ by

$$(\zeta(\sigma))(A, F) := (A, \rho_\sigma \circ F).$$

Isomorphism invariant polynomials

Definition (Isomorphism classes of structures)

We define

$$\mathrm{IsoStr}^{\rho}_{A} := \left\{ \mathrm{Orb}_{\zeta}(\mathbf{A}) \;\middle|\; \mathbf{A} \in \mathrm{Struct}^{\rho}_{A} \right\}.$$

Definition (Elementary symmetric polynomial)

Given a finite signature ρ, a finite set A, and an isomorphism class $\psi \in \mathrm{IsoStr}^{\rho}_{A}$ we define the *elementary symmetric polynomial* of ψ to be

$$s_{\psi} := \sum_{\mathbf{A} \in \psi} y_{\mathbf{A}}.$$

- The elementary symmetric polynomials are symmetric polynomials.

Isomorphism invariant polynomials

Theorem (A. 2022)

Given a polynomial $f \in \mathrm{SymPol}_A^{\rho}(\mathbf{R})$ *of degree* d *there exists a polynomial* $g \in R[Z_A^{\rho}]$ *of weight at most* d *such that* $f = g|_{Z_A^{\rho} = S_A^{\rho}}$.

Isomorphism invariant polynomials

- The proof is inductive and follows a proof of Hilbert's result.
- We first show that monomials factor as

$$\prod_{i=1}^{k} y_{\mathbf{A}_i} = y_{\bigvee_{i=1}^{k} \mathbf{A}_i} \mu$$

  where $\mu \in \mathrm{Pol}_A^\rho$.
- We then induct on the size of the universe A.

Isomorphism invariant polynomials

- Supposing we have the result for a universe $B = \{a_1, \ldots, a_{n-1}\}$ and we want to show it for $A = \{a_1, \ldots, a_n\}$ we define

$$A_n := \bigcup_{N \in \mathrm{Ob}(\mathscr{I})} \{\, x_{N,a} \mid a \in \rho_A(N) \setminus \mathrm{Im}(\rho_\iota(N)) \,\}$$

  to be the collection of variables in X_A^ρ depending on a_n.
- Since

$$f|_{A_n=0} \in \mathrm{SymPol}_B^\rho(\mathbf{R})$$

  there exists some $g_1 \in R[Z_B^\rho]$ of weight at most d such that $f|_{A_n=0} = g_1|_{Z_B^\rho = S_B^\rho}$.

Isomorphism invariant polynomials

- We conclude by arguing that replacing the monomials appearing in this g_1 with the corresponding monomials over A yields a new polynomial, which we abusively also call g_1, such that
$$f = (g_1 + g_2)|_{Z^\rho_A = S^\rho_A}$$
where the additional term g_2 is also a symmetric polynomial.

References

- Charlotte Aten. “Finite Generation of Families of Structures Equipped with Compatible Group Actions.” PhD thesis. 2022, p. 61. ISBN: 9798363518454
- Charlotte Aten. “Invariants of structures.” In: *arXiv e-prints* (Feb. 2024). arXiv: 2402.18063 [math.CT]
- Nicolas Bourbaki. *Theory of Sets*. Elements of Mathematics. Spring-Verlag, 2004. ISBN: 978-3-540-22525-6

Thank you!