An (exhaustive enough) *Algebra of Programming* Summary*

Philip Kaluđerčić
philip.kaludercic@fau.de

Last updated for the Winter Semester 2023/24,† last typeset on April 10, 2024.

1 Algebra of Programming

1.1 Complete Partial Orders

Def. 1. A *(pointed directed-)complete partial order* (CPO) is a partially ordered set $(X, \sqsubseteq)$ with a *bottom element* $\bot$ and *joins* for all chains

$$\bot \sqsubseteq x_0 \sqsubseteq x_1 \sqsubseteq x_2 \sqsubseteq \cdots \sqsubseteq \bigsqcup_{i=0}^{\infty} x_i \in X.$$

Def. 2. A map on posets $\varphi : (X, \sqsubseteq) \to (X', \sqsubseteq')$ is *monotone* if for any $x, y \in X$, $x \sqsubseteq y \implies \varphi(x) \sqsubseteq \varphi(y)$.

Def. 3. A map on CPOs $\varphi : (X, \sqsubseteq) \to (X', \sqsubseteq')$ is *(Scott-)continuous* if is monotone and it preserves joins for all chains $\forall\, (x_i)_{i\in\mathbb{N}}$:

$$\bigsqcup_{i=0}^{\infty}{}' \varphi(x_i) = \varphi\left(\bigsqcup_{i=0}^{\infty} x_i\right)$$

Thm. 1 (Kleene)**.** For a CPO $(X, \sqsubseteq)$ and a continuous endomap $\varphi : (X, \sqsubseteq) \to (X, \sqsubseteq)$, the *smallest fixpoint* (i.e. some value x for which $x = \varphi(x)$, and $x \sqsubseteq y$ for any fixpoint y with $y = \varphi(y)$) is the supremum

$$\mu\varphi = \bigsqcup_{i=0}^{\infty} \varphi^i(\bot),$$

Sk. 1 where φ^i denotes the i-times application of φ .

Def. 4. A *pre-fixed point* of a $\varphi : (X, \sqsubseteq) \to (X, \sqsubseteq)$, is an element x for which $\varphi(x) \sqsubseteq x$.

1.2 F-Algebras

The concept of a F-Algebra provides a uniform approach to study inductive data types (such as natural numbers, lists, trees, …) and their recursion schemes.

Def. 5. In a category $\mathscr{C}$, given an object $A \in \mathsf{Ob}(\mathscr{C})$ and an endofunctor $F : \mathscr{C} \to \mathscr{C}$ the pair $A, a : F(A) \to A$ is called
Sk. 2 a *F-Algebra*. A F-Algebra-homomorphism $f : (A, a) \to (B, b)$ ensures $f \circ a = b \circ F(f)$. F-Algebras and F-Algebra-homomorphisms constitute a separate category $\mathbf{Alg}(F)$.

Def. 6. In $\mathbf{Alg}(F)$, for any (A, a), the initial object (I, i) (*initial F-Algebra*) has a unique (cata)morphism denoted $(\!|a|\!)$ from (I, i) to (A, a). The morphism $(\!|a|\!)$ is also frequently referred to as `fold`.

Def. 7 (Identity Law)**.** For any initial F-Algebra (I, i), $(\!|i|\!) = \mathrm{id}_I$ holds by initiality of (I, i).

Def. 8 (Fusion Law)**.** For any initial F-Algebra (I, i), arbitrary (A, a), (B, b) and a $f : (A, a) \to (B, b)$, $f \circ (\!|a|\!) = (\!|b|\!)$ holds by initiality of (I, i).

Def. 9. The functor of a F-Algebra can be extended by a *parameter category* $\mathscr{A}$ to $F : \mathscr{C} \times \mathscr{A} \to \mathscr{C}$. For some $A \in \mathsf{Ob}(\mathscr{A})$, the initial algebra of $F(-, A)$ is

$$(I(A), \iota_A : F(I(A), A) \to I(A)),$$

for a *type-functor* $I : \mathscr{A} \to \mathscr{C}$.

Lem. 1 (Lambek)**.** Given an initial F-Algebra (I, i), the structure morphism $i : F(I) \to I$ is an iso. Sk. 5

Def. 10. In a category $\mathscr{C}$ with an initial object $\top$ and an endofunctor $F : \mathscr{C} \to \mathscr{C}$, a ω*-chain* is a chain of morphisms $\top \xrightarrow{\mathsf{i}} F(\top) \xrightarrow{F(\mathsf{i})} F(F(\top)) \xrightarrow{F(F(\mathsf{i}))} \dots$, or alternatively the limit of the infinite shape $\mathscr{J} = \{\bullet \to \bullet \to \bullet \to \dots\}$, which is equivalent to the category of the poset $(\mathbb{N}, \leq)$.

Def. 11. A endofunctor $F : \mathscr{C} \to \mathscr{C}$ is ω-*<u>co</u>continuous* if it preserves colimits of ω-chains.

Def. 12. For a ω-<u>co</u>continuous endofunctor $F : \mathscr{C} \to \mathscr{C}$, the initial F-Algebra is Sk. 3

$$\mu F = \operatorname*{colim}_{n\in\mathbb{N}} F^n \top,$$

1.3 F-Coalgebra

The concept of a F-Coalgebra provides a uniform approach to study infinite data types (such as streams or formal languages) and discrete dynamical systems (such as automata).

Def. 13. In a category $\mathscr{C}$, given an object $A \in \mathsf{Ob}(\mathscr{C})$ and an endofunctor $F : \mathscr{C} \to \mathscr{C}$ the pair $A, a : A \to F(A)$ is called a *F-Coalgebra*. A F-Coalgebra-homomorphism $f : (A, a) \to (B, b)$ ensures $f \circ a = b \circ F(f)$. F-Coalgebras and F-Coalgebra-homomorphisms (which respect the system dynamics) constitute a separate category $\mathbf{Coalg}(F)$, which is **not** dual to $\mathbf{Alg}(F)$, but to $\mathbf{Alg}(F^{\mathrm{op}})$. Sk. 4

Despite that qualification, results like lemma 1 or definition 12 can mostly be derived analogously.

Def. 14. In $\mathbf{Coalg}(F)$, for any (A, a) the terminal object (T, t) (*terminal F-Coalgebra*) has a unique (ana)morphism denoted $[\![a]\!]$ from (A, a) to $(\nu F, t)$. $[\![a]\!]$ or `unfold` thus provides the existence of "definition principle" via *corecursion*.

Def. 15. A endofunctor $F : \mathscr{C} \to \mathscr{C}$ is ω-*continuous* if it preserves limits of ω-chains.

Def. 16. For a ω^{op}-continuous endofunctor $F : \mathscr{C} \to \mathscr{C}$, the terminal F-Coalgebra is

$$\nu F = \operatorname*{colim}_{n<\omega} F^n \bot.$$

Thm. 2 (Worwell)**.** For a finitary functor F, $\nu F = F^{\omega+\omega}1$, that is to say one extends and repeats the ω^{op}-chain, starting with $\nu F = F^{\omega}$ instead of $\bot$.

Def. 17. For a endofunctor $F : \mathbf{Set} \to \mathbf{Set}$ and two F-Coalgebra (C, c), (D, d) states $x \in C$, $y \in D$, are *behaviourally equivalent*, if for some (E, e),

$$x \sim y \iff \exists h, k.\, (C, c) \xrightarrow{h} (E, e) \xleftarrow{k} (D, d).$$

Def. 18. For a endofunctor $F : \mathbf{Set} \to \mathbf{Set}$ and two F-Coalgebra (C, c), (D, d), a *bisimulation* is a relation $R \subseteq C \times D$ (or $x \in C, y \in D$ are *bisimilar*) if $(R, r : R \to FR)$ is a F-Coalgebra with F-Coalgebra-morphisms to (C, c) and (D, d). Bisimulation implies behavioural equivalence . Sk. 13

*Based on and written in mind for the lecture "Algebra des Programmierens" (2023/24), as held by Prof. Dr. Stefan Milius at the Chair of Theoretical Computer Science, at the University of Erlangen-Nuremberg. The numbering used in this document for definitions and theorems differ from those used in the lecture notes.

†The LaTeX sources should be available under `https://gitlab.cs.fau.de/oj14ozun/algprog-summary`, or ought also be accessible as a PDF attachment: , see `git-bundle(1)`.

2 Category Theory

2.1 Categories

Def. 19. A *category* $\mathscr{C}$ consists of a class of *objects* $\mathsf{Ob}(\mathscr{C})$ and for any $X, Y \in \mathsf{Ob}(\mathscr{C})$ a set of *morphisms* $\mathrm{Hom}_{\mathscr{C}}(X,Y) \ni m$ ("Hom-set"), that relate the *domain* $X = \mathrm{dom}(m)$ with the *codomain* $Y = \mathrm{cod}(m)$.

Def. 20. If $\mathsf{Ob}(\mathscr{C})$ is a set, the category is called *small*.

Def. 21. For every $X, Y, Z \in \mathsf{Ob}(\mathscr{C})$, any two morphisms $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$ and $g \in \mathrm{Hom}_{\mathscr{C}}(Y,Z)$ can be *composed* $g \circ f \in \mathrm{Hom}_{\mathscr{C}}(X,Z)$ associativley.

Def. 22. For every $X, Y \in \mathsf{Ob}(\mathscr{C})$ there exists an *identity morphism* $\mathrm{id}_X \in \mathrm{Hom}_{\mathscr{C}}(X,X)$, for which the composition $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$ holds, given any $f : X \to Y$.

Def. 23. An *iso(morphism)* for a morphism $f : X \to Y$ if there exists a unique *inverse morphism* $g : Y \to X$ for which $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$ hold.

Def. 24. A morphism $f : X \to Y$ is a *mono(morphism)* if $f \circ g = f \circ g' \implies g = g'$ for all $g, g' : Z \to X$ and an *epi(morphism)* if $h \circ f = h' \circ f \implies h = h'$ for all $h, h' : Y \to Z$. Every iso is an epi and mono, but the converse is not necessarily true. ↝ Sk. 8

Def. 25. Any category $\mathscr{C}$, an *opposite category* $\mathscr{C}^{\mathrm{op}}$ is said to be *"dual"*. It is defined by reversing the direction of all morphisms, e.g. $f : X \to Y$ in $\mathscr{C}$ has a $f' : Y \to X$ in $\mathscr{C}^{\mathrm{op}}$.

Def. 26. A *functor* $F : \mathscr{C} \to \mathscr{D}$ consists of a mapping of objects and morphisms from $\mathscr{C}$ to $\mathscr{D}$, so that for all $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$, $g \in \mathrm{Hom}_{\mathscr{D}}(X',Y')$, each composition $F(g \circ f) = F(g) \circ F(f)$ and for each identity morphism id_X $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ holds.

Def. 27. An *endofunctor* is a functor with the same domain and codomain $F : \mathscr{C} \to \mathscr{C}$.

Def. 28. A *constant* functor $F : \mathscr{C} \to \mathscr{D}$ maps all objects to a fixed object $X \in \mathsf{Ob}(\mathscr{D})$ in the codomain, and all morphisms to id_X.

Def. 29. A functor $F : \mathscr{C} \to \mathscr{D}$ is called *faithful*, if the morphism map F is injective, *full*, if the F is surjective, *fully faithful*, if an iso is given between every object in $\mathsf{Ob}(\mathscr{D})$ and $\mathsf{Ob}(F(\mathscr{C}))$, and *equivalence*, if all of the above hold.

Def. 30. A (covariant) *Hom-functor* $\mathrm{Hom}_{\mathscr{C}}(X,-) : \mathscr{C} \to$ **Set** maps an object $X \in \mathsf{Ob}(\mathscr{C})$ to the set of morphism from X and morphism $f : Y \to Z$ to the extended compositions $\mathrm{Hom}_{\mathscr{C}}(X,f) : \mathrm{Hom}_{\mathscr{C}}(X,Y) \to \mathrm{Hom}_{\mathscr{C}}(X,Z)$, i.e. $g \mapsto f \circ g$.

A *contravariant Hom-functor* is otherwise defined identically on the dual category $\mathrm{Hom}_{\mathscr{C}}(-,X) : \mathscr{C}^{\mathrm{op}} \to$ **Set**, and pre-composes morphisms $g \mapsto g \circ f$, preserving the codomain X.

Def. 31. Given two functors $F, G : \mathscr{C} \to \mathscr{D}$, a *natural transformation* $\eta : F \to G$ (or $\eta : F \Rightarrow G$) is a family of *component morphisms* $\eta_C : F(C) \to G(C)$ indexed by $C \in \mathsf{Ob}(\mathscr{C})$, such that for all morphisms $f : X \to Y$ in $\mathscr{C}$

$$G(f) \circ \eta_X = \eta_Y \circ F(f).$$

Def. 32. A *natural isomorphism* $\eta : F \to G$ is an iso in the functor category $f c \mathscr{C} \mathscr{D}$, or equivalently a natural transformation where all component morphisms are isomorphic in $\mathscr{D}$. ↝ Sk. 6

Lem. 2 (Yoneda)**.** In any category $\mathscr{C}$, for every object $A \in \mathsf{Ob}(\mathscr{C})$ and every functor $F : \mathscr{C} \to$ **Set**, ↝ Sk. 7

$$\mathrm{Hom}_{\mathbf{Set}^{\mathscr{C}}}(\mathrm{Hom}_{\mathscr{C}}(A,-), F) \cong F(A).$$

2.2 Universal Constructions

Category theory emphasises the relations of objects via morphisms over objects and their "internal structure" or what they represent. Of specific interest are *constructions* of objects and morphisms that are uniquely identifiable by specific morphisms, usually unique morphisms between objects (i.e. $|\mathrm{Hom}_{\mathscr{C}}(A,B)| = 1$).

Def. 33. A *diagram* is a functor $F : \mathscr{J} \to \mathscr{C}$ maps a *shape* (or "scheme") $\mathscr{J}$ into $\mathscr{C}$. For a *cone* $(C, (f_j : C \to F(j))_{j \in \mathsf{Ob}(\mathscr{J})})$ (or a natural transformation from a constant functor of the *apex* C to the diagram) and any $u : j \to j'$ in $\mathscr{J}$, $f_{j'} = F(u) \circ f_j$ holds.

Def. 34. A *limit* $\left(L, (\pi_j : C \to F(j))_{j \in \mathsf{Ob}(\mathscr{J})}\right)$ is a *universal* cone, when ↝ Sk. 12

$$\forall j \in \mathsf{Ob}(\mathscr{J}) \forall C \in \mathsf{Ob}(\mathscr{C}) \exists ! h : C \to L.\, \pi_j \circ h = f_j.$$

As a morphism from a limit is unique up to iso , names of limits may refer both to the object C and the morphism h.

Def. 35. A *terminal object* $\bot$ of the limit L of the shape $\mathscr{J} = \{\bullet\}$. For any object $X \in \mathsf{Ob}(\mathscr{C})$ there exists a unique morphism $¡ : X \to L = \bot$.

Def. 36. A (binary) *product* of the limit L of the shape $\mathscr{J} = \{\bullet\ \bullet\}$ ((discrete) category restricted to identity morphisms).

Def. 37. A *pullback* is the limit L of the shape $\mathscr{J} = \{\bullet \to \bullet \leftarrow \bullet\}$ (a poset with a $\bot$-element).

Def. 38. A *equaliser* is the limit L of the shape $\mathscr{J} = \{\bullet \rightrightarrows \bullet\}$.

Every equaliser morphism e is a mono. If a mono is an equaliser, then it is called *regular*. A regular mono $m : X \to Y$ that is also an epi is consequently an iso . ↝ Sk. 11

Def. 39. If for a category every (finite, ie. the domain is a finite shape) shape has a limit, then it is said to be *(finitely) complete*.

Finite completeness of $\mathscr{C}$ if equivalent to $\mathscr{C}$ having finite products and equalisers *or* products and pullbacks *or* a terminal object and pullbacks . ↝ Sk. 9

Def. 40. A *colimit* $\left(K, (\iota_j : F(j) \to K)_{j \in \mathsf{Ob}(\mathscr{J})}\right)$ is a *cocone*, dual to a limit, and ensures

$$\forall j \in \mathsf{Ob}(\mathscr{J}) \forall C \exists ! h : K \to C.\, h \circ \iota_j = f_j.$$

Def. 41. A *initial object* $\top$ of the colimit K of the shape $\mathscr{J} = \{\bullet\}$. For any object $X \in \mathsf{Ob}(\mathscr{C})$ there exists a unique morphism $! : K \to X$ from $\top$. Dual construction of terminal objects.

Def. 42. A (binary) *coproduct* of the colimit K of the shape $\mathscr{J} = \{\bullet\ \bullet\}$, dual construction of products.

Def. 43. A *pushout* is the colimit K of the shape $\mathscr{J} = \{\bullet \leftarrow \bullet \to \bullet\}$ (a poset with a $\top$-element, **not** dual to pullback).

Def. 44. A *coequaliser* is the colimit K of the shape $\mathscr{J} = \{\bullet \rightrightarrows \bullet\}$.

Every coequaliser morphism e is an epi. If a epi is an coequaliser, then it is called *regular*. A regular epi $e : X \to Y$ that is also an mono is consequently iso.

Def. 45. If for a category every (finite) shape has a colimit, then it is said to be (finitely) *cocomplete*. This is dual to the notion of completeness.

Finite completeness of $\mathscr{C}$ is equivalent to $\mathscr{C}$ having finite coproducts and coequalisers *or* coproducts and pushouts *or* an initial object and pushouts . ↝ Sk. 10

A Prolegomena & Precedents

Ex. 1. The category **Set** has sets as objects and morphisms $\mathrm{Hom}_{\mathbf{Set}}(X, Y)$ are all functions between the sets X and Y. In set-theory, (total) functions are defined as relation $f \subseteq X \times Y$ satisfying the conditions of totality and univalence:

$$\forall x \in X \exists y \in Y. (x, y) \in f \qquad (\text{“left-total”})$$

$$(x, y) \in f \wedge (x, y') \in f \implies y = y' \qquad (\text{“right-unique”})$$

Properties and Constructions in Set Since **Set** is complete, all the constructions in the following exist:

Monos are injective functions $f : X \to Y$,
$$\forall x, y \in X. f(x) = f(y) \implies x = y$$
and are always regular.

Epis are surjective functions, $f : X \to Y$
$$\forall y \in Y \exists x \in X. f(x) = y$$
and are always regular.

Isos are bijective functions, $\forall x \in X \exists! y \in Y. f(x) = y$.

Terminal objects are singleton sets $\{y\}$, for any $y \in Y$, as for any domain X we can construct a function
$$t = \{(x, y) | \forall x \in X\},$$
that is the constant function $x \mapsto y$. These are unique up to isomorphisms.

Initial objects are empty sets $\{\}$, as for an empty domain $X = \{\}$, both properties of functions are trivially given (universal quantification over an empty set).

Products are cartesian products $X \times Y$.

Coproducts are disjoint unions $X \uplus Y$.

Equalisers of two functions $f, g : X \to Y$ is the set
$$\mathrm{Eq}(f, g) \coloneqq \{x \in X \mid f(x) = f(x)\}.$$

Coequalisers of two functions $f, g : X \to Y$ is $Y/_\sim$, where $\sim \subseteq Y \times Y$ is the smallest equivalence relation for which $\forall y \in Y. f(y) \sim g(y)$.

Pullbacks of two functions $f : X \to Z$ to $g : Y \to Z$ is the set
$$\mathrm{Pb}(f, g) \coloneqq \{(x, y) \in X \times Y \mid f(x) = g(y)\}.$$

Pushouts of two functions $f : Z \to X$ to $g : Z \to Y$ where $\sim \subseteq X \times Y$ is the smallest equivalence relation for which $\forall z \in Z. f(z) \sim g(z)$.

Initial F-Algebras Examples include $F(X) = \ldots$

$1 + X$ are natural numbers,

$1 + A \times X$ are lists,

$A + X^2$ are binary trees,

$\prod_{\sigma \in \Sigma} X^{\mathrm{ar}\,\sigma}$, *Term-* or *Σ-algebra*, over a set of operations Σ and an arity function $\mathrm{ar} : \Sigma \to \mathbb{N}$.

Terminal F-Coalgebras Examples include $F(X) = \ldots$

$A \times X$ infinite streams,

$A \times X^\Sigma$ Moore automata,

$(A \times X)^\Sigma$ Mealy automata,

$2 \times X^\Sigma$ finite deterministic automata,

$2 \times (\mathcal{P}_f(X))^\Sigma$ finite non-deterministic automata (where $\mathcal{P}_f$ is the finite powerset-functor),

$\mathcal{P}(X)$ unlabeled transition systems (effectively digraphs),

$\mathcal{P}(A \times X)$ labeled transition systems,

$\coprod_{\sigma \in \Sigma} X^{\mathrm{ar}\,\sigma}$ codatatypes over a Σ-algebra.

Ex. 2. Given the categories $\mathscr{C}$ (small) and $\mathscr{D}$, the *functor category* $\mathscr{D}^{\mathscr{C}}$ has functors $F : \mathscr{C} \to \mathscr{D}$ as objects and natural transformations $\eta : F \to G$ as morphisms.

Ex. 3. The category $\mathbf{Vec}_k$ has k-dimensional vector spaces as objects and linear transformations as morphisms. That means that objects are spaces like $\mathbb{R}^k$ and morphisms $f : X \to Y$ are restricted to linear transformations that for $x, x' \in X$ and a scalar a ensure
$$f(a \cdot x + x') = a \cdot f(x) + f(x').$$

Ex. 4. The category **Gra** has di(-rected)graphs (V, E) as objects and graph homomorphisms as morphisms. That means that a morphism $f : \mathfrak{A} \to \mathfrak{B}$ have to preserve strongly connected components, i.e.
$$\forall a, b \in V(X). a \sim_{E(\mathfrak{A})} b \implies f(a) \sim_{E(\mathfrak{B})} f(b),$$
where $x \sim_{E(\mathfrak{G})} y$ says that there is a path from x to y in the digraph $\mathfrak{G}$, over the transitive-reflexive closure of edges.

The initial object are therefore the empty graph $V = \{\}$, since there are no components to be preserved, and the terminal object is the single-vertex graph $V = \{\bullet\}$, since it melds all strongly connected components into one (trivially) connected component.

Ex. 5. The category generate by a *partially ordered set* (poset) $(X, \leq)$ has elements of X as objects and morphisms defined as
$$\mathrm{Hom}_{(X,\leq)}(x, y) = \{(x, y) \mid x \leq y\}$$
represent each “less than” relation.

A poset may include a “greatest” element $\top$ and “least” element $\bot$, s.t. $\forall a \in X. \bot \leq a \leq \top$. These correspond to the terminal and initial objects respectively. Products are correspond to the greatest lower bound (*meet*, “$\wedge$”), as for any $x, y \in X$, $x \wedge y \leq x$ and $x \wedge y \leq y$. Coproducts analogously correspond to the least upper bound (*join*, “$\vee$”).

Ex. 6. The category **Pos** of partial orders and monotone functions. Note the difference to the category of *a* poset, in the sense that **Pos** is one “level above” each $(X, \leq)$, even if that forms a category of its own.

Ex. 7. In Algebra, a monoid $(M, \cdot : M \times M \to M, e)$ is a “set M with structure”, given by a binary operation $\cdot$ and a neutral element e, s.t. $\forall a, b, c \in M$
$$(a \cdot b) \cdot c = a \cdot b \cdot c = a \cdot (b \cdot c)$$
$$e \cdot a = a = a \cdot e$$

Examples include

$(\mathbb{N}, +, 0)$ Addition of natural numbers with 0 as a the neutral element.

$(\mathbb{N}, \times, 1)$ Multiplication of natural numbers with 1 as the neutral element.

$(\Sigma^\star, \oplus, \varepsilon)$ Concatenation of strings over some alphabet Σ with the empty string ε as the neutral element.

These properties rhyme with categories, and we can view each monoid as a small category with a single object $\mathsf{Ob}((M, \cdot, e)) = \{\bullet\}$ and morphisms corresponding to elements of the carrier set M
$$\mathrm{Hom}_{(M,\cdot,e)}(\bullet, \bullet) = M.$$

Ex. 8. The category **Mon** of have monoids as objects, and Monoid homomorphisms as morphisms. That means, a morphism $f : (M, \cdot_M, e_M) \to (N, \cdot_N, e_N)$ has to obey
$$f(x \cdot_M y) = f(x) \cdot_N f(y)$$
$$f(e_M) = e_N$$
for all $x, y \in M$.

Ex. 9. The category **Rel** has sets as objects and defines morphisms as arbitrary $\mathrm{Hom}_{\mathbf{Rel}}(X, Y) \subseteq X \times Y$.

Rel is *self-dual*, since $\mathbf{Rel}^{\mathrm{op}} \cong \mathbf{Rel}$.

Ex. 10. The category **Par** is comparable to **Set**, just by extending the morphisms from total to partial functions $f : X \to Y$ (not necessarily defined for every element in X).

Ex. 11. The category **Top** has topological spaces $(X, \mathcal{O}_X \subseteq \mathcal{P}(X))$ as objects and continuous functions as morphism.

B Sketches of the Proofs

NOTEME: The proofs in this section make no claim to be rigorous, just to convey an approximate approach taken in proving claims made in the lecture.

The document source is publicly available (see the frontpage), so any and all comments are much appreciated.

Sk. 1. The smallest fixpoint a continuous φ on a CPO $(X, \sqsubseteq)$ is $\mu\varphi$ (c.f. theorem 1).

Proof. This is a two-step proof. First we want to show that $\mu\varphi$ *is* a fixpoint, which be seen by equational reasoning

$$\underline{\varphi(\mu\varphi)} = \varphi\left(\bigsqcup_{i=0}^{\infty} \varphi^i(\bot)\right) \qquad \text{(expand def.)}$$

$$= \bigsqcup_{i=0}^{\infty} \varphi^{i+1}(\bot) = \bigsqcup_{i=1}^{\infty} \varphi^i(\bot) \qquad \text{(continuity)}$$

N.B.: Suprema are invariant under omission of finitely many elements of an infinite chain, so we can safely add the bottom element:

$$= \varphi^0(\bot) \sqcup \bigsqcup_{i=1}^{\infty} \varphi^i(\bot)$$

$$= \bigsqcup_{i=0}^{\infty} \varphi^i(\bot) = \underline{\mu\varphi} \qquad \text{(contract def.)}$$

To see that $\mu\varphi$ is the *smallest* fixpoint, consider any x — for which $\varphi(x) = x$ must hold — and the chain of inference

$$\bot \sqsubseteq x$$

$$\Longrightarrow \quad \varphi(\bot) \sqsubseteq \varphi(x) = x \qquad (\varphi \text{ is mono.})$$

$$\Longrightarrow \quad \varphi^2(\bot) \sqsubseteq \varphi^2(x) = \varphi(x) = x$$

$$\vdots \qquad \text{(i.e. induction)}$$

$$\Longrightarrow \quad \underline{\mu\varphi} = \bigsqcup_{i=0}^{\infty} \varphi^i(\bot) \sqsubseteq \bigsqcup_{i=0}^{\infty} \varphi^i(x) = \underline{x}$$

which demonstrates that respective to $\sqsubseteq$, $\mu\varphi$ must be "smaller" that any x. This concludes the entire proof. ∎

Sk. 2. Given an endofunctor F in $\mathscr{C}$, $\mathbf{Alg}(F)$ constitute a category.

Proof. Knowing the *objects* of $\mathbf{Alg}(F)$ are pairs (A, a), s.t. $FA \xrightarrow{a} A$ is a morphism in $\mathscr{C}$ and the *morphisms* of $\mathbf{Alg}(F)$ are morphisms $f : (A, a) \to (B, b)$ in $\mathscr{C}$ s.t. $f \circ a = b \circ F(f)$, we only need to justify that the properties of morphisms hold:

Identity For any (A, a), we can re-use id_A from $\mathscr{C}$, since

$$a = \mathrm{id}_A \circ a = a \circ F(\mathrm{id}_A) = a \circ \mathrm{id}_{FA} = a \circ \mathrm{id}_A = a.$$

Composition For any (A, a), (B, b) and (C, c) with $f : (A, a) \to (B, b)$ and $g : (B, b) \to (C, c)$, we know a that $g \circ f : (A, a) \to (C, c)$ must exist, as

$$g \circ f \circ a = c \circ F(g \circ f)$$

$$g \circ \underline{f \circ a} = \underline{c \circ F(g)} \circ F(f)$$

$$g \circ b \circ F(f) = \underline{g \circ b} \circ F(f),$$

where the underlined left and right terms respectively make use of the commutativity inherent in f and g. ∎

Sk. 3. The colimit μF of a ω-cocontinuous ω-chain is the initial F-Algebra.

Proof. To construct a unique morphism from $(\mu F, i)$ to an arbitrary F-Algebra (A, a), one needs to construct a cocone over the ω-chain with A as the coapex. For every element $F^n(\top)$ this morphism is

$$\underbrace{a \circ F(a) \circ F^2(a) \circ \ldots}_{n \text{ times}} \circ F^n!,$$

where $! : \top \to A$. The idea is that every element of the ω-chain is mapped from $F^n(\top)$ to $F^n(A)$ and then "reduced" to A via lifted applications of $a : F(A) \to A$.

There will be a unique morphism from μF to this A that can also be mapped under F to produce a F-Algebra-morphism. ∎

Sk. 4. Given an endofunctor F, $\mathbf{Coalg}(F)$ constitute a category.

Proof. This proof is dual to sketch 2. ∎

Sk. 5. The morphism $i : FI \to I$ of the initial F-Algebra (I, i) is an iso (c.f. lemma 1).

Proof. To prove that i is an isomorphism, we need to construct an inverse $i^{-1} : I \to FI$ in $\mathbf{Alg}(F)$.

Given the initial F-Algebra (I, i) we derive a further object (FI, Fi), for which there must exist a unique morphism $(\!|Fi|\!) : (I, i) \to (FI, Fi)$, which corresponds to i^{-1}. As (I, i) is initial, id_{FI} is the only morphism to (FI, Fi), hence $\mathrm{id}_I = i \circ i^{-1}$. The opposite direction, follows by equational reasoning:

$$\underline{i^{-1} \circ i} = Fi \circ Fi^{-1} \qquad \text{(comm. of cata.)}$$

$$= F(i \circ i^{-1}) \qquad \text{(prop. functor)}$$

$$= F(\mathrm{id}_I) \qquad \text{(see above)}$$

$$= \underline{\mathrm{id}_{FI}}$$

∎

Sk. 6. All component morphisms of a natural iso are isomorphic functors, and *vice versa*.

Proof. Assuming η is a natural iso (i.e. there is a η^{-1}) — i.e. an iso in $\mathscr{D}^{\mathscr{C}}$ – we have to prove that every $\eta_A : F(A) \to G(A)$ is an iso (i.e there is a $\eta_A{}^{-1}$). This can be trivially constructed by indexing η^{-1} by A, attaining $\eta_A^{-1} : G(A) \to F(A)$. The uniqueness of η_A^{-1} is inherited from the uniqueness of η^{-1}.

Assuming every η_A is an iso, we have to prove that η is an iso in $\mathscr{D}^{\mathscr{C}}$: This requires the construction of a family of morphisms $(\eta_A{}^{-1})_{A \in \mathsf{Ob}(\mathscr{C})}$ which are given by η_A being isos. In addition, the naturality condition must be verified. ∎

Sk. 7. There exists a (set-theoretical) bijection between the application of $A \in \mathsf{Ob}(\mathscr{C})$ on a functor $F : \mathscr{C} \to \mathbf{Set}$ and the morphisms between hom-functors from A to the functor F in the category of functors (c.f. lemma 2).

Proof. The proof of a bijection requires the construction of two functions, mapping between the two sets in opposite directions:

$$\aleph : \mathrm{Hom}_{\mathbf{Set}^{\mathscr{C}}}(\mathrm{Hom}_{\mathscr{C}}(A, -), F) \to F(A)$$

$$\aleph(\eta) = \eta_A\,(\mathrm{id}_A)$$

$$\beth : F(A) \to \mathrm{Hom}_{\mathbf{Set}^{\mathscr{C}}}(\mathrm{Hom}_{\mathscr{C}}(A, -), F)$$

$$\beth(x) = (h \mapsto (F(h))(x))_{B \in \mathsf{Ob}(\mathscr{C})}$$

These are their mutual inverse functions, as can be seen by equational reasoning. Given an $x \in F(A)$ and $\eta \in \mathrm{Hom}_{\mathbf{Set}^{\mathscr{C}}}(\mathrm{Hom}_{\mathscr{C}}(A, -), F)$,

$$\aleph(\underline{\beth(x)}) = \underline{\aleph}\,(h \mapsto (Fh)(x))$$

$$= (h \underline{\mapsto} (Fh)(x))\,\underline{(\mathrm{id}_A)}$$

$$= (\underline{F\mathrm{id}_A})(x) = \underline{\mathrm{id}_{FA}}(x) = x$$

and conversely for a $\eta \in \mathrm{Hom}_{\mathbf{Set}^{\mathscr{C}}}(\mathrm{Hom}_{\mathscr{C}}(A,-),F)$ and $m : A \to B$

$$\begin{aligned}
ב(\underline{\aleph(\eta_A)})(m) &= \underline{ב}\,(\eta_A\,(\mathrm{id}_A))\,(m) \\
&= (h\underline{\mapsto} Fh\,(\eta_A\,(\mathrm{id}_A)))\underline{(m)} \\
&= Fm\,(\eta_A\,(\mathrm{id}_A)) \qquad (*) \\
&= \eta_A\left(\underline{\mathrm{Hom}_{\mathscr{C}}(A,m)(\mathrm{id}_A)}\right) \\
&= \eta_A\left(\underline{m \circ \mathrm{id}_A}\right) = \eta_A\,(m)
\end{aligned}$$

Furthermore, for $(*)$ to work, one has to prove that for an x, $ב(x)$ actually constructs a natural transformation, by verifying the naturality condition,

$$Fm \circ ב(x) = ב(x) \circ \mathrm{Hom}_{\mathscr{C}}(A,m)$$

for an arbitrary $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$:

$$\begin{aligned}
Fm((\underline{ב(x)})(f)) &= (\underline{ב(x)})(\mathrm{Hom}_{\mathscr{C}}(A,m)(f)) \\
Fm(\underline{(h \mapsto Fh)(f)}) &= (h \mapsto Fh)(\underline{\mathrm{Hom}_{\mathscr{C}}(A,m)(f)}) \\
\underline{Fm(Ff)} &= \underline{(h \mapsto Fh)}(mf) \\
F(mf) &= F(mf)
\end{aligned}$$

■

Sk. 8. Every iso $f : X \to Y$ is a mono and epi, but not always conversely.

Proof. For any $g, h : Z \to X$

$$fg = fh \iff \underbrace{f^{-1}f}_{\mathrm{id}_X} g = \underbrace{f^{-1}f}_{\mathrm{id}_X} h \iff g = h,$$

and analogously for epi.

The reverse does not hold: In posets $(X, \leq)$ all morphisms are epi and mono, since for $x, y, z \in X$

$$x \leq y \leq z \implies x \leq y \wedge y \leq z,$$

i.e. shortening the pre- and post-composition, but only identity morphisms are iso, since

$$x \leq y \wedge y \leq x \iff x = y.$$

■

Sk. 9. A category $\mathscr{C}$ is finitely complete...

$$\begin{aligned}
&\iff \mathscr{C} \text{ has finite products and equaliser} && (1) \\
&\iff \mathscr{C} \text{ has finite products and pullback} && (2) \\
&\iff \mathscr{C} \text{ has terminal object and pullback} && (3)
\end{aligned}$$

Proof. Considering the “ $\Longleftarrow$ ” direction for each sub-claim:

(1) Given an arbitrary shape $\mathscr{J}$ and diagram $F : \mathscr{J} \to \mathscr{C}$, construct for an arbitrary morphism h in $\mathscr{J}$

$$\begin{tikzcd}
 & F(\mathrm{dom}(h)) \arrow[rr, "Fh"] & & F(\mathrm{cod}(h)) \\
E \arrow[r, "e"] & \prod\limits_{j \in \mathsf{Ob}(\mathscr{J})} Fj \arrow[u, "\pi_{\mathrm{dom}\,h}"] \arrow[rr, shift left, "\left\langle Fm \circ \pi_{\mathrm{dom}(m)} \right\rangle"] \arrow[rr, shift right, "\left\langle \pi_{\mathrm{cod}(m)} \right\rangle"'] \arrow[rrd, "\pi_{\mathrm{cod}\,h}"'] & & \prod\limits_{j \in \mathsf{Mor}(\mathscr{J})} F(\mathrm{cod}\,j) \arrow[u, "\pi_h"'] \arrow[d, "\pi_h"] \\
 & & & F(\mathrm{cod}(h))
\end{tikzcd}$$

where $\mathsf{Mor}(\mathscr{J}) = \bigcup_{j,j' \in \mathsf{Ob}(\mathscr{J})} \mathrm{Hom}_{\mathscr{J}}(j,j')$ is the set of all morphisms in $\mathscr{J}$.

The morphism $\lambda_j := \pi_j \circ e$ span a cone $\left(E, (\lambda_j)_{j \in \mathsf{Ob}(\mathscr{J})}\right)$, that inherits its universal property from that of the equaliser e.

(2) Equalisers of two morphisms $m, n : A \to B$ are pullbacks of the form $A \xrightarrow{m} B \xleftarrow{n} A$. Given this fact, we can reduce the proof to that finite products and equaliser.

(3) Products $A \times B$ are pullbacks of the form $A \to \perp \leftarrow B$. Equalisers can be constructed analogously to the second point. Using these constructions, the proof can be reduced to (1).

The opposite direction ($\mathscr{C}$ is complete $\implies \mathscr{C}$ has ...) is trivial, since finite completeness (i.e. has limits for any finite shape) is sufficient to construct any terminal object, product, equaliser or pullback. ■

Sk. 10. A category $\mathscr{C}$ being finitely cocomplete is equivalent to $\mathscr{C}$ having finite coproducts and coequalisers *or* coproducts and pushouts *or* an initial object and pushouts.

Proof. As colimits are dual to limits, we can *dualize* and refer to sketch 9. ■

Sk. 11. If a regular mono m is also epi, then m is an iso.

Proof. If $m : A \to B$ is regular mono, there must exist some $f, g : C \to A$ for which

$$f \circ m = g \circ m \implies f = g,$$

since m is epi as well. For m to be the equaliser of the same morphism twice, it is necessary for idB to be a possibly other equaliser of f and g, since

$$f = g \implies f \circ \mathrm{id}_B = g \circ \mathrm{id}_B.$$

Consequently there must be a unique $m^{-1} : B \to A$, so that $m^{-1} \circ m = \mathrm{id}_B$ holds, which demonstrates that m is an iso. An overview of this proof is found in this commutative diagram:

$$\begin{tikzcd}
A \arrow[r, "m"] & B \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & C \\
B \arrow[u, dotted, "m^{-1}"] \arrow[ur, "\mathrm{id}_B"'] & &
\end{tikzcd}$$

See sketch 8 for an example that a non-regular mono is insufficient. ■

Sk. 12. Limits are unique up to iso.

Proof. Assume two L and L' are limits for any shape $\mathscr{J}$. Then there must exist a unique morphism from L to L' and vice versa, which is the isomorphism. ■

Sk. 13. Bisimulation implies behavioural equivalence.

Proof. Given a bisimulation $(C,c) \xleftarrow{\pi_1} (R,r) \xrightarrow{\pi_2} (D,d)$ we can construct a pullback $\mathsf{Pb}(\pi_1,\pi_2) = (P,p)$. In **Set** this exist necessarily, meaning that the cone morphisms $(C,c) \xrightarrow{p_1} (P,p) \xleftarrow{p_2} (D,d)$ provide the intended behavioural equivalence. ■

References

[1] Jiří Adámek, Horst Herrlich, and George Strecker. *Abstract and concrete categories*. USA: Wiley-Interscience, 1990. ISBN: 0471609226. URL: http://katmat.math.uni-bremen.de/acc.

[2] Richard Bird and Oege de Moor. *Algebra of programming*. USA: Prentice-Hall, Inc., 1997. ISBN: 013507245X.

[3] Florian Guthmann. *Algebra of Programming – A Rival Summary*. 2024. URL: https://wwwcip.cs.fau.de/~oc45ujef/lectures/algprog/summary.html.

[4] Bart Jacobs. *Introduction to Coalgebra: Towards Mathematics of States and Observation*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2016.

[5] Saunders Mac Lane. *Categories for the working mathematician*. Vol. 5. Springer Science & Business Media, 2013.

[6] Bartosz Milewski. *Category theory for programmers*. Blurb, 2018. URL: https://bartoszmilewski.com/2014/10/28/.

[7] Benjamin C. Pierce. *Basic category theory for computer scientists*. Cambridge, MA, USA: MIT Press, 1991. ISBN: 0262660717.

[8] Jan J.M.M. Rutten. *Universal coalgebra: a theory of systems*. Tech. rep. NLD, 1996. URL: https://ir.cwi.nl/pub/48/0048D.pdf.