Mathematical foundations for symmetric programming and reasoning: eliminating symmetric cases with group actions

OHAD KAMMAR, University of Edinburgh, United Kingdom
MATIJA PRETNAR, University of Ljubljana & Institute of Mathematics, Physics and Mechanics, Slovenia

We develop a mathematical abstraction for uniformly exploiting symmetries in programming and reasoning based on the mathematical proof principle 'without-loss-of-generality' (w.l.o.g.). Given: group actions that describe symmetries of the input and the output; and a canoniser, which captures how arbitrary inputs get sent to canonical ones, our construction extends any function from the canonical inputs to the whole domain.

We characterise the conditions on the canonisers which guarantee that the construction gives the unique equivariant (i.e. symmetry-preserving) extension. Furthermore, we adapt the construction to a dependently-typed setting, where it captures traditional symmetric w.l.o.g. arguments via the Curry-Howard correspondence. Finally, we extend the construction to algebraic data types, where the symmetries of the constructors both uniquely determine the symmetries of the data type and pave the way for efficient execution.

CCS Concepts: • **Software and its engineering** → *Language features*; • **Theory of computation** → **Automated reasoning**; *Type theory*; *Type structures*; **Program constructs**; **Program reasoning**.

Additional Key Words and Phrases: groups, group actions, equivariance, invariance, symmetry, without loss of generality, algebra, wlog, stabilisers, coset space, semi-regular group actions, algebraic data types, indexed data types, initial algebra semantics, induction principles, nested folds, catamorphisms, binary search trees, correctness-by-construction, symmetrisation, Curry-Howard correspondence, dependent types

ACM Reference Format:
Ohad Kammar and Matija Pretnar. 2027. Mathematical foundations for symmetric programming and reasoning: eliminating symmetric cases with group actions. *Proc. ACM Program. Lang.* 10, POPL, Article 216 (November 2027), 61 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

When faced with repetition, programmers naturally turn to boilerplate or parametrisation. In this paper, we focus on repetition that arises from *symmetry*. We develop mathematical foundations that explicitly and uniformly capture existing implicit patterns in programming and reasoning, and define a construction that removes redundant symmetric cases from functions and proofs.

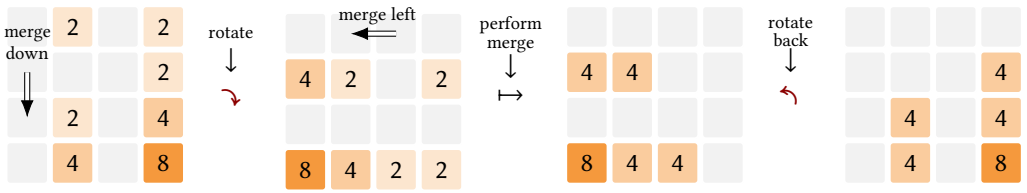
Consider Gabriele Cirulli's famous game of 2048[1], in which the player slides tiles labelled by powers of 2, merging tiles with identical labels. The player can slide tiles in all four directions, and the game source-code accommodates that ability through a general merging code that takes the direction as a parameter, builds a sequence of matrix indices to consider, and traverses over them[2].

Our anecdotal experience with half a dozen student projects suggests this parametrisation can be difficult to implement correctly. Here is an approach that is simpler to understand and to implement. Define the merging logic only for a single direction, say left, and exploit the inherent symmetry of the game for the other three directions: rotate the board so that the task is to slide left, perform the merge, and rotate back, restoring the original orientation. Here is an example downwards merge:

[1]Available to play: https://play2048.co
[2]See `GameManager.prototype.move`: https://github.com/gabrielecirulli/2048/blob/478b6ec/js/game_manager.js#L129.

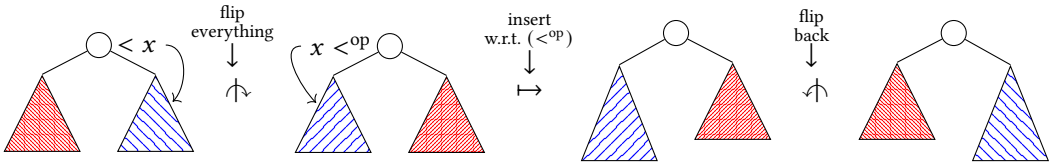
Authors' Contact Information: Ohad Kammar, ohad.kammar@ed.ac.uk, University of Edinburgh, Laboratory for the Foundations of Computer Science, School of Informatics, Edinburgh, Scotland, United Kingdom; Matija Pretnar, matija.pretnar@fmf.uni-lj.si, University of Ljubljana & Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia.

2027. ACM 2475-1421/2027/11-ART216
https://doi.org/XXXXXXX.XXXXXXX



Another common example of symmetry is that of binary search trees, in which elements smaller than the root go to the left subtree, while larger elements go to the right. Operations such as search, insertion, or deletion behave completely symmetrically. One way of avoiding repetition by parametrisation is to store both subtrees in an array of length two, and then use the offset $1 - i$ to refer to the tree opposite to the one at offset i. In practice, though, the additional complexity is often not worth losing the high-level abstraction, and programmers prefer to duplicate code.

But we can again avoid this repetition with the same approach and implement the code only for one case. For example, when inserting an element into the right subtree, we can flip the tree (and its ordering relation!), insert the element into the left subtree, and then flip the resulting tree back:



A reader may justifiably worry about the cost of flipping the whole tree each time we descend right, but a more efficient implementation fits the same pattern.

Our final example comes from mathematics, where one often invokes a *without loss of generality* (or w.l.o.g.) argument when we treat a canonical case, and derive the remaining cases by symmetry. Consider the pigeonhole principle given as an example in the Wikipedia entry for w.l.o.g. [97]:

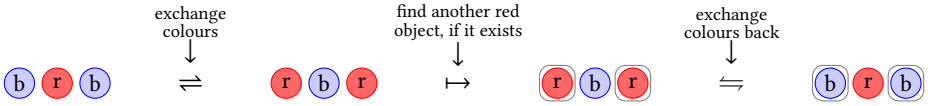
> If three objects are each painted either red or blue, then there must be at least two objects of the same color.
>
> **Proof.** Assume, without loss of generality, that the first object is red. If either of the other two objects is red, then we are finished; if not, then the other two objects must both be blue and we are also finished.

On paper, w.l.o.g. appeals to an intuitive understanding that nothing has been lost by considering a special case. But if the symmetry is complex or if we want to convince a proof assistant, we need to explicate the reduction of the general case to the special one.

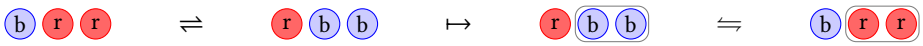
We can generalise the special case as a parametric proof that covers all cases. Above, we could take the colour of the first object as a parameter and then instantiate it to both red and blue. But as Harrison argues in his seminal study of w.l.o.g. in the context of the HOL proof assistant—and we agree—this formulation is not faithful to the informal proof [45].

Modern proof assistants offer special tactics to treat w.l.o.g. arguments, but approach them from various directions. Some tactics or theorems named `wlog` work in a very restricted setting, such as symmetric relations or negation, and some cut in arbitrary additional statements that do not involve symmetries. These divergent approaches point towards a missing mathematical foundation. Furthermore, none treat the underlying symmetry as a first-class citizen, and as Dijkstra argues—and we agree—"omissions [of the underlying symmetry] make most 'w.l.o.g. proofs' rather unsatisfactory" [27].

We can explicate this symmetry by following the same pattern we used for programming. In the excluded case where the first object is blue, we can exchange the colours to make it red, use the specialised argument, and then revert the colours back to the original. For example, one of the three cases where there is another blue object in addition to the first one proceeds as:



while if both remaining objects are red, we similarly proceed as:



In this paper, we develop this pattern into a uniform construction, and use it to eliminate symmetric cases in definitions of functions and in reasoning. On the surface, this pattern is conceptually simple, and so one may, just like us, be quickly tempted to implement it, either in a programming language or in a proof assistant. We experimented in simply- and dependently-typed languages, and unsurprisingly, each obstacle pushed us back to pen-and-paper redesigns and forced us to enrich the underlying mathematical foundation.

For this reason, while still keeping computational applications in mind, this work focuses on these mathematical foundations. We postpone a bona fide implementation to future work. Such future implementations will allow us to explore symmetric programming on more involved examples, in a machine-checked environment, design the best interface for exposing it to the programmer, to build a comprehensive library for symmetric programming and mechanised reasoning, and revisit existing w.l.o.g. formalisations systematically. While we keep these downstream goals in mind, we pursue none of them in the present work, and remain solely mathematical.

Our contributions:

- In §2, we identify three ingredients: *group actions* capturing the symmetries of the input and output, a *canoniser* map that assigns a canonising group element to each input, and a *core function* that defines the construction on canonical inputs. We then characterise our symmetric w.l.o.g. construction as the unique symmetry-preserving (i.e. equivariant) extension of the core function to all the inputs.
- In §3, we extend this theory to the setting of *dependent types*. We show how via the Curry-Howard correspondence, symmetry-invariant propositions correspond to types equipped with a group action. We show how proofs via the symmetric w.l.o.g. argument amount to dependent functions obtained by the above construction.
- In §4, we further extend the theory to (simply- and dependently-typed) *algebraic data types* and their induction principles. The main construct we introduce is *symmetry strength*, which defines a group action in terms of data constructors, paving the way for symmetric reasoning on data types, and efficient partial evaluation.

We conclude with related and future work in §5. The Appendix has further details and proofs.

Remark 1.1. Our development has been informed by category theoretic structure. To keep exposition accessible, we do not rely on the language of and concepts from category theory in the lion's share of this work. The notable exception is our account of symmetric data types (§4). There, generic accounts of the computational structure are close to their underlying categorical structure, and consequently we explicitly employ the categorical language. Readers who wish to reconstruct the category theoretic picture can consult Fig. 1 in §4.5 alongside the development.

2 Without loss of generality

Having observed the common pattern in the preceding examples, let us detail the ingredients:

(1) Capture the inherent symmetries of our problem using **group actions**.
(2) Obtain a **canonising** symmetry for each input.
(3) Give the **core function**, defined only on canonical elements.

The **symmetric w.l.o.g. construction** combines these ingredients, covering all inputs:

	canonise input using a symmetry		apply the core function		transform output back using the inverse symmetry	
a general input	↓ ↦	a canonical input	↓ ↦	an output for the canonical input	↓ ↦	the desired output for the general input

Our previous examples fit this pattern as:

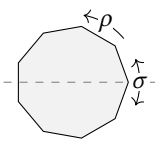
	2048 merge	**tree insertion**	**pigeonhole principle**
general input	board & direction	element & tree	arbitrary colouring
desired output	merged board	extended tree	general proof
symmetry	rotation	flipping	colour exchange
canonical input	direction is left	inserted key ≤ root key	first object is red
core function	merge left	insert left as needed	special-case proof

2.1 Groups and actions

Before turning to symmetric w.l.o.g. abstractions, let us start with a short group theory tutorial. A *concrete symmetry* on a set is a bijection from the set to itself. When we compare different sets, we need to relate their symmetries. A *group* gives these symmetries a name, and its *actions* allow us to use the same abstract symmetry to refer to concrete symmetries on different sets.

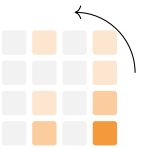
Groups. Recall that a *group* $G = \langle \underline{G}, e, (*), (-)^{-1} \rangle$ is a tuple consisting of: a *carrier* set $\underline{G}$, whose elements we call *symmetries*; a *neutral* element $e \in \underline{G}$; a *composition* $(*) : \underline{G} \to \underline{G} \to \underline{G}$; and an *inverse* map $(-)^{-1} : \underline{G} \to \underline{G}$; such that:

- composition is associative: $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for all $g_1, g_2, g_3 \in \underline{G}$;
- the neutral element is neutral w.r.t. composition: $e * g = g * e = g$ for all $g \in \underline{G}$; and
- the inverse map picks inverses: $g * g^{-1} = g^{-1} * g = e$ for all $g \in \underline{G}$.



Two famous examples of groups are the *symmetric group* $\mathbf{S}_n$ of all permutations of the set $\mathsf{Fin}\, n := \{0, \ldots, n-1\}$, and the *dihedral group* $\mathbf{D}_n$ of all symmetries of a regular n-gon, i.e. n rotations and n reflections. The dihedral group is *generated* by a $2\pi/n$ rotation ρ and a single reflection σ, meaning every other symmetry can be obtained by a suitable composition of ρ and σ.

In our examples, both the mirroring symmetry of trees and exchange of colours are described by the symmetric group $\mathbf{S}_2 = \{\mathtt{I}, \mathtt{F}\}$, where $\mathtt{I}$ is the identity permutation and $\mathtt{F}$ flips the two elements. The 2048 board is symmetric with respect to the dihedral group $\mathbf{D}_4$, though for our use, it is sufficient to consider the *cyclic group* $\mathbf{C}_4$, generated by the quarter-turn rotation marked here as ↰.



Actions. Groups capture symmetries abstractly. Symmetries between elements of a particular set are captured by *group actions*. Given a group G, recall that a G-*action* $A = \langle \underline{A}, (\circledast) \rangle$ consists of a *carrier* set $\underline{A}$; and a map $(\circledast) : \underline{G} \to \underline{A} \to \underline{A}$, writing $(\circledast^A)$ when ambiguous, such that:

- every element is symmetric to itself via the neutral symmetry: $e \circledast x = x$ for $x \in \underline{A}$; and
- symmetry is transitive via composition: $(g_1 * g_2) \circledast x = g_1 \circledast (g_2 \circledast x)$ for $g_1, g_2 \in \underline{G}$, $x \in \underline{A}$.

Example 2.1. The symmetric group $\mathbf{S}_n$ acts on the finite sets $\mathsf{Fin}\, n = \{0, 1, \ldots, n-1\}$ by $\pi \circledast i \coloneqq \pi i$, and on vectors $\mathsf{Vect}_n X \coloneqq X^n$ by $\pi \circledast \langle x_0, \ldots, x_{n-1}\rangle \coloneqq \left\langle x_{\pi^{-1}0}, \ldots, x_{\pi^{-1}(n-1)}\right\rangle$ sending the i-th element to the position πi. □

Example 2.2. We define the sets of valid $n \times n$ boards of 2048 by:

$$\mathsf{Tile} \coloneqq \{0\} \cup \left\{2^i \,\middle|\, i \in \mathbb{N}_+\right\} \qquad \mathsf{Row}_n = \mathsf{Vect}_n \mathsf{Tile} \qquad \mathsf{Board}_n = \mathsf{Vect}_n(\mathsf{Row}_n)$$

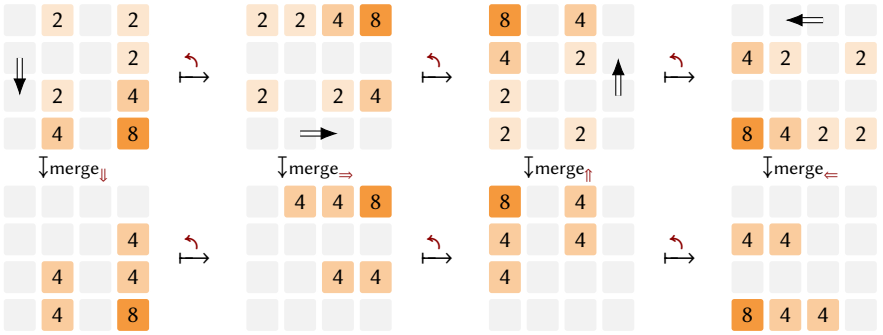
And the action $(\circledast) : \mathbf{C}_4 \to \mathsf{Board}_n \to \mathsf{Board}_n$ is given by rotating the board entries as:

$$\curvearrowleft \circledast \begin{pmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,n} \end{pmatrix} = \begin{pmatrix} x_{1,n} & \cdots & x_{n,n} \\ \vdots & \ddots & \vdots \\ x_{1,1} & \cdots & x_{n,1} \end{pmatrix}$$

Since $\curvearrowleft$ generates $\mathbf{C}_4$, any other rotation is of the form $\curvearrowleft^k$ for some k, and so the action of other rotations is uniquely determined by the group action laws to be $\curvearrowleft^k \circledast b = \curvearrowleft \circledast (\curvearrowleft^{k-1} \circledast b)$.

Note, however, that not all definitions on generators extend to the whole group, as they must also respect the equalities between group elements. For example, since $\curvearrowleft^4 = e$, we must also have that $\curvearrowleft^4 \circledast b = b$ for any board b, and the above definition respects that since rotating the entries four times gives us back the original matrix. □

Equivariance. The game 2048 exhibits symmetry not only by permitting rotations of the board, but also by the fact that merging respects it: if we rotate the board and then merge in the rotated direction, we get the same result as first merging and then rotating the resulting board:



Equivariance captures symmetry preservation. Given G-actions A and B, recall that an *equivariant* map $\varphi : A \circledast\!\!\to B$ is a map $\varphi : \underline{A} \to \underline{B}$ satisfying $\varphi(g \circledast^A a) = g \circledast^B \varphi a$ for all $g \in \underline{G}$ and $a \in \underline{A}$.

Example 2.3. Take any $f : X \to Y$. Its pointwise application $\mathbf{map}\, f : \mathsf{Vect}_n X \to \mathsf{Vect}_n Y$ is equivariant with respect to the permuting action of $\mathbf{S}_n$ on vectors since:

$$\begin{aligned} \mathbf{map}\, f(\pi \circledast \langle x_0, \ldots, x_{n-1}\rangle) &= \mathbf{map}\, f(\left\langle x_{\pi^{-1}0}, \ldots, x_{\pi^{-1}(n-1)}\right\rangle) = \left\langle f x_{\pi^{-1}0}, \ldots, f x_{\pi^{-1}(n-1)}\right\rangle \\ &= \pi \circledast \langle f x_0, \ldots, f x_{n-1}\rangle = \pi \circledast (\mathbf{map}\, f\, \langle x_0, \ldots, x_{n-1}\rangle) \end{aligned}$$ □

Before the next example, recall that a *product* $A \times B$ of G-actions A and B is given on $\underline{A \times B} \coloneqq \underline{A} \times \underline{B}$ component-wise by: $g \circledast^{A\times B} \langle a, b\rangle \coloneqq \left\langle g \circledast^A a, g \circledast^B b\right\rangle$. Furthermore, the *exponential action* $A \to B$ is given on the set of all functions, not only the equivariant ones, $\underline{A \to B} \coloneqq \underline{A} \to \underline{B}$ by *conjugation*: $(g \circledast^{A\to B} f) \coloneqq a \mapsto g \circledast^B f(g^{-1} \circledast^A a)$. Finally, the *trivial* action $\mathrm{Triv}X$ on a set X is defined by $\underline{\mathrm{Triv}X} \coloneqq X$ and $g \circledast x \coloneqq x$. An *invariant* map is an equivariant map $f : A \circledast\!\!\to \mathrm{Triv}X$.

Example 2.4. We can equip the set Tree of binary trees with values in $\mathbb{N}$ (fixed for simplicity) with the recursive S_2-action $\mathsf{F} \circledast^{\mathsf{Tree}} \mathsf{Leaf} = \mathsf{Leaf}$ and $\mathsf{F} \circledast^{\mathsf{Tree}} \mathsf{Node}(\ell, n, r) = \mathsf{Node}(\mathsf{F} \circledast r, n, \mathsf{F} \circledast \ell)$. Furthermore, let Path be the set of lists over step directions $\mathbf{Step} = \{\mathsf{L}, \mathsf{R}\}$. We can equip Path with an S_2-action by mapping the S_2-action $\mathsf{F} \circledast \mathsf{L} = \mathsf{R}$ and $\mathsf{F} \circledast \mathsf{R} = \mathsf{L}$.

Take lookup : Tree $\to$ Path $\to$ Maybe $\mathbb{N}$, which takes a path through a tree (a list of steps left or right) and returns the resulting value, if it exists. This function is invariant under symmetry: if we flip both the tree and the direction of all the steps, we should get back the same value. More precisely, lookup is equivariant in its curried form Tree $\circledast\!\!\to$ (Path $\to$ Triv(Maybe $\mathbb{N}$)) with respect to the exponential action, while the uncurried form Tree $\times$ Path $\circledast\!\!\to$ Triv(Maybe $\mathbb{N}$) is invariant. □

2.2 The w.l.o.g. construction

Canonisers. The first step in our construction is to map each input to a *canonical* representative. Crucially, we canonise via an explicit symmetry in the group, rather than through an arbitrary function, as we need to apply the inverse symmetry to reconstruct the output for the original input.

For example, we canonise search trees by flipping the tree when the inserted key is strictly larger than the root key. Thus, the remaining canonical inputs are those that: insert into an empty tree, insert the redundant key equal to the one in the root; and insert to the left subtree. For the pigeonhole principle example, the canonising symmetry is the identity if the first object is red, and F that exchanges the colours if the first object is blue. Thus, the canonical elements are triples in which the first object is red.

Definition 2.5. Let A be a G-action. A *canoniser* for A is a function $c : \underline{A} \to \underline{G}$. For each $a \in \underline{A}$, we call the symmetry $ca \in \underline{G}$ the *c-canonising symmetry* of a, and the element $ca \circledast a \in \underline{A}$ the *canonical form* of a. We define the set of *canonical* elements to be $\mathsf{Can}_A\, c \coloneqq \{\, ca \circledast a \mid a \in \underline{A} \,\}$.

Canonisers need not respect the structure of the action on A, as many of the interesting examples indeed do not. However, there are still some examples that respect it, and we study them and their impact on the equivariance of the w.l.o.g. construction in §2.3.

Example 2.6. Let P be a *strict partial order*, i.e., a set equipped with an irreflexive and transitive relation $<_P$. We say that an n-tuple $\vec{p} \in \mathsf{Vect}_n P$ is *sorted* when $p_i < p_j$ implies $i < j$ for all indices $i, j \in \mathsf{Fin}\, n$. Then, a *sorting function* is a function sort : $\mathsf{Vect}_n P \to \underline{\mathsf{S}_n}$ that maps a tuple to a permutation that sorts it. Every such function is a canoniser for the permuting action of S_n on $\mathsf{Vect}_n P$ from Example 2.1.

Given an n-tuple $\vec{p}$, the sorted tuple $(\mathsf{sort}\, \vec{p}) \circledast \vec{p}$ is the canonical form of $\vec{p}$, and every $p \in \mathsf{Can}\ \mathsf{sort}$ is sorted. If the sorting function returns the identity permutation for sorted tuples—for example when the sorting is stable—the set $\mathsf{Can}\ \mathsf{sort}$ is exactly the set of sorted tuples. □

Example 2.7. Continuing Example 2.2, the input for the 2048's merge is the board together with the merge direction. Define $\mathsf{Dir} \coloneqq \{\Rightarrow, \Uparrow, \Leftarrow, \Downarrow\}$ and its action $(\circledast) : \mathsf{C}_4 \to \mathsf{Dir} \to \mathsf{Dir}$ by:

$$\curvearrowleft \circledast \Rightarrow \coloneqq \Uparrow \qquad \curvearrowleft \circledast \Uparrow \coloneqq \Leftarrow \qquad \curvearrowleft \circledast \Leftarrow \coloneqq \Downarrow \qquad \curvearrowleft \circledast \Downarrow \coloneqq \Rightarrow$$

Define $\mathsf{mkLft} : \mathsf{Dir} \to \underline{\mathsf{C}_4}$ to pick the unique rotation turning its input left, i.e. $(\mathsf{mkLft}\, d) \circledast d = \Leftarrow$:

$$\mathsf{mkLft} \Rightarrow \coloneqq \curvearrowleft^2 = \curvearrowright \qquad \mathsf{mkLft} \Uparrow \coloneqq \curvearrowleft \qquad \mathsf{mkLft} \Leftarrow \coloneqq e = \circlearrowleft \qquad \mathsf{mkLft} \Downarrow \coloneqq \curvearrowleft^{-1} = \curvearrowright$$

Thus the only canonical direction is left $\mathsf{Can}\ \mathsf{mkLft} = \{\Leftarrow\}$. We can extend the canoniser to input pairs $\mathsf{Dir} \times \mathsf{Board}_n$ by $\mathsf{mkLft} \circ \pi_1$. □

We frequently encounter similar canonisers that depend only on a part of the input.

Lemma 2.8. *Let A and B be G-actions. Every A-canoniser $c : \underline{A} \to \underline{G}$ induces an $(A \times B)$-canoniser $c \circ \pi_1 : \underline{A \times B} \to \underline{G}$. We then have* $\mathsf{Can}\ (c \circ \pi_1) = \mathsf{Can}\ c \times \underline{B}$.

Core functions. Given G-actions A and B, we want to define a function $A \to B$ while avoiding symmetric cases. Once we have an A-canoniser c and its set of canonical elements $\mathsf{Can}\, c$ in place, the only thing missing is the *core function* $f : \mathsf{Can}\, c \to \underline{B}$: merging of tiles in 2048, insertion into a subtree, or the special case in the pigeonhole principle. Typical symmetric w.l.o.g. arguments only explicate canonical elements and core functions, but gloss over groups, actions, and canonisers.

Example 2.9. Continuing Example 2.7, let us define the core function merging the tiles in 2048. We choose left merges as the canonical direction since vertical merges go against the structure of vectors of rows, while rightward merges have edge cases coalescing empty tiles. First, we define $\mathsf{merge}_{\Leftarrow}^{\mathsf{Row}} : \mathsf{Row}_n \to \mathsf{Row}_n$ using pattern matching as all the relevant tiles are on the left:

$$\mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_0}\,\langle\rangle \coloneqq \langle\rangle \qquad \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_1}(x :: \langle\rangle) \coloneqq \langle x\rangle \qquad \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_{1+n}}(0 :: r) \coloneqq \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_n}(r) +\!\!+ \langle 0\rangle$$

$$\mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_{2+n}}(x :: y :: r) \coloneqq \begin{cases} 2x :: \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_n}(r) +\!\!+ \langle 0\rangle & (x = y) \\ \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_{1+n}}(x :: r) +\!\!+ \langle 0\rangle & (y = 0) \\ x :: \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_{1+n}}(y :: r) & (x \neq y \neq 0) \end{cases}$$

We merge the whole board simply by merging each row:

$$\mathsf{merge}_{\Leftarrow} : \mathsf{Board}_n \to \mathsf{Board}_n \qquad \mathsf{merge}_{\Leftarrow} \coloneqq \mathbf{map}\, \mathsf{merge}_{\Leftarrow}^{\mathsf{Row}_n} \qquad \square$$

The construction. We now formally define the w.l.o.g. construction we sketched a number of times, extending a core function $f : \mathsf{Can}\, c \to \underline{B}$ to the whole carrier $\underline{A}$. Take any $a \in \underline{A}$ and compute its canonical form $ca \circledast a$. By definition, the canonical form lies in $\mathsf{Can}\, c$, so we can apply the core function to obtain $f(ca \circledast a)$. Even though this result has the expected type B, we still need to apply the inverse symmetry $(ca)^{-1}$. Indeed, making a downward merge in 2048 would result in a rotation, followed by a leftward merge, followed by the inverse rotation.

Definition 2.10. Let A and B be G-actions, $c : \underline{A} \to \underline{G}$ a canoniser, and $f : \mathsf{Can}\, c \to \underline{B}$ a core function. Then, the *w.l.o.g. construction* $\mathsf{wlog}(c, f) : \underline{A} \to \underline{B}$ is defined as

$$\mathsf{wlog}(c, f) \coloneqq a \mapsto (ca)^{-1} \circledast^B f(ca \circledast^A a)$$

Using Example 2.9, we define $\mathsf{merge} : \mathsf{Dir} \times \mathsf{Board}_n \to \mathsf{Board}_n$ as $\mathsf{wlog}(\mathsf{mkLft} \circ \pi_1, \mathsf{merge}_{\Leftarrow} \circ \pi_2)$.

2.3 Equivariance of the w.l.o.g. construction

In addition to extending the core function $f : \mathsf{Can}\, c \to \underline{B}$ to the whole domain, we often want the extension $\varphi : \underline{A} \to \underline{B}$ to be equivariant. This requirement implies that the core function f must already behave equivariantly where defined. To see this, consider a canonical element $x \in \mathsf{Can}\, c$ that also has a symmetric canonical element $g \circledast x \in \mathsf{Can}\, c$. Then:

$$\begin{array}{ccccc} & \varphi \text{ extends } f & & \varphi \text{ is equivariant} & & \varphi \text{ extends } f & \\ & \downarrow & & \downarrow & & \downarrow & \\ f(g \circledast x) & = & \varphi(g \circledast x) & = & g \circledast \varphi(x) & = & g \circledast fx \end{array}$$

We generalise the notion of equivariance to domains that may not be closed under the action:

Definition 2.11. Take G-actions A, B, a subset $X \subseteq \underline{A}$, and a function $f : X \to \underline{B}$. We call f *equivariant*, writing $f : (X \subseteq A) \circledast\!\!\to B$, when $g \circledast x \in X \implies f(g \circledast x) = g \circledast fx$ for $g \in \underline{G}$, $x \in X$.

Example 2.12. Every core function for the 2048 canoniser from Example 2.7 is vacuously equivariant: only $\Leftarrow$ is canonical, and any $g \in \mathbf{C}_4 \setminus \{e\}$ changes the direction to a non-canonical input. Therefore, if $x, g \circledast x$ are canonical, then $g = e$ and $g \circledast f\, x = f\, x = f(g \circledast x)$.

Insertion into binary search trees features non-trivial corner cases of core function equivariance. Flipping the empty tree yields back the empty tree, which is again a canonical element. Thus

inserting a key into a "flipped" empty tree needs to be the same as first inserting the key into the empty tree and then flipping the result. However, the resulting tree is a single root with two empty subtrees, which is invariant under flipping, thus the core function is equivariant. A similar case occurs when inserting a key that is equal to the root value. □

Equivariance of core functions is easily overlooked when canonical elements are treated in isolation, especially since the overlap usually occurs on trivial cases. On a more positive note, the condition is not only necessary, but also sufficient for the existence of an equivariant extension. Furthermore, w.l.o.g. gives the unique such extension:

Theorem 2.13. *Let A and B be G-actions and $c : \underline{A} \to \underline{G}$ a canoniser. If $f : (\mathsf{Can}\ c \subseteq A) \circledast\!\!\longrightarrow B$ is an equivariant core function, then $\mathsf{wlog}(c, f) : A \circledast\!\!\longrightarrow B$ is the unique equivariant function extending f to the whole $\underline{A}$, along the inclusion $\mathsf{Can}\ c \subseteq \underline{A}$.*

Example 2.14. Recall the 2048 function $\mathsf{merge} = \mathsf{wlog}(\mathsf{mkLft}, \mathsf{merge}_{\Leftarrow}) : \mathsf{Dir} \times \mathsf{Board}_n \to \mathsf{Board}_n$. It indeed behaves as expected: for leftward merges, it extends $\mathsf{merge}_{\Leftarrow}$, while for other directions, it is uniquely determined by the equivariant behaviour. □

In concrete cases, equivariance of core functions is often easily discharged, but we can further relax it when the canoniser c has additional properties. A natural property is the equivariance of the canoniser. Since $\left(ca * g^{-1}\right) \circledast (g \circledast a) = ca \circledast a$ is canonical, it is natural to ask whether $ca * g^{-1}$ is the c-canonising symmetry of $g \circledast a$, i.e. whether $c(g \circledast a) = ca * g^{-1}$. More succinctly, this property means c is an equivariant map $c : A \circledast\!\!\longrightarrow G^{-1}$ where G^{-1} is the action of G on itself, defined by $g \circledast^{G^{-1}} h \coloneqq h * g^{-1}$. It validates the axioms since:

$$e \circledast^{G^{-1}} s = s * e^{-1} = s \qquad g \circledast^{G^{-1}} (h \circledast^{G^{-1}} s) = (s * h^{-1}) * g^{-1} = s * (g * h)^{-1} = (g * h) \circledast^{G^{-1}} s$$

Definition 2.15. A canoniser $c : \underline{A} \to \underline{G}$ is *strictly equivariant* when $c\ (g \circledast a) = ca * g^{-1}$, i.e. when it is an equivariant map $c : A \circledast\!\!\longrightarrow G^{-1}$.

As we shall soon see, strict equivariance is a powerful assumption, but also a very strong restriction, thus we reserve the name *equivariant canonisers* for a weaker and more natural notion that we introduce in §3.4, after we discuss dependent types.

Example 2.16. The canoniser mkLft from Example 2.7 is strictly equivariant since $\mathsf{mkLft}\ d$ is the unique rotation that makes d canonical. On the other hand, if in Example 2.6, we take a non-total ordering P and a stable sorting algorithm, the canoniser $\mathsf{sort} : \mathsf{Vect}_n P \to \underline{\mathbf{S}_n}$ is not strictly equivariant since for every two incomparable elements p, q, we have:

$$\mathsf{sort}\left((0 \leftrightarrow 1) \circledast \langle p, q\rangle\right) = \mathsf{sort}\,\langle q, p\rangle = \mathrm{id} \neq (0 \leftrightarrow 1) = \mathrm{id} * (0 \leftrightarrow 1)^{-1} = (0 \leftrightarrow 1) \circledast \mathsf{sort}\,\langle p, q\rangle \qquad \square$$

Strict equivariance guarantees equivariance of arbitrary core functions, and thus also of the w.l.o.g. construction. The converse also holds, though we do not need it for our applications.

Theorem 2.17. *Let $c : \underline{A} \to \underline{G}$ be a canoniser. Then, c is strictly equivariant iff for every action B, every core function $f : \mathsf{Can}\ c \to \underline{B}$ is equivariant.*

Strict equivariance is too strong, as it restricts the action to be *semi-regular*, meaning that only the identity can fix an element: $g \circledast a = a \implies g = e$.

Lemma 2.18 (semi-regularity)**.** *If A has a strictly equivariant canoniser, then A is semi-regular.*

For example, the $\mathbf{C}_4$ action on Board_n is not semi-regular, since all rotations preserve the empty 2048 board. It is only the addition of the direction, which all non-trivial symmetries affect, that makes the action on $\mathsf{Dir} \times \mathsf{Board}_n$ semi-regular.

Strictly equivariant canonisers satisfy $c(ca \circledast a) = ca * (ca)^{-1} = e$, meaning that canonisation is a one-step process and that further canonisation symmetries are identities. This observation leads us to a weaker natural property of canonisers, and one that all examples in this paper enjoy:

Definition 2.19. A canoniser c is *immediate* when for all $a \in \underline{A}$, we have $c(ca \circledast a) = e$.

Proposition 2.20. *A strictly equivariant canoniser $c : A \circledast\!\!\longrightarrow G^{-1}$ is immediate.*

The converse does not hold: as we saw in Example 2.16, a stable sorting function is not a strictly equivariant canoniser, but it is immediate since the canonical elements are exactly the sorted tuples, and the sorting permutation for sorted tuples is the identity.

We will often derive a canoniser for $A \times B$ from a canoniser for A through projection. For example, we derive the canoniser for $\mathsf{Dir} \times \mathsf{Board}_n$ from that of Dir.

Lemma 2.21. *For G-actions A, B, if $\underline{A} \xrightarrow{c} \underline{G}$ is strictly equivariant/immediate, then so is $\underline{A} \times \underline{B} \xrightarrow{c \circ \pi_1} \underline{G}$.*

To apply the w.l.o.g. construction, we need to provide both the canoniser c and the core function f. If we have $ca = e$ for some $a \in \underline{A}$, then $a = ca \circledast a \in \mathsf{Can}\, c$, and so we need to define the value fa. In the ideal case, we want to consider each element of $\underline{A}$ only once and define the core function only on elements with trivial canonising symmetries. More precisely, we want the sets $\{a \in \underline{A} \mid ca \neq e\}$ and $\mathsf{Can}\, c$ to be disjoint. But in general, the two sets may overlap. In the extreme case, if $c : \mathsf{Dir} \to \underline{\mathbf{C}_4}$ is the constant function $_ \mapsto \curvearrowleft$, they are both equal to the whole domain Dir. However, immediate canonisers are exactly those for which the domain $\underline{A}$ cleanly splits into two:

Proposition 2.22. *A canoniser $c : \underline{A} \to \underline{G}$ is immediate iff* $\mathsf{Can}\, c = c^{-1}[e] \coloneqq \{a \in \underline{A} \mid ca = e\}$.

3 Symmetric dependent types

To precisely show how our construction captures traditional w.l.o.g. arguments, we need to move to a more expressive setting. For that, we use dependent types, which also allow us to impose richer invariants on programming examples such as binary search trees.

We start by recalling the framework of *families* (§3.1), which gives a mathematical interpretation of familiar dependent-type notions. Afterwards, we generalise our constructs and results to a dependent setting (§3.2) and show how via the Curry-Howard correspondence, they capture proofs that use w.l.o.g. arguments (§3.3). Finally, we use the additional power of dependent types to define a more refined notion of canoniser equivariance (§3.4).

3.1 Families

A *family* $\Gamma \vdash X$ is a pair consisting of a set Γ and an assignment of a set $X\gamma$ to each element $\gamma \in \Gamma$. We call Γ the *indexing* set, its elements $\gamma \in \Gamma$ *indices*, and each set $X\gamma$ the *fibre* over the index γ. A *term* $\Gamma \vdash t : X$ in a family $\Gamma \vdash X$ is an assignment of an element $t\gamma \in X\gamma$ to each $\gamma \in \Gamma$. A family $\Gamma \vdash X$ is a *subfamily* of $\Gamma \vdash Y$, which we write as $\Gamma \vdash X \subseteq Y$ if $X\gamma \subseteq Y\gamma$ for all $\gamma \in \Gamma$.

Example 3.1. To eliminate the necessity for the Maybe type in the tree lookup from Example 2.4, let us define the family $\mathsf{Tree} \vdash \mathsf{InPath}$ of *node paths* that contains all paths ending at an internal node of the index tree. More precisely, the fibre $\mathsf{InPath}\, t$ is empty if t is empty, and is otherwise the set of lists over $\mathbf{Step} = \{\mathsf{L}, \mathsf{R}\}$ which are either Nil, representing the root of the index tree, or $d :: p$ that start with a step direction d followed by a path p in that subtree. This set can be given inductively as:

$$\frac{}{\mathsf{Nil} \in \mathsf{InPath}\left(\ell \,\diagup^{x}\diagdown\, r\right)} \qquad \frac{p \in \mathsf{InPath}\,\ell}{(\mathsf{L} :: p) \in \mathsf{InPath}\left(\ell \,\diagup^{x}\diagdown\, r\right)} \qquad \frac{p \in \mathsf{InPath}\,r}{(\mathsf{R} :: p) \in \mathsf{InPath}\left(\ell \,\diagup^{x}\diagdown\, r\right)}$$

□

When specifying fibres or terms as assignments of the form $\gamma \mapsto X$ or $\gamma \mapsto t$, which explicitly use a generic index $\gamma \in \Gamma$, we write them as $\gamma : \Gamma \vdash X$ and $\gamma : \Gamma \vdash t : X$. We will continue to distinguish these uses, denoting generic indices for the purpose of defining a family by $\gamma : \Gamma$, and use $\gamma \in \Gamma$ when we refer to elements of an indexing set Γ for any other purpose. Note that despite using a convenient type-theoretic notation, we continue to keep our development purely mathematical, constructing objects without any recourse to a syntactic type system. Were we to present such a syntactic type system and differentiate between syntactic contexts Γ and their interpretations as indexing sets $[\![\Gamma]\!]$, then we would distinguish between $\gamma : \Gamma$ and $\gamma \in [\![\Gamma]\!]$.

Continuing this approach, we allow fibres and terms to depend on a context of variables. For the empty context, we take the indexing set $\mathbb{1} \coloneqq \{\star\}$ and identify families $\mathbb{1} \vdash X$ with their only fibre $X\star$. Then, we write fibres over $\mathbb{1}$ simply as $\vdash X$, and similarly for terms.

For context extension, we employ the *Grothendieck construction*. Recall that for a family $\Gamma \vdash X$, it is defined as the set $\coprod_\Gamma X \coloneqq \coprod_{\gamma \in \Gamma} X\gamma$, consisting of pairs $\langle \gamma, x \rangle$ where $\gamma \in \Gamma$ and $x \in X\gamma$, together with a projection function $\pi_1 \coloneqq (\langle \gamma, x \rangle \mapsto \gamma) : \coprod_\Gamma X \to \Gamma$. We write $\Gamma, x : X \vdash Y$ and $\Gamma, x : X \vdash t : Y$ for fibres and terms indexed by $\coprod_\Gamma X$ and use x to refer to the second component of the index pair from $\coprod_\Gamma X$ in Y and t.

Given two families $\Gamma \vdash X$ and $\Gamma, x : X \vdash Y$, we have the family of *dependent pairs* $\Gamma \vdash (x : X) \times Y$ whose fibre at $\gamma \in \Gamma$ is the Grothendieck construction $\coprod_{x \in X\gamma} Y\,\langle \gamma, x \rangle$, and the family of *dependent functions* $\Gamma \vdash (x : X) \to Y$ whose fibre at γ is the product $\prod_{x \in X\gamma} Y\,\langle \gamma, x \rangle$. As usual, we write $X \to Y$ when the codomain family Y does not depend on the argument of the function. To distinguish between indices and arguments of dependent functions $\Gamma \vdash f : (x : X) \to Y$, we apply them as $f_\gamma x$ for $\gamma \in \Gamma$ and $x \in X\gamma$, or even as $f\,x$ when γ can be inferred.

Example 3.2. With dependent types, we can refine the lookup function $\mathsf{Tree} \to \mathsf{Path} \to \mathsf{Maybe}\,\mathbb{N}$ from Example 2.4 to a dependent function $\vdash \mathsf{lookup} : (t : \mathsf{Tree}) \to \mathsf{InPath}\,t \to \mathbb{N}$, as the path now must point to a node in the tree. We can define it as:

$$\mathsf{lookup}\Big(\ {}_{\ell}\diagup{}^{n}\diagdown_{r}\ \Big)\,\mathsf{Nil} \coloneqq n \qquad \mathsf{lookup}\Big(\ {}_{t_\mathsf{L}}\diagup{}^{n}\diagdown_{t_\mathsf{R}}\ \Big)(d :: p) \coloneqq \mathsf{lookup}\,t_d\,p$$

Note that since we have two trees $t_\mathsf{L}, t_\mathsf{R}$ rather than a function $\mathbf{Step} \to \mathsf{Tree}$, the parametrisation t_d that we use in the second case is just repetition in disguise. Later, we will show how to properly avoid this repetition by using the w.l.o.g. construction. □

3.2 Indexed actions

Just as in Example 2.4, the function lookup from Example 3.2 is invariant with respect to flipping: flipping both the tree and the path returns the same value. But note that once we flip the tree t, the flipped path no longer lies in $\mathsf{InPath}\,t$, but in $\mathsf{InPath}\,(\mathsf{F} \circledast t)$. For example:

$$\mathsf{F} \circledast \left(\mathsf{L} :: \mathsf{R} :: \mathsf{Nil} \in \mathsf{InPath}\left(\ {}_{1}\diagup{}^{2}\diagdown{}^{3}_{4}\ \right)\right) = \mathsf{R} :: \mathsf{L} :: \mathsf{Nil} \in \mathsf{InPath}\left(\ {}^{3}\diagdown{}^{2}_{4}\diagdown{}_{1}\ \right)$$

In general, an action over a family $\Gamma \vdash A$ should thus consist of an action over the index set Γ, and an action over each fibre $A\gamma$, which tracks the indexing action: if $a \in A\gamma$, then $g \circledast a \in A(g \circledast \gamma)$.

Definition 3.3. Given a G-action Γ, an *indexed G-action* $\Gamma \vdash A$ consists of a *carrier* family $\underline{\Gamma} \vdash \underline{A}$ and a dependent function $(\circledast_) : (g : \underline{G}) \to (\gamma : \underline{\Gamma}) \to \underline{A}\gamma \to \underline{A}(g \circledast^{\Gamma} \gamma)$, which we apply as $g \circledast_\gamma a$, such that $e \circledast_\gamma a = a$ and $(g * h) \circledast_\gamma a = g \circledast_{h \circledast \gamma} (h \circledast_\gamma a)$.

When A is ambiguous, we add a superscript and write $\circledast^A_\gamma$, and when we can infer the index γ, we elide it and write $g \circledast a$ instead of $g \circledast_\gamma a$.

Example 3.4. The action of the cyclic group $\mathbf{C}_4$ on 2048 boards can be generalised to an indexed action on the family of arbitrary matrices $\mathbb{N} \times \mathbb{N} \vdash \mathsf{Mat}$. First, take Γ to be the action of $\mathbf{C}_4$ on dimensions $\underline{\Gamma} \coloneqq \mathbb{N} \times \mathbb{N}$, defined as: $\curvearrowleft \circledast \langle m, n\rangle \coloneqq \langle n, m\rangle$. We then have a Γ-indexed action defined as in Example 2.2:

$$\curvearrowleft \circledast_{\langle m,n\rangle} \left(\begin{pmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{m,n} \end{pmatrix} \in \mathsf{Mat}_{m\times n} \right) = \begin{pmatrix} x_{1,n} & \cdots & x_{m,n} \\ \vdots & \ddots & \vdots \\ x_{1,1} & \cdots & x_{m,1} \end{pmatrix} \in \mathsf{Mat}_{n\times m} \qquad \square$$

Example 3.5. Take indexed G-actions $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$. Then, we can define the *dependent pair* action $\Gamma \vdash (x : A) \times B$ as:

$$\underline{\Gamma \vdash (x : A) \times B} \coloneqq \underline{\Gamma} \vdash \left(x : \underline{A}\right) \times \underline{B} \qquad g \circledast_\gamma^{(x:A)\times B} \langle a, b\rangle \coloneqq \left\langle g \circledast_\gamma^A a, g \circledast_{\langle \gamma, a\rangle}^B b \right\rangle$$

Furthermore, we can define the *dependent function* action $\Gamma \vdash (x : A) \to B$ as:

$$\underline{\Gamma \vdash (x : A) \to B} \coloneqq \underline{\Gamma} \vdash \left(x : \underline{A}\right) \to \underline{B}$$

$$g \circledast_\gamma^{(x:A)\to B} f \coloneqq (a : \underline{A}(g \circledast \gamma)) \mapsto g \circledast^B_{\langle \gamma, g^{-1}\circledast a\rangle} f_\gamma(g^{-1} \circledast^A_{g\circledast\gamma} a)$$

It is straightforward to check that both definitions satisfy the indexed action laws. $\square$

Definition 3.6. Given a G-action Γ and an indexed G-action $\Gamma \vdash A$, a term $\underline{\Gamma} \vdash t : \underline{A}$ is *equivariant* when its components are: $t(g \circledast^\Gamma \gamma) = g \circledast_\gamma t\gamma$ for all $\gamma \in \underline{\Gamma}, g \in \underline{G}$.

Equivariance of terms is preserved by reindexing and substitution. Furthermore, an equivariant term $\Gamma, x : A \vdash t : B$ induces an equivariant dependent function $\Gamma \vdash (x : A \mapsto t) : (x : A) \to B$, and two equivariant terms $\Gamma \vdash t : A$ and $\gamma : \Gamma \vdash s : B\langle\gamma, t\gamma\rangle$ induce an equivariant term given by the dependent pair in each fibre $\Gamma \vdash \langle t, s\rangle : (x : A) \times B$. For more details and proofs, see Appendix C.

The ease of compositionality should come as no surprise given that the definition of an indexed action is in fact just a reformulation of the notion of a family internally to the topos of G-actions:

Proposition 3.7. *Let Γ be a G-action. Then, a Γ-indexed action A amounts to an action $\coprod_\Gamma A$ over the Grothendieck construction for which the projection is equivariant: $\underline{\coprod_\Gamma A} = \coprod_{\underline{\Gamma}} \underline{A}$ and $\pi_1 : \coprod_\Gamma A \circledast\!\!\longrightarrow \Gamma$.*

We have used this connection above to reformulate standard notions from dependent types to the symmetric setting, and continue to do so with canonisers, core functions, and the w.l.o.g. construction. Ignoring the additional indices, we recover the simply-typed notions from §2.

Definition 3.8. Let $\Gamma \vdash A$ be an indexed G-action. An *indexed canoniser* for A is a $\underline{\Gamma}$-indexed term $\underline{\Gamma} \vdash c : \underline{A} \to \underline{G}$. For each $a \in \underline{A}\gamma$, we call the symmetry $c_\gamma a \in \underline{G}$ the *c-canonising symmetry* of a, and the element $ca \circledast_\gamma a$ the *canonical form* of a. We define the family of *canonical* elements $\underline{\Gamma} \vdash \mathsf{Can}\, c$ with the fibres $(\mathsf{Can}\, c)\gamma \coloneqq \left\{ ca \circledast_{\gamma'} a \,\middle|\, \gamma' \in \Gamma, a \in \underline{A}\gamma', ca \circledast \gamma' = \gamma \right\}$ for each $\gamma \in \underline{\Gamma}$.

Example 3.9. To capture the symmetry of the lookup function from Example 3.2, we define a canoniser for the indexed $\mathbf{S}_2$-action on $t : \mathsf{Tree} \vdash \mathsf{InPath}\, t$:

$$c_{\mathsf{Node}\langle \ell,n,r\rangle} \mathsf{Nil} \coloneqq \mathsf{I} \qquad c_{\mathsf{Node}\langle \ell,n,r\rangle}(\mathsf{L} :: p) \coloneqq \mathsf{I} \qquad c_{\mathsf{Node}\langle \ell,n,r\rangle}(\mathsf{R} :: p) \coloneqq \mathsf{F}$$

The canonical elements in $\mathsf{InPath}\, t$ are Nil and $(\mathsf{L} :: p) \in \mathsf{InPath}(\mathsf{Node}\, \langle \ell, n, r\rangle)$ where $p \in \mathsf{InPath}\, \ell$ can be an arbitrary path, even one that moves right on any of its steps. $\square$

Definition 3.10. Take indexed G-actions $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$, a subfamily $\underline{\Gamma} \vdash X \subseteq \underline{A}$, and a function $\underline{\Gamma} \vdash f : (x : X) \to \underline{B}$. We write $\Gamma \vdash f : (x : X \subseteq A) \circledast\!\!\longrightarrow B$ and say that f is *equivariant* when $g \circledast_\gamma^A x \in X(g \circledast \gamma) \implies f_{g\circledast\gamma}(g \circledast_\gamma^A x) = g \circledast^B_{\langle\gamma,x\rangle} f_\gamma x$ for all $g \in \underline{G}$, $\gamma \in \underline{\Gamma}$, and $x \in X\gamma$.

We can now define the dependently-typed version of the w.l.o.g. construction:

Definition 3.11. Let $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$ be indexed G-actions, $\Gamma \vdash c : \underline{A} \to \underline{G}$ an indexed canoniser, and $\Gamma \vdash f : (x : \mathrm{Can}\, c) \to \underline{B}$ a dependent core function. Then, the *indexed w.l.o.g. construction* $\mathrm{wlog}(c, f) : (x : \underline{A}) \to \underline{B}$ is defined as:

$$\mathrm{wlog}(c,f)_\gamma \coloneqq (a : \underline{A}\gamma) \mapsto (c_\gamma a)^{-1} \circledast^B_{\langle c_\gamma a \circledast^\Gamma \gamma, c_\gamma a \circledast^A_\gamma a \rangle} f_{c_\gamma a \circledast^\Gamma \gamma}(c_\gamma a \circledast^A_\gamma a)$$

With all the indices precisely spelt out, the definition can look a bit intimidating, but if we elide them we get $\mathrm{wlog}(c, f) = a \mapsto (ca)^{-1} \circledast^B f(ca \circledast^A a)$ as in the simply-typed case. And just as before in Theorem 2.13, the w.l.o.g. construction gives the unique equivariant extension of a core function.

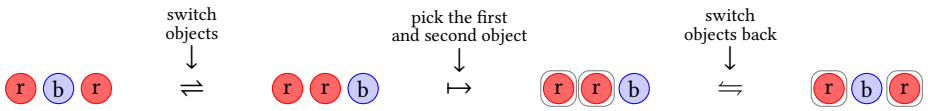
Theorem 3.12 (indexed representation)**.** *Let $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$ be indexed G-actions and $\Gamma \vdash c : \underline{A} \to \underline{G}$ an indexed canoniser for A. If $\Gamma \vdash f : (x : \mathrm{Can}\, c \subseteq A) \circledast\!\!\to B$ is an equivariant dependent core function, then $\mathrm{wlog}(c, f) : (x : A) \circledast\!\!\to B$ is the unique equivariant function extending f to the whole $\underline{\Gamma} \vdash \underline{A}$.*

Example 3.13. Let us revisit the pigeonhole principle [97] from the introduction and extend it in two ways. First, instead of a proof, let us construct a function $\mathrm{findSame} : (xyz : \{\mathsf{r}, \mathsf{b}\}^3) \to \mathrm{Same}\, xyz$ where $\mathrm{Same}\, xyz \coloneqq \{(i, j) : (\mathrm{Fin}\, 3)^2 \mid i \neq j \wedge \pi_i xyz = \pi_j xyz\}$ is the family of distinct positions of the same colour, indexed by the colouring xyz.

And second, we shall see that in the special case of the proof, there is another opportunity to use the w.l.o.g. argument. Informally, our proof goes as follows:

> W.l.o.g., the first object is red. The other two objects either have the same colour or different colours. If they have the same colour, choose $(1, 2)$. If they have different colours, w.l.o.g. the second object is red, so choose $(0, 1)$.

Such nested uses of w.l.o.g. may be suspicious and confusing, which is exactly why it is important to make all aspects of w.l.o.g. arguments explicit. In this case, this use is valid. For example, when the second object is not red and the third is red, the inner argument exchanges their positions:



In the outer level, S_2 acts on $\{\mathsf{r}, \mathsf{b}\}$ by flipping the two colours, and on the domain $\{\mathsf{r}, \mathsf{b}\}^3$ with the component-wise product action. On the codomain $\{\mathsf{r}, \mathsf{b}\}^3 \vdash \mathrm{Same}$, we lift the trivial action to preserve the elements of the fibre, but change the index. This is a sub-action (i.e. an action that preserves a subset) since if objects at two positions are of the same colour, they remain so after we exchange the colours. For example, $\mathsf{F} \circledast_{(\mathsf{r},\mathsf{r},\mathsf{b})} (0, 1) = (0, 1) \in \mathrm{Same}\, (\mathsf{b}, \mathsf{b}, \mathsf{r})$

By swapping colours, we make the first object red, thus the outer canoniser is:

$$\mathrm{makeFirstRed}(\mathsf{r}, b, c) \coloneqq \mathsf{I} \qquad \mathrm{makeFirstRed}(\mathsf{b}, b, c) \coloneqq \mathsf{F}$$

and using it, we can define

$$\mathrm{findSame} \coloneqq \mathrm{wlog}\left(\mathrm{makeFirstRed}, (\mathsf{r}, b, c) \mapsto \begin{cases} (1, 2) & (b = c) \\ \mathrm{findOtherRed}(b, c) & (b \neq c) \end{cases}\right)$$

where we still need to define

$$\mathrm{findOtherRed} : \left((y, z) : \left\{(b, c) \in \{\mathsf{r}, \mathsf{b}\}^2 \,\middle|\, b \neq c\right\}\right) \to \mathrm{Same}\, (\mathsf{r}, y, z)$$

Again, we employ symmetry, but now, the S_2-action on the domain swaps the two components of the pair, but not their colour, i.e., $\mathsf{F} \circledast (b, c) \coloneqq (c, b)$. For the codomain, define an action on $\mathrm{Fin}\, 3$

that swaps 1 and 2, and extend it component-wise to the product $(\mathsf{Fin}\,3)^2$. Since b and c are of different colours, it is easy to check that this action again preserves the defining property of Same and thus lifts to a sub-action on the codomain. For example, $\mathsf{F} \circledast_{(\mathsf{r},\mathsf{b})} (0,1) = (0,2) \in \mathsf{Same}\,(\mathsf{r},\mathsf{b},\mathsf{r})$.

The inner canoniser now makes the second object red:

$$\mathsf{makeSecondRed}(\mathsf{r},\mathsf{b}) \coloneqq \mathsf{I} \qquad \mathsf{makeSecondRed}(\mathsf{b},\mathsf{r}) \coloneqq \mathsf{F}$$

and so $\mathsf{findOtherRed} \coloneqq \mathsf{wlog}(\mathsf{makeSecondRed}, (\mathsf{r},\mathsf{b}) \mapsto (0,1))$. Equivariance is immediate since both core functions are vacuously equivariant. □

3.3 Propositional reasoning

So far we have used the w.l.o.g. construction to define functions. To formalise mathematical proofs, we apply the Curry-Howard correspondence and identify propositions with types, and their proofs with terms. We could have also approached this differently and e.g., transferred the w.l.o.g. construction to higher-order logic or first-order logic, but this would require us to duplicate the definitions for concepts such as group actions or equivariance for proofs.

For concreteness, let us first borrow a running example of Schur's inequality from Harrison [45], which states that for all $x, y, z, t \geq 0$, we have

$$x^t(x-y)(x-z) + y^t(y-z)(y-x) + z^t(z-x)(z-y) \geq 0$$

Since the inequality is symmetric in the three variables, the standard proof assumes that w.l.o.g., $x \leq y \leq z$ and rearranges the expression to an evidently non-negative form.

Let $\mathsf{Prop} \coloneqq \{\mathsf{True}, \mathsf{False}\}$ be the set of logical values. Each *proposition* $\Gamma \vdash \varphi : \mathsf{Prop}$ determines a family $\Gamma \vdash \mathsf{Proof}\,\varphi$ such that for each $\gamma \in \Gamma$, the fibre $(\mathsf{Proof}\,\varphi)\gamma = \mathbb{1} = \{\star\}$ when $\varphi\gamma = \mathsf{True}$ and $(\mathsf{Proof}\,\varphi)\gamma = \emptyset$ when $\varphi\gamma = \mathsf{False}$. As is conventional, we overload the notation and identify propositions with their proofs, writing $\Gamma \vdash \mathsf{Proof}\,\varphi$ simply as $\Gamma \vdash \varphi$. Then, any proof term $\Gamma \vdash p : \varphi$ is an explicit witness that φ holds at every $\gamma \in \Gamma$.

Example 3.14. Schur's inequality is the proposition $(x,y,z) : \mathbb{R}^3_+ \vdash \mathsf{Schur}(x,y,z) : \mathsf{Prop}$ where

$$\mathsf{Schur}(x,y,z) \coloneqq \forall t \geq 0.\ x^t(x-y)(x-z) + y^t(y-z)(y-x) + z^t(z-x)(z-y) \geq 0$$

Recall from Example 2.1 that $\mathbf{S}_3$ acts on $\mathbb{R}^3_+$ by permutation. The proposition Schur is invariant under those permutations. □

Definition 3.15. A proposition $\Gamma \vdash \varphi : \mathsf{Prop}$ is *invariant* when it is equivariant as a term with respect to the trivial G-action on Prop, i.e. $\varphi(g \circledast \gamma) = \varphi\gamma$ for all $\gamma \in \Gamma$.

In addition to equivariant substitutions, like all equivariant terms, invariant propositions are also preserved by logical connectives and quantifiers. Each invariant proposition $\Gamma \vdash \varphi : \mathsf{Prop}$ induces a Γ-indexed action on its proof family $\Gamma \vdash \varphi$. Moreover, given a Γ-indexed action A, each invariant proposition $\Gamma, x : A \vdash \varphi : \mathsf{Prop}$ induces a Γ-indexed action on the subfamily $\Gamma \vdash \{x : A \mid \varphi\} \subseteq A$. For more details and proofs, again see Appendix C.

Example 3.16. Coming back to Schur's inequality, we can see that the w.l.o.g. argument again fits the now familiar pattern:

$$x_0, x_1, x_2 \in \mathbb{R}_+ \quad \overset{\text{sort using a permutation } \pi^{-1}}{\mapsto} \quad x_{\pi 0} \leq x_{\pi 1} \leq x_{\pi 2} \quad \overset{\text{prove using additional assumption}}{\mapsto} \quad \mathsf{Schur}(x_{\pi 0}, x_{\pi 1}, x_{\pi 2}) \quad \overset{\mathsf{Schur}\text{ is invariant under permutations}}{\mapsto} \quad \mathsf{Schur}(x_0, x_1, x_2)$$

Let us use the w.l.o.g. construction to obtain a proof, i.e. a function $\left((x,y,z) : \mathbb{R}^3_+\right) \to \mathsf{Schur}(x,y,z)$. From Example 3.14 we already have an $\mathbf{S}_3$-action on $\mathbb{R}^3_+$, and since Schur is an invariant proposition, we also get an indexed $\mathbf{S}_3$-action on $\mathbb{R}^3_+ \vdash \mathsf{Schur}$. For the canoniser, we take a stable sorting function

$\mathsf{sort} : \mathbb{R}^3_+ \to \mathsf{S}_3$ from Example 2.6 so that Can sort is exactly the set of sorted triples. The last thing we need is the core function $f : \left\{(x,y,z) : \mathbb{R}^3_+ \,\middle|\, x \le y \le z\right\} \to \mathsf{Schur}(x,y,z)$, which we can define using the rearrangement in the standard proof. □

The resulting function $\mathsf{wlog}(\mathsf{sort}, f)$ is equivariant since in the case of propositions, core functions are always equivariant due to proof irrelevance:

Lemma 3.17. *Let* $\Gamma, x : A \vdash \varphi : \mathsf{Prop}$ *be an invariant proposition, and* $\Gamma \vdash c : \underline{A} \to \underline{G}$ *a canoniser. Every core function* $\Gamma \vdash f : \mathsf{Can}\ c \to \varphi$ *is equivariant.*

Harrison suggests proving Schur's inequality using the following tactic[3], which states that it is sufficient to prove permutation invariant propositions only for sorted triples [45, page 44]:

$$\frac{\forall x,y,z.\ P(x,y,z) \Rightarrow P(y,x,z) \wedge P(x,z,y) \qquad \forall x,y,z.\ (x \le y) \wedge (y \le z) \Rightarrow P(x,y,z)}{\forall x,y,z.\ P(x,y,z)}$$

Let us see how this bespoke tactic relates to our general w.l.o.g. construction. In contrast to our approach, the symmetry group S_3 is left implicit, as is the canoniser. Instead, only its set of canonical elements $\left\{(x,y,z) : \mathbb{R}^3_+ \,\middle|\, x \le y \le z\right\}$ is spelt out. Furthermore, the first assumption corresponds to an indexed S_3-action on the proposition P, and the second assumption is exactly the core function.

The latter is evident, while for the former, first recall from Example 2.2 that a group action is already uniquely determined by the action of any set of generators. The symmetry group S_3 is generated by the two transpositions $(0 \leftrightarrow 1)$ and $(1 \leftrightarrow 2)$, hence the action of S_3 is determined by maps $(0 \leftrightarrow 1) \circledast -$ and $(1 \leftrightarrow 2) \circledast -$. Spelling out the indices more precisely, these two maps are:

$$(0 \leftrightarrow 1) \circledast_{(x,y,z)} - : P(x,y,z) \to P((0 \leftrightarrow 1) \circledast (x,y,z)) \quad \text{equivalently} \quad P(x,y,z) \to P(y,x,z)$$
$$(1 \leftrightarrow 2) \circledast_{(x,y,z)} - : P(x,y,z) \to P((1 \leftrightarrow 2) \circledast (x,y,z)) \quad \text{equivalently} \quad P(x,y,z) \to P(x,z,y)$$

And this is exactly the contents of the first assumption.

As in Example 2.2, we must ensure that such a definition by generator cases respects all the equalities of the group. For example in any S_n-action, $(0 \leftrightarrow 1) \circledast -$ must be its own inverse (amongst other relations) since $(0 \leftrightarrow 1) * (0 \leftrightarrow 1) = e$. However, in the case of propositions, once again proof irrelevance implies this condition.

Exposing the symmetric structure in proofs also allows us to use existing results in group theory. Consider Harrison's proof in the tactic, which explicitly lists all six permutations [45]. For S_3, this number may still be manageable, but in general, the group S_n has $n!$ elements, so when n increases, the size of the proof script quickly becomes prohibitively large. Also, such an approach precludes a proof of a general wlog_n principle if n is a variable, as one cannot explicitly list all the $n!$ cases in the script. In contrast, we can lean on the general group-theoretic result, whose proof is independent of the concrete value of n, that S_n is generated, for example, by a single cycle $(0\,1\,2\,\cdots\,n-1)$ and a single transposition of adjacent elements such as $(0 \leftrightarrow 1)$. So it suffices to prove two cases to define any propositional S_n-action, yielding a single parametric principle wlog_n.

3.4 Equivariant canonisers

In §2.3, we saw that all w.l.o.g. constructions of a canoniser are equivariant iff the canoniser is strictly equivariant (Theorem 2.17). This result is significant because it allows us to do away completely with the equivariance of the core function, which involves comparing every pair of symmetric canonical elements. However, only the semi-regular actions can have such canonisers (Lemma 2.18). We now investigate a weaker notion of equivariance. It is also characterised through equivariant extension, but of *stable* core functions. A core function f is stable when every *stabilising* symmetry g

[3] Available here: https://github.com/jrh13/hol-light/blob/e5236a5/int.ml#L612.

of an element—$g \circledast a = a$—also stabilises the image $f\,a$. This necessary condition is natural and often easy to check. Furthermore, if we assume the axiom of choice, all actions admit equivariant canonisers, making them a viable—albeit theoretical—class of canonisers.

Both $c(g \circledast a)$ and $ca * g^{-1}$ canonise $g \circledast a$. Strictly equivariant canonisers equate these two symmetries: $c(g \circledast a) = ca * g^{-1}$. Equivariant canonisers merely relate them: $c(g \circledast a) \sim ca * g^{-1}$.

Definition 3.18. Take a G-action A. Then, for each $a \in \underline{A}$, we equip $\underline{G}$ with an *indistinguishability* relation $g \overset{a}{\sim} h \iff g \circledast a = h \circledast a$. Let $[g]_{\overset{a}{\sim}}$ be the equivalence class of g in $\underline{G}/\overset{a}{\sim}$. Define an indexed G-action $A \vdash G/A$ with the fibre $(G/A)\,a \coloneqq \underline{G}/\overset{a}{\sim}$ and with $\circledast^{G/A}$ defined as: $g \circledast_a^{G/A} [h]_{\overset{a}{\sim}} \coloneqq [h * g^{-1}]_{g \circledast a}$.

The action is well-defined since $h_1 \overset{a}{\sim} h_2$ implies $h_1 * g^{-1} \overset{g \circledast a}{\sim} h_2 * g^{-1}$. The relation $\overset{a}{\sim}$ is closely related to the *stabiliser* $G_a \coloneqq \left\{ g \in \underline{G} \,\middle|\, g \circledast a = a \right\} = [e]_{\overset{a}{\sim}}$, i.e. a subgroup of all symmetries that preserve a. In particular, $g \overset{a}{\sim} h$ is equivalent to $(h^{-1} * g) \circledast a = a$, i.e. $h^{-1} * g \in G_a$.

Remark 3.19. The equivalence classes of the indistinguishability relation are precisely the cosets of the stabiliser group. Therefore, we can recast the celebrated Orbit-Stabiliser theorem as an *equivariant* isomorphism between the actions on orbits and stabiliser cosets.

Given a G-action A, the fibres of the dependent family of *orbits* contain all the symmetric elements of an index, i.e. $a : \underline{A} \vdash G \circledast [a] \coloneqq \left\{ h \circledast a \,\middle|\, h \in \underline{G} \right\}$. On orbits, we can define an indexed action as:

$$g \circledast_a (h \circledast a \in G \circledast [a]) \coloneqq h \circledast a = (h * g^{-1}) \circledast (g \circledast a) \in G \circledast [g \circledast a]$$

Even though the action does not change the fibres, it is not trivial, since it changes the indices.

Theorem 3.20 (Orbit-Stabiliser)**.** *Let A be a G-action. We have an equivariant isomorphism:*

$$a : A \vdash \varphi_a : (G/A)a \overset{\cong}{\circledast\longrightarrow} G \circledast [a] \qquad \varphi_a [h]_{\overset{a}{\sim}} \coloneqq h \circledast a \qquad \varphi_a^{-1}(h \circledast a) \coloneqq [h]_{\overset{a}{\sim}}$$

The indexed action G/A generalises G^{-1} and allows us to consider a weaker property in which the equality $c\left(g \circledast^A a\right) = g \circledast^{G^{-1}} ca$ of strictly equivariant canonisers is replaced by indistinguishability:

Definition 3.21. A canoniser $c : \underline{A} \to \underline{G}$ is *equivariant* when post-composing it with the quotient map yields an equivariant map $(a \mapsto [c\,a]_a) : (a : A) \circledast\longrightarrow (\underline{G}/A)a$, i.e. when $c(g \circledast^A a) \overset{g \circledast a}{\sim} g \circledast^{G^{-1}} ca$.

Example 3.22. For a totally ordered set P, we can define the S_2-action on $P \times P$ by $\mathtt{F} \circledast \langle p, q \rangle \coloneqq \langle q, p \rangle$ and a canoniser $c : P \times P \to \underline{\mathrm{S}_2}$ such that $c\,\langle p, q \rangle = \mathtt{I}$ if $p \leq q$, and $c\,\langle p, q \rangle = \mathtt{F}$ if $p > q$. Then c is not strictly equivariant since for any $p \in P$, we have:

$$c\,(\mathtt{F} \circledast \langle p, p \rangle) = c\,\langle p, p \rangle = \mathtt{I} \neq \mathtt{F} = \mathtt{I} * \mathtt{F}^{-1} = \mathtt{F} \circledast_{\langle p,p \rangle} c\,\langle p, p \rangle$$

It is, however, equivariant, since $c\,(\mathtt{F} \circledast \langle p, p \rangle) = \mathtt{I} \overset{\langle p,p \rangle}{\sim} \mathtt{F} = \mathtt{F} \circledast_{\langle p,p \rangle} c\,\langle p, p \rangle$. □

Note that for every equivariant function f and every stabilising element we have:

$$g \in G_a \implies g \circledast fa = \underset{\text{equivariance}}{\downarrow} f(g \circledast a) = \underset{\text{stabiliser}}{\downarrow} fa \implies g \in G_{fa} \qquad \text{i.e.:} \quad G_a \subseteq G_{fa}$$

We thus arrive at the following condition on core functions:

Definition 3.23. Take indexed G-actions $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$, a subfamily $\underline{\Gamma} \vdash X \subseteq \underline{A}$. A function $\underline{\Gamma} \vdash f : (x : X) \to \underline{B}$ is *stable* when it preserves the stabiliser: $G_x \subseteq G_{fx}$ for all $x \in X\gamma$.

Example 3.24. Just as in Example 2.16, consider a non-total ordering P and a stable sorting function, and the permutation sub-action on all tuples with distinct elements $\{\vec{p} \in P^n \mid \forall i, j \in \mathsf{Fin}\, n. p_i \neq p_j\}$. Then, we can define $\mathsf{indexMin} : \underline{P^n} \to \mathsf{Fin}\, n$ that finds the index of a minimal element by $\mathsf{indexMin} \coloneqq \mathsf{wlog}(\mathsf{sort}, (_ \mapsto 0))$.

Now, for any two incomparable p, q, both $\langle p, q\rangle$ and $\langle q, p\rangle$ are sorted, thus canonical. However:

$$(0 \leftrightarrow 1) \circledast ((_ \mapsto 0)\, \langle p, q\rangle) = (0 \leftrightarrow 1) \circledast 0 = 1 \neq 0 = (_ \mapsto 0)\, \langle q, p\rangle = (_ \mapsto 0)\, \big((0 \leftrightarrow 1) \circledast \langle p, q\rangle\big)$$

and so $(_ \mapsto 0)$ is not equivariant on Can sort. It is, however, vacuously stable. Indeed, take a canonical $\vec{p}$ and a $\vec{p}$-stabilising permutation $\pi \in G_{\vec{p}}$. Since all the elements in $\vec{p}$ are distinct, yet $\pi \circledast \vec{p} = \vec{p}$, we have that $\pi = \mathrm{id}$. Therefore $\pi \in G_{f\vec{p}} = G_0$. □

So, in general, stability is strictly weaker than equivariance. Nonetheless, in the presence of an equivariant canoniser, stability and equivariance coincide.

Theorem 3.25. *Let $\Gamma \vdash A$ be an indexed G-action and let $\underline{\Gamma} \vdash c : \underline{A} \to \underline{G}$ be an indexed canoniser. Then, c is equivariant iff for every indexed G-action $\Gamma, x : A \vdash B$, every stable Γ-indexed core function $\Gamma \vdash f : (x : \mathsf{Can}\, c) \to \underline{B}$ is equivariant.*

Unlike before, where only semi-regular actions admitted strictly equivariant canonisers, here every action admits an equivariant canoniser, although we may need to invoke the axiom of choice.

Theorem 3.26. *Using the axiom of choice, every indexed G-action has an equivariant canoniser.*

To us, this use of the axiom of choice indicates that identifying symmetry is a creative activity, rather than a mechanical one.

4 Symmetric algebraic data types

Let us return to the tree lookup function $\mathsf{lookup} : (t : \mathsf{Tree}) \to \mathsf{InPath}\, t \to \mathbb{N}$ from Example 3.2. Consider the symmetry in the two recursive cases

$$\mathsf{lookup}\Big(\ell \swarrow^{n} \searrow r\Big)(\mathsf{L} :: p) \coloneqq \mathsf{lookup}\, \ell\, p \qquad \mathsf{lookup}\Big(\ell \swarrow^{n} \searrow r\Big)(\mathsf{R} :: p) \coloneqq \mathsf{lookup}\, r\, p$$

and define the canoniser on paths by $\mathsf{goLeft}\, \mathsf{Nil} = \mathsf{goLeft}(\mathsf{L} :: p) = \mathtt{I}$ and $\mathsf{goLeft}(\mathsf{R} :: p) = \mathtt{F}$. Then, we can define lookup as follows, with dependent types ruling out inaccessible cases:

$$\mathsf{lookup} \coloneqq \Big(\ell \swarrow^{n} \searrow r\Big) \mapsto \mathsf{wlog}\left(\mathsf{goLeft}, \begin{cases} \mathsf{Nil} & \mapsto n \\ \mathsf{L} :: p' & \mapsto \mathsf{lookup}\, \ell\, p' \end{cases}\right)$$

However, note that lookup and the core function are mutually recursive: lookup is defined in terms of the core function, which then recursively calls lookup on descent. This recursion is structural, but via interdependence through a higher-order function.

Languages such as Agda and Idris have an implicit structural recursion and a termination checker that tries to detect size changes. This type of implicit mutual recursion, called through the canoniser and group action, is typically beyond the termination checker's ability to detect a size change. Some languages provide eliminators explicitly, such as Rocq and Lean, generating an appropriate recursion or induction principle, which the user can use to: (1) define the action on the data type; (2) compose the recursion principle with w.l.o.g. reasoning; and (3) develop induction principles for equivariant reasoning. In this section we will isolate an additional piece of data in addition to the data type, in the form of an action of the group on the data type's *constructors*. From this structure we derive (1)–(3). Furthermore, an implementation that naively defines lookup as above is inefficient. It flips the tree each time the path changes the step direction. Our theory suggests implementation techniques that avoid this inefficiency.

We proceed as follows. We use the well-established framework of *initial algebras*. After a brief recall of functors and their initial algebras (§4.1), we extend them to the symmetric setting (§4.2) through *symmetry strengths* that describe actions in terms of data type constructors. They package folds of equivariant algebras as equivariant traversals. Next, we show how to reuse canonisers for traversals over the same constructors (§4.3), and how symmetry strengths avoid unnecessary data type traversals by progressively acting only on a single layer of constructors (§4.4). Finally, we combine these results with the previous section (§3), adapting data types to the indexed setting (§4.5).

4.1 Initial algebras

In *initial algebra semantics*, each data type signature is specified by a *structure functor* $F : \mathbf{Set} \to \mathbf{Set}$. For example, trees over natural numbers and paths in them from Example 2.4 are given by the following two functors, which closely correspond to their usual data type definitions:

$$\mathbf{data}\ \mathsf{Tree} = \mathsf{Leaf} \mid \mathsf{Node}\ \mathsf{Tree}\ \mathbb{N}\ \mathsf{Tree} \qquad F_{\mathsf{Tree}} X \coloneqq \mathbb{1} + X \times \mathbb{N} \times X$$

$$\mathbf{data}\ \mathsf{Path} = \mathsf{Nil} \mid \mathbf{Step} :: \mathsf{Path} \qquad F_{\mathsf{Path}} X \coloneqq \mathbb{1} + \mathbf{Step} \times X$$

Each functor F has an evident component-wise map $F : (X \to Y) \to (FX \to FY)$, for example:

$$F_{\mathsf{Tree}}\ f\ (\iota_1 \star) \coloneqq \iota_1 \star \qquad F_{\mathsf{Tree}}\ f\ (\iota_2 \langle \ell, n, r\rangle) \coloneqq \iota_2 \langle f\ \ell, n, f\ r\rangle$$

$$F_{\mathsf{Path}}\ f\ (\iota_1 \star) \coloneqq \iota_1 \star \qquad F_{\mathsf{Path}}\ f\ (\iota_2 \langle d, p\rangle) \coloneqq \iota_2 \langle d, f\ p\rangle$$

An *algebra* $\langle X, f\rangle$ for a functor F is a set X together with a function $f : FX \to X$, which describes the evaluation of constructors. For example, the node-counting algebra is the F_{Tree}-algebra $\langle \mathbb{N}, c : (\mathbb{1} + \mathbb{N} \times \mathbb{N} \times \mathbb{N}) \to \mathbb{N}\rangle$, given by $c(\iota_1 \star) \coloneqq 0$ and $c(\iota_2 \langle m_1, _, m_2\rangle) \coloneqq 1 + m_1 + m_2$. A *homomorphism* of F-algebras $h : \langle X, f\rangle \to \langle Y, g\rangle$ is a function $h : X \to Y$ such that $h \circ f = g \circ F\, h$.

We interpret data types by *initial* algebras, denoted by $\langle \boldsymbol{\mu} F, (\mathbf{roll} : F\boldsymbol{\mu} F \to \boldsymbol{\mu} F)\rangle$, whose defining universal property is that for every other F-algebra $\langle X, f\rangle$, there is a unique homomorphism $\mathbf{fold}\ f : \langle \boldsymbol{\mu} F, \mathbf{roll}\rangle \to \langle X, f\rangle$. This homomorphism interprets structurally recursive functions. For example, the initial F_{Tree}-algebra, which we label by $\langle \mathsf{Tree}, \mathbf{roll}_{\mathsf{Tree}}\rangle$, satisfies:

$$\mathbf{roll}_{\mathsf{Tree}}\ \iota_1 \star = \mathsf{Leaf} \qquad \mathbf{roll}_{\mathsf{Tree}}\ \iota_2 \langle \ell, n, r\rangle = \mathsf{Node}\ \ell\ n\ r$$

When readability is more important than precision, we are going to elide **roll**, and identify e.g. $\iota_1 \star$ with Leaf, and $\iota_2 \langle \ell, n, r\rangle$ with Node $\ell\ n\ r$.

For a given F-algebra $\langle X, f\rangle$, the universal property of the initial algebra becomes the recurrence:

$$\mathbf{fold}\ f\ \mathsf{Leaf} = f(\iota_1 \star) \qquad \mathbf{fold}\ f\ (\mathsf{Node}\ \ell\ n\ r) = f(\iota_2 \langle \mathbf{fold}\ f\ \ell, n, \mathbf{fold}\ f\ r\rangle)$$

Through the algebra $\langle \mathbb{N}, c\rangle$, we can compute the number of nodes in a tree t by $\mathbf{fold}\ c\ t$ since

$$\mathbf{fold}\ c\ \mathsf{Leaf} = 0 \qquad \mathbf{fold}\ c\ (\mathsf{Node}\ \ell\ n\ r) = 1 + \mathbf{fold}\ c\ \ell + \mathbf{fold}\ c\ r$$

4.2 Initial equivariant algebras

To transfer our framework to the context of data types, it is not sufficient to equip the initial F-algebra with a G-action $(\circledast) : G \to \boldsymbol{\mu} F \to \boldsymbol{\mu} F$, as this does not tell us what to do for other F-algebras. Instead, we take a more refined construct that describes the interaction of the group with the data type constructors:

Definition 4.1. Let G be a group. A *G-symmetry-strong functor* $F = \left\langle \underline{F}, \mathbf{st}^{G;F} \right\rangle$, or a *$G$-strong functor* for short, is a functor $\underline{F} : \mathbf{Set} \to \mathbf{Set}$ together with a *G-symmetry strength* $\mathbf{st}^{G;F}$, or *G-strength* for

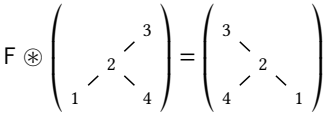
short, which is a natural transformation $\mathbf{st}_X^{G;F} : (\underline{G} \times \underline{F}X) \to \underline{F}(\underline{G} \times X)$ satisfying

$$\mathbf{st}_X(e, u) = \underline{F}(x \mapsto \langle e, x\rangle)\, u$$
$$\mathbf{st}_X(g * h, u) = \underline{F}(\langle g', h', x\rangle \mapsto \langle g' * h', x\rangle)(\mathbf{st}_{G\times X}(g, \mathbf{st}_X(h, u)))$$

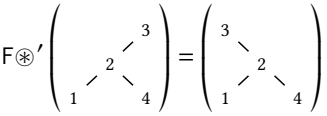
for all $u \in \underline{F}X$ and for all $g, h \in \underline{G}$.

Note that unlike group actions, symmetry strengths also feature the group in the codomain, which allows us to specify how to act on particular sub-terms.

Example 4.2. We can imagine two different $\mathbf{S}_2$-actions on trees, one that recursively flips the whole tree, and one that flips only the top node, with corresponding strengths:



$$\mathbf{st}\ \langle \mathsf{F}, \mathsf{Node}\ \ell\ n\ r\rangle \coloneqq \mathsf{Node}\ \langle \mathsf{F}, r\rangle\ n\ \langle \mathsf{F}, \ell\rangle$$



$$\mathbf{st}'\ \langle \mathsf{F}, \mathsf{Node}\ \ell\ n\ r\rangle \coloneqq \mathsf{Node}\ \langle \mathtt{I}, r\rangle\ n\ \langle \mathtt{I}, \ell\rangle$$

The first strength propagates F to the subtrees, while the second strength propagates $\mathtt{I}$.

We only need to define the strength for F since the first axiom forces it at $\langle \mathtt{I}, u\rangle$ to be $F(x \mapsto \langle \mathtt{I}, x\rangle)u$, i.e., $\mathbf{st}\ \langle \mathtt{I}, \mathsf{Node}\ \ell\ n\ r\rangle \coloneqq \mathbf{st}'\ \langle \mathtt{I}, \mathsf{Node}\ \ell\ n\ r\rangle \coloneqq \mathsf{Node}\ \langle \mathtt{I}, \ell\rangle n \langle \mathtt{I}, r\rangle$. For leaves, we define both strengths to act trivially $\mathbf{st}\ \langle g, \mathsf{Leaf}\rangle \coloneqq \mathbf{st}'\ \langle g, \mathsf{Leaf}\rangle \coloneqq \mathsf{Leaf}$. □

Remark 4.3. The notion of a symmetry strength is related to, but different from the usual Cartesian or monoidal strength. Recall that a *Cartesian strength* for a functor $F : \mathbf{Set} \to \mathbf{Set}$ is a natural transformation $\mathbf{st}^F_{\Gamma,X} : \Gamma \times FX \to F(\Gamma \times X)$ satisfying $\mathbf{st}_{\mathbb{1},X}(\star, u) = F(x \mapsto \langle \star, x\rangle)u$ for all $u \in FX$, and $\mathbf{st}_{\Gamma\times\Delta,X}((\gamma, \delta), u) = F(\langle \gamma', \delta', x\rangle \mapsto \langle\langle \gamma', \delta'\rangle, x\rangle)\left(\mathbf{st}_{\Gamma,\Delta\times X}(\gamma, \mathbf{st}_{\Delta,X}(\delta, u))\right)$ for all $\gamma \in \Gamma$, and $\delta \in \Delta$. (Cf. Lemma D.1 in the Appendix for the diagrams.) Every Cartesian strength is also a G-strength, which leaves constructors as they are and propagates the same group element into the sub-terms. For example, for trees, it acts as:

$$\mathbf{st}_{\underline{G},X}\ \langle g, \mathsf{Leaf}\rangle \coloneqq \mathsf{Leaf} \qquad \mathbf{st}_{\underline{G},X}\ \langle g, \mathsf{Node}\ \ell\ n\ r\rangle \coloneqq \mathsf{Node}\ \langle g, \ell\rangle\ n\ \langle g, r\rangle$$

Symmetry strengths are an instance of the more general *distributive laws* between a monad and a functor [11]. We use this perspective pervasively in our proofs (cf. Appendix F). Here, the monad is the *free G-action* monad, a special case of the *Writer monad*, sometimes known as the *complexity monad* [17]. We use this monadic perspective in §4.4 and §4.5.

We use G-symmetry strengths to lift any action on X to an action on FX:

Lemma 4.4. *Let G be a group and F a G-strong functor. Then, for every G-action A, we have a G-action FA given by:*

$$\underline{FA} \coloneqq \underline{F}\,\underline{A} \qquad (\circledast^{FA}) : \underline{G} \times \underline{FA} \xrightarrow{\mathbf{st}_{\underline{A}}} \underline{F}(\underline{G} \times \underline{A}) \xrightarrow{F(\circledast^A)} \underline{FA}$$

Furthermore, if $h : A \circledast\!\!\longrightarrow B$ is equivariant, so is $F\,h : FA \circledast\!\!\longrightarrow FB$.

Example 4.5. The two tree symmetry strengths from Example 4.2 induce the two expected actions: action induced by the first strength flips the node and propagates symmetry, while for the second strength, the action only flips the top node and does not propagate the symmetry further. Cartesian strengths induce the pointwise lifting of actions. □

Symmetry-strong functors not only lift actions, but as we will see shortly, also uniquely determine actions on their initial algebras. Even more, the resulting algebra structure and the action are compatible in the following sense:

Definition 4.6. Let F be a G-strong functor. An *equivariant F-algebra* $\langle A, f\rangle$ consists of a G-action A and an equivariant map $f : FA \circledast\!\!\longrightarrow A$, i.e., an $\underline{F}$-algebra $\langle \underline{A}, f\rangle$ such that:

$$\begin{array}{ccccc} \underline{G} \times \underline{FA} & & \xrightarrow{\mathbf{st}} & & \underline{F}(\underline{G} \times \underline{A}) \xrightarrow{F(\circledast)} \underline{FA} \\ {\scriptstyle \mathrm{id} \times f}\downarrow & & = & & \downarrow{\scriptstyle f} \\ \underline{G} \times \underline{A} & & \xrightarrow[(\circledast)]{} & & \underline{A} \end{array}$$

An *equivariant algebra homomorphism* $h : \langle A, f\rangle \circledast\!\!\longrightarrow \langle B, g\rangle$ is simultaneously an $\underline{F}$-homomorphism $h : \langle \underline{A}, f\rangle \to \langle \underline{B}, g\rangle$ that is also equivariant $h : A \circledast\!\!\longrightarrow B$.

Recall that initial algebra semantics supports a modular account of data types [86]: coproducts $F_1 + F_2$ of functors are given pointwise by $(F_1 + F_2)X = F_1X + F_2X$, and an algebra for this coproduct functor is given by an algebra structure for each functor over the same carrier set. This modularity extends to symmetry-strong functors and their equivariant algebras:

Proposition 4.7 (modularity)**.** *Let $F_1, F_2 : \mathbf{Set} \to \mathbf{Set}$ be G-strong functors with symmetry strengths $\mathbf{st}_1, \mathbf{st}_2$. The cotupled map $\left[\mathbf{st}_1, \mathbf{st}_2\right] \langle g, \iota_i x\rangle \coloneqq \iota_i\, \mathbf{st}_i \langle g, x\rangle$ is a G-symmetry strength for the coproduct functor $\underline{F}_1 + \underline{F}_2 : \mathbf{Set} \to \mathbf{Set}$. Moreover, given an action A, an equivariant algebra $f : (F_1 + F_2)A \circledast\!\!\longrightarrow A$ for this strength amounts to a pair of equivariant algebra structures $f_i : F_iA \circledast\!\!\longrightarrow A$.*

Using (cf. Appendix D) an appropriate notion of parameterised initiality originally proposed by Bird and Paterson [13], the symmetry strength lets us equip the initial algebra with an action that makes it the *initial equivariant algebra*. Then, to define an equivariant homomorphism $h : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$, we need to define an equivariant F-algebra $g : FA \circledast\!\!\longrightarrow A$, possibly with the w.l.o.g. construction.

Theorem 4.8 (equivariant initiality)**.** *Let F be a G-strong functor and $\mathbf{roll} : \underline{F}\boldsymbol{\mu}\underline{F} \to \boldsymbol{\mu}\underline{F}$ the initial algebra of $\underline{F}$ in $\mathbf{Set}$. Then, there is a unique action $\boldsymbol{\mu}F = \left\langle \boldsymbol{\mu}\underline{F}, (\circledast^{\mu F})\right\rangle$ satisfying*

$$\begin{array}{ccccc} \underline{G} \times \underline{F}\boldsymbol{\mu}\underline{F} & & \xrightarrow{\mathbf{st}} & & \underline{F}(\underline{G} \times \boldsymbol{\mu}\underline{F}) \xrightarrow{F(\circledast^{\mu F})} \underline{F}\boldsymbol{\mu}\underline{F} \\ {\scriptstyle \mathrm{id} \times \mathbf{roll}}\downarrow & & = & & \downarrow{\scriptstyle \mathbf{roll}} \\ \underline{G} \times \boldsymbol{\mu}\underline{F} & & \xrightarrow[(\circledast^{\mu F})]{} & & \boldsymbol{\mu}\underline{F} \end{array}$$

making $\langle \boldsymbol{\mu}F, \mathbf{roll}\rangle$ into an initial equivariant F-algebra, i.e., the initial F-algebra on G-actions: for any equivariant F-algebra $f : FA \circledast\!\!\longrightarrow A$, the unique $\underline{F}$-homomorphism is equivariant: $\mathbf{fold}\, f : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$.

Example 4.9. To see all the modular building blocks in action, define the path lookup function from Example 2.4. The mirroring symmetry of the type Path is captured by the strength:

$$\mathbf{st}^{\mathsf{Path}}\, \langle g, \mathsf{Nil}\rangle \coloneqq \mathsf{Nil} \qquad\qquad \mathbf{st}^{\mathsf{Path}}\, \langle g, d :: x\rangle \coloneqq (g \circledast d) :: \langle g, x\rangle$$

and we can compute that the action given by Theorem 4.8 satisfies:

$$\begin{array}{l} g \circledast (d :: p) = \big((\circledast) \circ (\mathrm{id} \times \mathbf{roll})\big)\, \langle g, \iota_2\, \langle d, p\rangle\rangle = \big(\, \mathbf{roll} \circ F_{\mathsf{Path}}(\circledast) \circ \mathbf{st}\, \big)\, \langle g, \iota_2\, \langle d, p\rangle\rangle \\ \qquad\qquad \text{strength def} \qquad\qquad\qquad\qquad\qquad\qquad \text{equivariant algebra} \\ \qquad\qquad \downarrow \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \uparrow \\ \qquad = \big(\, \mathbf{roll} \circ F_{\mathsf{Path}}(\circledast)\big)(\iota_2\, \langle g \circledast d, \langle g, p\rangle\rangle) = \mathbf{roll}(\iota_2\, \langle g \circledast d, g \circledast p\rangle) = (g \circledast d) :: g \circledast p \end{array}$$

A similar calculation for Nil shows we get the expected action for Path, and a similar set of calculations shows we get the expected recursive action for Tree from the propagating strength

from Example 4.2. We now construct lookup and simultaneously show it is equivariant as a map $\mathsf{Path} \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$. By Theorem 4.8, we can instead define an equivariant algebra:

$$\mathsf{lookup}^{\mathrm{Elim}} : F_{\mathsf{Path}}(\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N}) \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$$

Thanks to the Modularity Proposition 4.7, it suffices to define two equivariant algebra structures for each case of summand of $F_{\mathsf{Path}} = \mathbb{1} + \mathbf{Step} \times -$.

The Nil summand's algebra structure $\mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}} : \mathbb{1} \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$:

$$\mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}} \star\ \mathsf{Leaf} \coloneqq \mathsf{Nothing} \qquad \mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}} \star\ (\mathsf{Node}\ \ell\, n\, r) \coloneqq \mathsf{Just}\, n$$

To show that $\mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}}$ is equivariant, we refer to the fact that currying preserves equivariance, and calculate the behaviour of the uncurried version on the only interesting case:

$$\mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}}(\mathsf{F} \circledast \langle \star, \mathsf{Node}\ \ell\, n\, r\rangle) = \mathsf{lookup}^{\mathrm{Elim}}_{\mathsf{Nil}}\langle \star, \mathsf{Node}\ (\mathsf{F} \circledast r)\, n\, (\mathsf{F} \circledast \ell)\rangle = \mathsf{Just}\, n = \mathsf{F} \circledast \mathsf{Just}\, n$$

For $(::)$, define the algebra $\mathsf{lookup}^{\mathrm{Elim}}_{(::)} : \mathbf{Step} \times (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N}) \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$. Here, we use w.l.o.g. reasoning, as stepping right is the same as stepping left on the flipped tree with the rest of the path flipped. Define the **Step**-canoniser $c' : \mathbf{Step} \circledast\!\!\longrightarrow \mathrm{S}_2^{-1}$ that ensures canonical steps are left steps, i.e. $c'\mathsf{L} = \mathsf{I}$ and $c'\mathsf{R} = \mathsf{F}$. Then, extend it to a canoniser c for the whole domain through projection via Lemma 2.8. Its canonical elements are the tuples $\langle \mathsf{L}, f\rangle$, where f is the recursive call we make when traversing (necessarily left). Thus, we eliminated the symmetric cases in the following core function $\mathsf{lookLeft} : \mathsf{Can}\ c \to (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$:

$$\mathsf{lookLeft}\,\langle \mathsf{L}, f\rangle \coloneqq \begin{cases} \mathsf{Leaf} & \mapsto \mathsf{Nothing} \\ \mathsf{Node}\ \ell\, n\, r & \mapsto f\,\ell \end{cases}$$

Now, we only need to assemble the pieces. As c' is strictly equivariant, so is c by Lemma 2.21, and by Theorem 2.17, all core functions are equivariant, including lookLeft. Thus $\mathsf{lookup}^{\mathrm{Elim}}_{(::)}$ is equivariant by Theorem 2.13. By Proposition 4.7, so is $\mathsf{lookup}^{\mathrm{Elim}}$, and by Theorem 4.8 so is lookup.

To see that lookup indeed matches the expected behaviour, let us compute its behaviour on the symmetric case, recalling that the exponential action conjugates, $(g \circledast f)(a) = g \circledast f(g^{-1} \circledast a)$:

$$\begin{aligned}
&\mathsf{lookup}\ (\mathsf{R} :: p)\ (\mathsf{Node}\ \ell\, n\, r) = \big(\mathbf{fold}(\mathsf{lookup}^{\mathrm{Elim}})\ (\mathsf{R} :: p)\big)(\mathsf{Node}\ \ell\, n\, r) \\
&= \big(\mathsf{lookup}^{\mathrm{Elim}}\ (\iota_2\,\langle \mathsf{R}, \mathsf{lookup}\, p\rangle)\big)(\mathsf{Node}\ \ell\, n\, r) = \big(\mathsf{F} \circledast \mathsf{lookLeft}\,\langle \mathsf{L}, \mathsf{F} \circledast \mathsf{lookup}\, p\rangle\ \big)(\mathsf{Node}\ \ell\, n\, r) \\
&= \mathsf{F} \circledast \Big(\mathsf{lookLeft}\,\langle \mathsf{L}, \mathsf{F} \circledast \mathsf{lookup}\, p\rangle\ \big(\ \mathsf{Node}\ (\mathsf{F} \circledast r)\, n\, (\mathsf{F} \circledast \ell)\big)\Big) \\
&= \mathsf{F} \circledast \big((\mathsf{F} \circledast \mathsf{lookup}\, p)\ (\mathsf{F} \circledast r)\big) = \mathsf{F} \circledast \big(\mathsf{F} \circledast (\mathsf{lookup}\, p\ (\mathsf{F} \circledast \mathsf{F} \circledast r))\big) = \mathsf{lookup}\, p\, r
\end{aligned}$$ □

4.3 Data type traversals w.l.o.g.

The steps in Example 4.9 are common, and we often traverse a data type in different ways but with the same canoniser. In this section, we present reusable abstractions that streamline these steps.

Definition 4.10. Let F be a G-strong functor. A *canoniser* for F is a natural transformation $c_X : \underline{FX} \to \underline{G}$. Each such canoniser induces the *canonical elements functor*:

$$\mathsf{Can}\ c : G\text{-}\mathbf{Act} \to \mathbf{Set} \quad (\mathsf{Can}\ c)A \coloneqq \mathsf{Can}_{FA}\, c_{\underline{A}} \coloneqq \big\{(c_{\underline{A}} u) \circledast^{FA} u \,\big|\, u \in \underline{FA}\big\} \quad (\mathsf{Can}\ c)h : u \mapsto (\underline{Fh})u$$

A canoniser c thus induces a natural assignment of canonisers $c_{\underline{A}} : \underline{FA} \to \underline{G}$ for each lifted G-action FA. The naturality condition means canonisers are determined by their component at the singleton $\mathbb{1}$, i.e., by a canoniser for $\underline{F\mathbb{1}}$. The unique extension of such a canoniser $c_{\mathbb{1}} : \underline{F\mathbb{1}} \to \underline{G}$ to a canoniser for F is given by the following composition $c_X : \underline{FX} \xrightarrow{\underline{F\langle\rangle}} \underline{F\mathbb{1}} \xrightarrow{c_{\mathbb{1}}} \underline{G}$.

Example 4.11. The $\mathbb{S}_2$-strong functor F_{Path} has the canoniser (cf. p. 16) and canonical elements:

$$\mathsf{goLeft}\ \mathsf{Nil} \coloneqq \mathtt{I} =: \mathsf{goLeft}(\mathsf{L} :: p) \quad \mathsf{goLeft}(\mathsf{R} :: p) \coloneqq \mathtt{F} \qquad \mathsf{Can}_A\,\mathsf{goLeft} \coloneqq \left\{\mathsf{Nil}, \mathsf{L} :: a \,\middle|\, a \in \underline{A}\right\} \quad \square$$

We can now streamline the data we need to specify to traverse a symmetric data type using an algebra, or to reason about such traversals using symmetry:

Definition 4.12. Let F be a G-strong functor and $c : \underline{F} \to \underline{G}$ a canoniser for it. A *c-core F-algebra* $\langle A, f\rangle$ consists of a G-action A equipped with a function $f : (\mathsf{Can}\ c)A \to \underline{A}$. It is *equivariant* when f is equivariant $f : ((\mathsf{Can}\ c)A \subseteq FA) \circledast\!\!\longrightarrow A$. A *homomorphism* of equivariant c-core F-algebras $h : \langle A, f\rangle \to \langle B, g\rangle$ is an equivariant map $h : A \circledast\!\!\longrightarrow B$ satisfying: $h(f\,u) = g\,((\mathsf{Can}\ c)h\,u)$.

We can rearrange the constructs in Example 4.9 using these concepts:

Example 4.13. We have the following equivariant goLeft-core F_{Path}-algebra:

$$\mathsf{lookup}^{\mathsf{Core}} : (\mathsf{Can}\ \mathsf{goLeft})(\mathsf{Tree} \to \mathsf{Triv}\mathsf{Maybe}\,\mathbb{N}) \to \underline{\mathsf{Tree} \to \mathsf{Triv}\mathsf{Maybe}\,\mathbb{N}} = (\mathsf{Tree} \to \mathsf{Maybe}\,\mathbb{N})$$

$$\mathsf{Nil} \mapsto \begin{cases} \mathsf{Leaf} & \mapsto \mathsf{Nothing} \\ \mathsf{Node}\ \ell\ n\ r & \mapsto \mathsf{Just}\ n \end{cases} \qquad \left(\mathsf{L} :: (\mathsf{Tree} \xrightarrow{\mathsf{rec}} \mathsf{Maybe}\,\mathbb{N})\right) \mapsto \begin{cases} \mathsf{Leaf} & \mapsto \mathsf{Nothing} \\ \mathsf{Node}\ \ell\ n\ r & \mapsto \mathsf{rec}\,\ell \end{cases} \quad \square$$

These ingredients streamline the steps of Example 4.9, using the portmanteau fold wlog:

$$\left(\mathsf{Can}_{FA}\,c_{\underline{A}} = (\mathsf{Can}\ c)A \xrightarrow{f} \underline{A}\right) \mapsto \left(F\underline{A} \xrightarrow{\mathsf{wlog}(c_{\underline{A}}, f)} \underline{A}\right) \mapsto \left(\mathbf{flog}_A(c, f) : \underline{\boldsymbol{\mu}F} \xrightarrow{\mathbf{fold}\ \mathsf{wlog}(c_{\underline{A}}, f)} \underline{A}\right)$$

We chain Theorem 2.13 and the Equivariant Initiality Theorem 4.8:

Theorem 4.14 (core initiality). *Let F be a G-strong functor,* $\mathbf{roll} : \underline{F\boldsymbol{\mu}F} \to \underline{\boldsymbol{\mu}F}$ *an initial algebra of* $\underline{F}$*, and c a canoniser for F. Then restricting* **roll** *to canonical elements makes $\boldsymbol{\mu}F$ into the initial c-core F-algebra* $\mathbf{roll} : (\mathsf{Can}\ c)\boldsymbol{\mu}F \circledast\!\!\longrightarrow \boldsymbol{\mu}F$*: for any equivariant c-core F-algebra $f : (\mathsf{Can}\ c)A \circledast\!\!\longrightarrow A$, the unique equivariant c-core F-algebra homomorphism into f is:* $\mathbf{flog}(c, f) : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$.

This theorem implies, for example, that the lookup function from Example 4.13 is the unique equivariant goLeft-core F_{Path}-homomorphism given by **flog**.

Example 4.15. We reuse the canoniser to define the *subtree projection* function

$$\mathsf{subtree} \coloneqq \mathbf{flog}(\mathsf{goLeft}, \mathsf{subtree}^{\mathsf{Core}}) : \mathsf{Path} \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathsf{Tree})$$

$$\mathsf{subtree}^{\mathsf{Core}} : (\mathsf{Can}\ \mathsf{goLeft})(\mathsf{Tree} \to \mathsf{Maybe}\,\mathsf{Tree}) \circledast\!\!\longrightarrow (\mathsf{Tree} \to \mathsf{Maybe}\,\mathsf{Tree})$$

$$\mathsf{Nil} \mapsto (t \mapsto \mathsf{Just}\ t) \qquad (\mathsf{L} :: \mathsf{Tree} \xrightarrow{\mathsf{rec}} \mathsf{Maybe}\,\mathsf{Tree}) \mapsto \begin{cases} \mathsf{Leaf} & \mapsto \mathsf{Nothing} \\ \mathsf{Node}\ \ell\ n\ r & \mapsto \mathsf{rec}\,\ell \end{cases} \quad \square$$

4.4 Partially evaluating actions

Both lookup from Example 4.9 and subtree from Example 4.15 give us the result we want. But implementations that naively follow our definitions will repeatedly flip their arguments, and the subtree implementation will also flip its result, leading to high time and space complexity. Faithful to our motivation, we only demonstrate which mathematical structures underlie a more efficient implementation, and leave a systematic account of performance engineering to future work.

We use a general principle from modern partial evaluation folklore: instead of performing an expensive operation repeatedly, axiomatise its properties and design an efficient implementation for its free algebra. Then evaluate the free algebra back into the desired structure after partial evaluation. In our case, we shall build on top of the *free action* $G \circledast X$ on a set X, given by $\underline{G \circledast X} = \underline{G} \times X$

and $g \circledast^{G \boxtimes X} \langle h, x\rangle = \langle g * h, x\rangle$. The free action lets us accumulate the symmetries while leaving the input unchanged, and a pair $\langle h, x\rangle \in \underline{G \boxtimes X}$ captures a delayed evaluation of $h \circledast^{A} x$ for some G-action A with $\underline{A} = X$.

In particular, consider $G \boxtimes \boldsymbol{\mu} F$, the free G-action on the initial F-algebra. When at some point in a definition we want to inspect $\langle g, t\rangle$, we should not simply unroll t, as that ignores the accumulated symmetries. We also do not want to compute $g \circledast t$ in implementations, since that is inefficient. What we do instead is use the symmetry strength to act only on the first layer of the data type and propagate the action into a delayed evaluation of a subtree represented by the free-action monad:

$$\underline{G \boxtimes \boldsymbol{\mu} F} = \underline{G} \times \boldsymbol{\mu} F \xrightarrow{\underline{G} \times \mathbf{unroll}} \underline{G} \times F \boldsymbol{\mu} F \xrightarrow{\mathbf{st}^{F}_{\boldsymbol{\mu} F}} F(\underline{G} \times \boldsymbol{\mu} F) = F(\underline{G \boxtimes \boldsymbol{\mu} F})$$

From Theorem 4.8, we get $g \circledast t = F(\circledast)(\mathbf{st}\ \langle g, t\rangle)$ (ignoring unrolling), meaning that the symmetry strength both gives us a symmetry-respecting pattern matching of a data type, and represents a symmetry-accumulating implementation that avoids inefficient repeated transformations.

To see the construction in action, we can equivalently compute subtree $p\ t$ with the free action:

$$\begin{array}{ll} \mathsf{subtree}\ p\ t = & \text{where:} \\ \quad \mathsf{let}\ \langle g, s\rangle = \mathsf{subtree}^{\mathsf{aux}}\ p\ \langle \mathtt{I}, t\rangle & \quad \mathsf{subtree}^{\mathsf{aux}} : \mathsf{Path} \circledast\!\!\longrightarrow (\mathsf{S}_2 \boxtimes \mathsf{Tree} \to \mathsf{S}_2 \boxtimes \mathsf{Maybe\,Tree}) \\ \quad \mathsf{in}\ g \circledast s & \quad \mathsf{subtree}^{\mathsf{aux}} = \mathbf{flog}(\mathsf{goLeft}, \mathsf{subtree}^{\mathsf{auxCore}}) \end{array}$$

and $\mathsf{subtree}^{\mathsf{auxCore}}$ is an equivariant goLeft-core F_{Path}-algebra over $\mathsf{S}_2 \boxtimes \mathsf{Tree} \to \mathsf{S}_2 \boxtimes \mathsf{Maybe\,Tree}$:

$$\mathsf{subtree}^{\mathsf{auxCore}} : \mathsf{Can\ goLeft}\ (\mathsf{S}_2 \boxtimes \mathsf{Tree} \to \mathsf{S}_2 \boxtimes \mathsf{Maybe\,Tree}) \to (\mathsf{S}_2 \boxtimes \mathsf{Tree} \to \mathsf{S}_2 \boxtimes \mathsf{Maybe\,Tree})$$

$$\mathsf{Nil} \mapsto (\langle g, t\rangle \mapsto \langle g, \mathsf{Just}\ t\rangle)$$

$$\left(\mathsf{L} :: \left(\begin{array}{c}\mathsf{S}_2 \boxtimes \mathsf{Tree} \xrightarrow{\mathrm{rec}} \\ \mathsf{S}_2 \boxtimes \mathsf{Maybe\,Tree}\end{array}\right)\right) \mapsto \left(\langle g, t\rangle \mapsto \begin{cases} \langle g, \mathsf{Nothing}\rangle & (\mathbf{st}\ \langle g, t\rangle = \mathsf{Leaf}) \\ \mathrm{rec}\ \langle g_\ell, \ell\rangle & (\mathbf{st}\ \langle g, t\rangle = \mathsf{Node}\ \langle g_\ell, \ell\rangle\ n\ \langle g_r, r\rangle) \end{cases}\right)$$

Whether the tree in the last case is flipped or not, applying the strength ensures the correct sub-structure resides in the left sub-tree and g_ℓ appropriately propagates the symmetry. More importantly, an implementation of this design never flips the tree. For example, we have:

$$\begin{aligned} &\mathsf{subtree}^{\mathsf{aux}}(\mathsf{R} :: \mathsf{Nil})\ \langle \mathtt{I}, \mathsf{Node}\ \ell\ n\ r\rangle \\ &\qquad = \mathsf{F} \circledast \mathsf{subtree}^{\mathsf{auxCore}}(\mathsf{L} :: \mathsf{subtree}^{\mathsf{aux}}(\mathsf{F} \circledast \mathsf{Nil}))(\mathsf{F} \circledast \langle \mathtt{I}, \mathsf{Node}\ \ell\ n\ r\rangle) \\ &\qquad = \mathsf{F} \circledast \mathsf{subtree}^{\mathsf{auxCore}}(\mathsf{L} :: \mathsf{subtree}^{\mathsf{aux}}\mathsf{Nil})\ \langle \mathsf{F}, \mathsf{Node}\ \ell\ n\ r\rangle \\ &\qquad = \mathsf{F} \circledast \mathsf{subtree}^{\mathsf{aux}}\mathsf{Nil}\ \langle \mathsf{F}, r\rangle = \mathsf{F} \circledast \langle \mathsf{F}, \mathsf{Just}\ r\rangle = \langle \mathtt{I}, \mathsf{Just}\ r\rangle \end{aligned}$$

where in the reduction of $\mathsf{subtree}^{\mathsf{auxCore}}$, we used that $\mathbf{st}\ \langle \mathsf{F}, \mathsf{Node}\ \ell\ n\ r\rangle = \mathsf{Node}\ \langle \mathsf{F}, r\rangle\ n\ \langle \mathsf{F}, \ell\rangle$. As we can see, the only evaluated actions were the free ones, and the subtree r, for example, remained unflipped throughout the argument.

There are further opportunities for optimisation. For example, instead of stacking output symmetries $g \circledast -$ (in contrast to the input ones that get absorbed by the free action) we could combine them into a single symmetry as $g \circledast (h \circledast a) = (g * h) \circledast a$. In fact, in this specific example, we can go even further and ignore the output symmetries altogether. By the Core Initiality Theorem 4.14, we have $(\circledast^{\mathsf{Maybe\,Tree}}) \circ \mathsf{subtree}^{\mathsf{aux}}\ p\ \langle g, t\rangle = \mathsf{subtree}\ p(g \circledast^{\mathsf{Tree}} t)$. Furthermore, we can show that $\pi_1\ (\mathsf{subtree}^{\mathsf{aux}}\ p\ \langle g, t\rangle) = g$, hence $\mathsf{subtree}\ p\ t = \pi_2\ (\mathsf{subtree}^{\mathsf{aux}}\ p\ \langle \mathtt{I}, t\rangle)$ and the output symmetry is never used, but is merely a reasoning device for the correctness of the implementation.

simply-typed concept	dependently-typed concept	categorical concept
Set	$\mathbf{Fam}_{\underline{\Gamma}}$	category C
functor $F : \mathbf{Set} \to \mathbf{Set}$	functor $F : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$	functor $F : C \to C$
free G-action monad $\underline{P}X \coloneqq \underline{G} \times X$	free Γ-indexed G-action monad $\underline{P}(\underline{\Gamma} \vdash X) \coloneqq \underline{\Gamma} \vdash G \circledast X$	monad structure P over $\underline{P} : C \to C$
G-action $\underline{G} \times \underline{A} \xrightarrow{\langle g,a\rangle \mapsto g \circledast a} \underline{A}$	Γ-indexed G-action $G \circledast \underline{A} \xrightarrow{\langle g,a\rangle \mapsto g \circledast_{g^{-1} \circledast \gamma} a} \underline{A}$	P-algebra $P\underline{A} \to \underline{A}$
G-strength $\mathbf{st} : \underline{G} \times FX \to F(\underline{G} \times X)$	Γ-indexed G-strength $\mathbf{st} : G \circledast (FX) \to F(G \circledast X)$	monad-functor distributive law $\mathbf{st} : PF \to FP$
functor $S\underline{X} \coloneqq \underline{G} \to X$	functor $S(\underline{\Gamma} \vdash X) \coloneqq \underline{\Gamma} \vdash G \multimap X$	right-adjoint $\underline{P} \dashv E$ (cf. Theorem F.4)
parameterised traversal $\underline{G} \times \boldsymbol{\mu}F \xrightarrow{\mathbf{pfold}\left(FX \xrightarrow{f} X\right)} X$	indexed parameterised traversal $G \circledast \boldsymbol{\mu}F \xrightarrow{\mathbf{pfold}\left(FX \xrightarrow{f} X\right)} X$	parameterised fold $T\boldsymbol{\mu}F \xrightarrow{\mathbf{pfold}\left(FX \xrightarrow{f} X\right)} X$
equivariant F-algebra $f : FA \circledast\!\!\to A$	indexed equivariant F-algebra $f : FA \circledast\!\!\to A$	F-algebra for lifted functor $F : C^P \to C^P$
canoniser $c : F \to \underline{G}$	indexed canoniser $c : F \to \underline{G}$	
canonical elements $\mathsf{Can}\ c : G\text{-}\mathbf{Act} \to \mathbf{Set}$	canonical elements $\mathsf{Can}\ c : G\text{-}\mathbf{Act}_{\Gamma} \to \mathbf{Fam}_{\underline{\Gamma}}$	canonical elements $\mathsf{Can}\ c : C^P \to C$

Fig. 1. Summary of symmetric data type theory

4.5 Indexed data types

In Example 4.9, we fell back to simple types, but thanks to the generality of the initial algebra semantics approach, a dependently-typed development follows the same lines and recovers the finer version from Example 3.2. Moreover, it uncovers nuances that degenerate in the simply-typed case. For example, the notion of a symmetry strength must in fact be phrased in terms of the *free action* $G \circledast X$ over a family. The carrier of the free action coincides with the Cartesian product $\underline{G} \times X$ in the simply-typed case, but differs in the indexed case. As we pointed out in Remark 4.3, viewing this product as the free-action monad also emphasises the role of the symmetry strength as a monad-functor distributive law. Once we explicate this structure, much of the development amounts to repeating the simply-typed development with the adjective 'indexed' peppered throughout. Appendix A repeats the development, and we describe the changes here. Fig. 1 summarises the difference between the simply typed theory and its dependently typed counterpart as follows. Where appropriate, we also describe the categorical concept.

Although the categorical theory does not capture all concepts, e.g. canonisers, it suffices to assign to almost every concept its type. The theory includes indexed versions of the Modularity Proposition 4.7, the Equivariant Initiality Theorem 4.8 and Core Initiality Theorem 4.14.

We generalise from the category **Set** to $\mathbf{Fam}_{\underline{\Gamma}}$, the category of $\underline{\Gamma}$-indexed sets and vertical maps. The main technical device we use to generalise from **Set** to $\mathbf{Fam}_{\underline{\Gamma}}$ is the free Γ-indexed G-action adjunction between $\mathbf{Fam}_{\underline{\Gamma}}$ and G-$\mathbf{Act}_{\Gamma}$—the category of Γ-indexed G-sets and vertical equivariant maps. Its monadicity means we can capture its structure categorically, and we use the existence of a right adjoint S to the resulting monad T over $\mathbf{Fam}_{\underline{\Gamma}}$ in one of the proofs (cf. Theorem F.4).

For G-action Γ, we define, for each $\underline{\Gamma}$-family X, the *free* Γ*-indexed* G*-action over* X:

$$\underline{(g : G) \times g \circledast X}_{\gamma} \coloneqq (g : \underline{G}) \times X_{g^{-1} \circledast \gamma} \qquad g \circledast_{\gamma} \langle h, x : X_{h^{-1} \circledast \gamma} \rangle \coloneqq \langle g * h, x : X_{h^{-1} \circledast g^{-1} \circledast g \circledast \gamma} \rangle$$

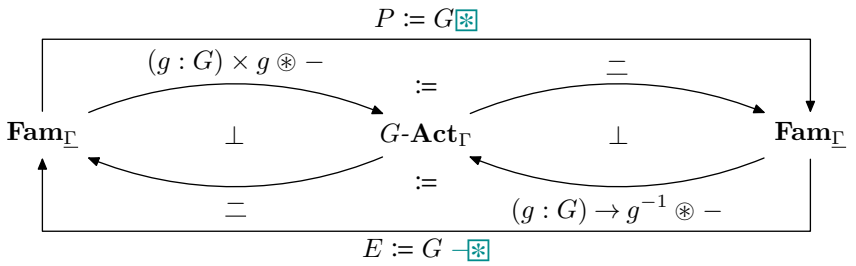


Fig. 2. Categorical situation for indexed G-action

We also define $(g : G) \to g^{-1} \circledast X$, the *cofree* Γ*-indexed* G*-action over* X. Its fibres are the dependent-function fibres $\underline{(g : G) \to g^{-1} \circledast X}_\gamma := (g : \underline{G}) \to X_{g \circledast \gamma}$, defined by:

$$g \circledast_\gamma (f : (k : \underline{G}) \to X_{k \circledast \gamma}) := h \mapsto f(h * g) \in (h : \underline{G}) \to X_{h \circledast g \circledast \gamma}$$

They are the two adjoints to the forgetful functor from Γ-indexed actions to Γ-indexed families:

Theorem 4.16. *For a* G*-action* Γ *and family* $\underline{\Gamma} \vdash X$*, the map* $\Gamma \vdash x \mapsto \langle e, x\rangle : X \to \underline{(g : G) \times (g \circledast X)}$ *is the universal* Γ*-indexed* G*-action over* X*. The map* $\underline{\Gamma} \vdash \mathrm{eval}\,\langle -, e\rangle : \underline{(g : G) \to g^{-1} \circledast X} \to X$ *is the universal* Γ*-indexed* G*-action under* X*. The resulting two adjunctions are (co)monadic.*

This theorem generalises the non-indexed case, where $\underline{G} \times X$ has the structure of the free G-action over X. The existence of the adjoints and their (co)monadicity follow from abstract reasons. Let: $\oint F$ be the Grothendieck construction for a presheaf $F : \mathbb{C}^{\mathrm{op}} \to \mathbf{Set}$; $|C|$ be the discrete category underlying a category C, and $\hat{\mathbb{C}}$ the presheaf category of $\mathbb{C}$. Consider a G-action Γ as a presheaf over the category with one object and morphisms the G-elements. We then have the following two equivalences. First, Γ-indexed actions are equivalent to presheaves over $\oint \Gamma$ $G\text{-}\mathbf{Act}_\Gamma \simeq \widehat{\oint \Gamma}$. Forgetting the functorial action then recovers the category of $\underline{\Gamma}$-indexed families, a presheaf category itself: $\mathbf{Fam}_{\underline{\Gamma}} \simeq \widehat{\oint \underline{\Gamma}} = \widehat{\left|\oint \Gamma\right|}$. The forgetful functor $G\text{-}\mathbf{Act}_\Gamma \to \mathbf{Fam}_{\underline{\Gamma}}$ arises as precomposition by $J : \oint \Gamma \leftarrow \left|\oint \Gamma\right|$. Consequently, the two adjoints are given by (co)end formulae, and their monadicity follows by surjectivity of this functor [32, Prop. 1.1]. This situation is exploited by Fiore and Szamozvancev to account for mathematical and computational representations of abstract syntax with binding and substitution [33, 34, 87]. One can use the coend formula to calculate the explicit descriptions we gave the two adjoints. We show directly (cf. Appendix E) that these descriptions are the adjoints, and for completeness, we also show monadicity and comonadicity using Beck's theorem. We then have the situation in Fig. 2. Therefore, P is a monad, E is a comonad, and $P \dashv E$. Moreover, $P^2 := P \circ P \dashv E^2$.

5 Conclusion

5.1 Related work

W.l.o.g. in theorem provers. Given that w.l.o.g. is a common phrase in mathematical proofs, it comes as no surprise that several major theorem provers feature a similarly named concept. What is more compelling is that the treatment is far from uniform, pointing toward a missing uniform foundation. Our work provides a uniform foundation for symmetric uses of w.l.o.g..

For example, the Rocq library, SSReflect [43], Isabelle/HOL's Archive of Formal Proofs [89] and the Lean 4 Mathlib [88], define tactics named `wlog`, which cut in an additional statement ψ

when proving φ. Rocq's tactic[4] creates an additional subgoal $(\psi \Rightarrow \varphi) \Rightarrow \varphi$. Isabelle/HOL's tactic similarly adds assumptions w.l.o.g., and further accounts for generalisation of variables, explicitly documenting symmetric arguments as the motivation. Lean's tactic[5] additionally assumes $\neg\psi$, adding a subgoal $(\psi \Rightarrow \varphi) \Rightarrow \neg\psi \Rightarrow \varphi$. In all three tactics, the additional subgoal (e.g., ψ in Rocq and Lean) can be arbitrary and not tied to any particular symmetry, so it could be worth investigating how many of its uses correspond to the assumption of canonicity in our framework.

Agda Stdlib defines[6] `wlog` : $(\forall(a\,b : A).a\,R\,b \Rightarrow Q\,a\,b) \Rightarrow (\forall a\,b.Q\,a\,b)$ for any total relation R and a symmetric predicate Q. Here, we have a swapping S_2-action on the domain $A \times A$, while Q provides an appropriate indexed action on the codomain. The totality of R encodes the canoniser implicitly, and the assumption exactly corresponds to our core function. Dijkstra [27] uses a similar setting to criticise w.l.o.g. arguments for not explicating the underlying symmetry.

A richer collection of symmetries can be found in Harrison's [45] seminal paper on w.l.o.g. tactics in HOL. In addition to the tactic discussed in §3.3, Harrison develops four additional tactics for w.l.o.g. reasoning in geometry, using a bank of results about invariance and equivariance of various operations under translations and orthonormal transformations. Three tactics are immediate special cases of our principle, while the fourth one is a reduction from a predicate on points of the form $(x, y, 0) \in \mathbb{R}^3$ to a predicate on $\mathbb{R}^2$. Schmoetten et al. [78, 79] use Harrison's approach and prove further w.l.o.g. lemmata when formalising Schutz's axioms for Minkowski spacetime [80].

In summary, our work does not account for all previous principles named `wlog`. Instead, we offer a crisp criterion by which one can distinguish symmetric w.l.o.g. arguments.

Nominal techniques. Nominal techniques are a close topic in programming languages, an established approach to treating bound variables, in which α-equivalence is defined with groups of permutations of atoms acting on terms built from such atoms [66, 68, 69]. Our approach borrows from, builds upon, and is analogous to these nominal techniques. Like nominal techniques, we make pervasive use of, and rely on, equivariance and related concepts [68]. Our use of symmetry strengths is similar to Blanchette et al.'s [14] use of bounded natural functors. The proof obligations we require to establish the existence of recursively defined functions and their compatibility with the relevant operators is also similar to the recursors and induction principles in nominal techniques [14, 38, 63, 67, 73, 74, 91], and so on. Nominal techniques are typically used with the group of finitely-supported permutations of names, but not always. The finite-support requirement is sometimes relaxed [14, 19, 29]. The names we permute may have additional structure [15]. Nominal metatheory typically employs w.l.o.g. reasoning pervasively, cf., e.g., Cheney's [19] thesis.

Unlike nominal techniques, our recursion principles do not solely account for binders and α-equivalence. They do require the additional structure of canonisers. Whereas in nominal techniques one stays equivariant throughout, in symmetric programming there is no such requirement and outside the definition of a w.l.o.g. construction, code or reasoning may violate equivariance. We want to revisit this comparison after we develop symmetric programming and reasoning further. An even more interesting direction is to combine symmetric programming and nominal techniques, pervasively maintaining nominal equivariance, but potentially violating equivariance for non-nominal symmetries. Mechanically representing and reasoning about nominal data is a wide area of research [1–3, 6, 7, 12, 14, 18, 20, 21, 25, 30, 37–40, 42, 44, 46, 51–54, 62, 64, 65, 72, 75, 77, 82, 84, 85, 90, 96]. While there are first steps towards nominal type theories [5, 70], we still lack an implementation of a nominal dependently-typed system.

[4] Rocq Reference Manual: https://rocq-prover.org/doc/V9.2.0/refman/proof-engine/ssreflect-proof-language.html#rocq:tacn.wlog
[5] Mathlib4 documentation: https://leanprover-community.github.io/mathlib4_docs/Mathlib/Tactic/WLOG.html
[6] Agda Stdlib: https://github.com/agda/agda-stdlib/blob/c2abce1b8e72ccae49f73791d0996eaf23674357/src/Relation/Binary/Consequences.agda#L197

Relational parametricity. If we view each symmetry $g \in G$ as a relation $a \equiv_g b$ given by $g \circledast a = b$, then equivariance becomes relational preservation: $a \equiv_g b \implies f\ a \equiv_g f\ b$. This perspective suggests some connections with logical relations [71] and with relational parametricity [76]. A possible connection is the work of Atkey [4] on using parametricity and Noether's theorem to derive invariants of physical systems. A shared theme is identifying the group actions that describe a system's symmetries. However, applying Noether's theorem requires a notion of differentiation, which is not necessarily present in our general setting. One direction for future work is to investigate which of our action combinators can be translated to smooth-manifold settings, and whether they can serve as compositional operators for describing physical systems. It may be fruitful to explore other connections. For example, there might be some proofs for free theorems [92] that appeal to parametricity through relations defined via symmetry. There might be symmetric invariants for restricted programming languages (e.g., with nominal features) provable via logical relations.

Symmetry in programming languages and type theory. A more recent development on symmetries in programming is a Hoare logic for symmetry properties by Mehta and Hsu [60]. It features triples that relate the symmetries of preconditions to those of postconditions. In particular, a triple of the form $(G, A)C(H, B)_\varphi$ uses a G-action A to capture symmetries of input states and an H-action B to capture symmetries of output states after executing the program C. The program C is required to be equivariant with respect to a group homomorphism $\varphi : G \to H$. More precisely: $\forall g \in G, a \in \underline{A}.C(g \circledast^A a) = \varphi(g) \circledast^B C(a)$. Beyond general action constructions such as (non-dependent) products and pre-/post-composition, the paper develops a forward-reasoning system that simultaneously derives an action on the output and proves the equivariance of C. As we move from mathematical foundations toward more practical symmetric programming, we may adapt these rules to ease the construction of the group actions required by the w.l.o.g. construction.

Symmetry elsewhere in computer science. Computer science is vast, and group theory is pervasive, so there are many points of contact between the two. Rather than attempting a comprehensive review, we highlight a few representative areas and point to recent surveys for further reading.

In computer algebra and computational group theory, groups are both the object of study and a computational resource, shaping algorithm design and complexity analysis in areas such as permutation-group algorithms and constructive recognition [47, 81]. The concept of *canonical labelling* from nauty/Traces [59], which finds the vertex permutation mapping a graph into its representative element w.r.t. graph isomorphism, exactly matches our canonisers. It is worth investigating how many algorithms building on it fit into our w.l.o.g. pattern.

In constraint programming and satisfiability, symmetries have long been a central concern. A large body of work studies symmetry-breaking techniques, which add constraints that rule out symmetric solutions while preserving satisfiability [41, 48, 95]. In machine learning, symmetry appears both as an architectural prior (equivariance/invariance) and as an analysis tool. In computer vision, it supports tasks such as recognition, reconstruction, and compression of geometric data [8, 26, 98].

Similarly, model checking techniques and tools exploit symmetry to mitigate the state-space explosion problem [23, 24, 28, 61, 83]. Model checkers typically try to compute the relevant symmetries [e.g. 16, 22, 55, 93, 94], and in the general case this computational task is equivalent to the graph isomorphism problem [49], whose precise complexity class is still open.

5.2 Future work

On the foundational side, it may be interesting to explore richer data type constructions, such as: co-data and co-recursion via terminal co-algebras; and universes. The theory of distributive laws also applies to F-coalgebras, suggesting there is a similar theory of coinductive data-types. Universes offer various directions, depending on the symmetries one may want to equip the inhabitants of

the universe. One option is to equip a universe of types with the trivial action, as we did with the universe of propositions (§3.3).

A richer direction involves a universe $\mathcal{U}_G$ of G-actions, for some or each group G. Here each value of the universe is a code for the underlying carrier and the G-action. This universe supports the various type constructors using the usual type-interpretation in the category of G-actions. While we can equip this universe with a trivial G-action, we can also equip it with other actions.

For example, given a symmetry $g \in \underline{G}$ and an inhabitant $A \in \mathcal{U}_G$ with $[\![A]\!] = (\underline{A}, \circledast)$, define $g \circledast_{\mathcal{U}_G} A$ as the action with the carrier unchanged $\underline{g \circledast A} \coloneqq \underline{A}$ which acts through conjugation $h \circledast_{g \circledast A} x \coloneqq (g^{-1} * h * g) \circledast x$. These definitions give a map $\underline{G} \times \mathcal{U}_G \to \mathcal{U}_G$, and moreover this map is a G-action over $\mathcal{U}_G$. So in this case there is some room to explore symmetries on a universe of G-actions and potential to employ symmetric programming/reasoning here. In another direction the equivariant initial algebra theorem may internalise to an equivariant function on codes.

In another kind of universe, each inhabitant describes a group G and a code in a universe $\mathcal{U}_{[\![G]\!]}$ of G-actions. One can then similarly look for useful actions and symmetric programming/reasoning there. Another direction in this area would be to explore codes for homomorphisms between codes for G-actions and actions and corresponding transport functions between their decoded G-actions and actions. This direction may open up questions regarding coherence of the resulting type theory.

That said, our development does not need a universe, it is merely compatible with these various choices, and we plan to explore them in future work.

On the practical side, we want to refine the developed modular mathematical abstractions into programming constructs, guided by more involved symmetric programming and reasoning examples. In the first instance, we want to complete the full set of operations on self-balancing binary search trees [58]. Another promising example is Escardó's [31] representation of exact reals using infinite streams of signed-digit numerals. Operations on these streams and proofs about these operations contain multiple symmetric cases, including swapping the roles of symmetric variables, and reflecting the digits around 0. Computable representations of the constructive Dedekind reals [9, 10, 50] employ symmetric operations on the cut's lower and upper sets, with symmetric programming potential.

It may be worth exploring symmetric programming and reasoning for model checking. Since symmetric programming exposes symmetric program paths explicitly, it may alleviate the need to automatically detect symmetry when checking symmetric programs. A more interesting direction is whether a symmetry-detecting model checker can suggest refactoring opportunities that use symmetry more explicitly. Another direction involves using symmetric programming when implementing model checkers or constraint solvers.

In addition to being interesting in their own right, such examples should guide us in developing abstractions for performance engineering, as well as on how to most ergonomically present groups, actions, canonisers, core functions, and equivariance to the programmer. For example, immediate canonisers (see Proposition 2.22) could admit an interface similar to *lazy constructors* [56], where we extend a data type definition with non-canonical constructors together with their non-trivial canonising symmetries, but list only canonical cases in pattern matching, since the non-canonical ones are covered by the w.l.o.g. construction.

We already explored the landscape with two experiments in Idris and Lean. Having a clean mathematical resolution of issues that surfaced, such as termination and efficiency, we can now return to both the programming language and the proof assistant: not to increase confidence in the results' correctness, but to develop a library of reusable results and lay a foundation for future implementation and mechanisation.

Acknowledgments

Supported by a Royal Society University Research Fellowship, an Advanced Research and Invention Agency (ARIA) Safeguarded AI grant Qbs4Safety, and an Alan Turing Institute Seed Funding grant. This material is partly based upon work supported by the Air Force Office of Scientific Research under award number FA9550-21-1-0024.

We are grateful to the anonymous referees and the following individuals for useful comments, suggestions, and pointers: Guillaume X. Allais, Andrej Bauer, Greg Brown, James Cheney, Rob Cornish, Pierre-Evariste Dagand, Marcelo P. Fiore, Nicola Gambino, Jeremy Gibbons, Justin Hsu, Martin E. Hyland, András Kovács, Neel Krishnaswami, Sam Lindley, Justus Matthiesen, Amaury Mazoyer, James McKinna, Georg Moser, Sean K. Moss, Bruno Oliveira, Andrew M. Pitts, Greg Restall, Tom Schrijvers, Alex Simpson, Sam Staton, Tina Šfiligoj, Armin Walch, Robert Wright, Nick Wu, Jeremy D. Yallop, and Nejc Zajc.

The second author used Anthropic's Claude models to obtain feedback on the prose and to proofread drafts for errors.

Copyright addendum. For the purpose of open access, the authors have applied a Creative Commons attribution (CC BY) licence to any Author Accepted Manuscript version arising.

References

[1] Andreas Abel, Guillaume Allais, Aliya Hameer, Brigitte Pientka, Alberto Momigliano, Steven Schäfer, and Kathrin Stark. 2019. POPLMark reloaded: Mechanizing proofs by logical relations. *Journal of Functional Programming* 29 (2019), e19. https://doi.org/10.1017/S0956796819000170

[2] Guillaume Allais, Robert Atkey, James Chapman, Conor McBride, and James McKinna. 2021. A type- and scope-safe universe of syntaxes with binding: their semantics and proofs. *Journal of Functional Programming* 31 (2021). https://doi.org/10.1017/S0956796820000076

[3] Thorsten Altenkirch and Bernhard Reus. 1999. Monadic Presentations of Lambda Terms Using Generalized Inductive Types. In *Computer Science Logic, 13th International Workshop, CSL '99, 8th Annual Conference of the EACSL, Madrid, Spain, September 20-25, 1999, Proceedings (Lecture Notes in Computer Science, Vol. 1683)*, Jörg Flum and Mario Rodríguez-Artalejo (Eds.). Springer, 453–468. https://doi.org/10.1007/3-540-48168-0_32

[4] Robert Atkey. 2014. From parametricity to conservation laws, via Noether's theorem. In *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, Suresh Jagannathan and Peter Sewell (Eds.). ACM, 491–502. https://doi.org/10.1145/2535838.2535867

[5] Brian Aydemir, Aaron Bohannon, and Stephanie Weirich. 2007. Nominal Reasoning Techniques in Coq (Extended Abstract). *Electronic Notes in Theoretical Computer Science* 174, 5 (2007), 69–77. https://doi.org/10.1016/j.entcs.2007.01.028 Proceedings of the First International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP 2006).

[6] Brian Aydemir, Arthur Charguéraud, Benjamin C. Pierce, Randy Pollack, and Stephanie Weirich. 2008. Engineering formal metatheory. In *Proceedings of the 35th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (San Francisco, California, USA) *(POPL '08)*. Association for Computing Machinery, New York, NY, USA, 3–15. https://doi.org/10.1145/1328438.1328443

[7] Brian E. Aydemir, Aaron Bohannon, Matthew Fairbairn, J. Nathan Foster, Benjamin C. Pierce, Peter Sewell, Dimitrios Vytiniotis, Geoffrey Washburn, Stephanie Weirich, and Steve Zdancewic. 2005. Mechanized Metatheory for the Masses: The PoplMark Challenge. In *Theorem Proving in Higher Order Logics*, Joe Hurd and Tom Melham (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 50–65.

[8] Ramzan Basheer and Deepak Mishra. 2025. Symmetry group equivariant convolutions for representation learning: a survey. *International Journal of Data Science and Analytics* 22 (12 2025). https://doi.org/10.1007/s41060-025-00994-7

[9] Andrej Bauer. 2008. Efficient computation with Dedekind reals. (2008). https://math.andrej.com/wp-content/uploads/2008/08/abstract-cca2008.pdf Fifth International Conference on Computability and Complexity in Analysis (CCA 2008).

[10] Andrej Bauer and Paul Taylor. 2009. The Dedekind Reals in Abstract Stone Duality. *Mathematical Structures in Computer Science* 19 (2009), 757–838. https://doi.org/10.1017/S0960129509007695

[11] Jon Beck. 1969. Distributive laws. In *Seminar on Triples and Categorical Homology Theory*, B. Eckmann (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 119–140.

[12] Nick Benton, Chung-Kil Hur, Andrew J. Kennedy, and Conor McBride. 2012. Strongly Typed Term Representations in Coq. *J. Autom. Reason.* 49, 2 (Aug. 2012), 141–159. https://doi.org/10.1007/s10817-011-9219-0

[13] Richard Bird and Ross Paterson. 1999. Generalised folds for nested datatypes. *Form. Asp. Comput.* 11, 2 (Sept. 1999), 200–222. https://doi.org/10.1007/s001650050047

[14] Jasmin Christian Blanchette, Lorenzo Gheri, Andrei Popescu, and Dmitriy Traytel. 2019. Bindings as bounded natural functors. *Proc. ACM Program. Lang.* 3, POPL, Article 22 (Jan. 2019), 34 pages. https://doi.org/10.1145/3290335

[15] Mikolaj Bojanczyk, Bartek Klin, and Slawomir Lasota. 2011. Automata with Group Actions. In *2011 IEEE 26th Annual Symposium on Logic in Computer Science*. 355–364. https://doi.org/10.1109/LICS.2011.48

[16] Dragan Bošnački, Dennis Dams, and Leszek Holenderski. 2002. Symmetric Spin. *International Journal on Software Tools for Technology Transfer* 4, 1 (01 Oct 2002), 92–106. https://doi.org/10.1007/s100090200074

[17] Pietro Cenciarelli and Eugenio Moggi. 1993. A syntactic approach to modularity in denotational semantics. *Proc. 5th CTCS, CWI Technical report* (1993).

[18] Arthur Charguéraud. 2012. The locally nameless representation. *Journal of automated reasoning* 49 (2012), 363–408.

[19] James Cheney. 2004. *Nominal Logic Programming*. Ph. D. Dissertation. Cornell University, USA.

[20] James Cheney. 2005. Toward a general theory of names: binding and scope. In *Proceedings of the 3rd ACM SIGPLAN Workshop on Mechanized Reasoning about Languages with Variable Binding* (Tallinn, Estonia) *(MERLIN '05)*. Association for Computing Machinery, New York, NY, USA, 33–40. https://doi.org/10.1145/1088454.1088459

[21] Adam Chlipala. 2008. Parametric higher-order abstract syntax for mechanized semantics. In *Proceedings of the 13th ACM SIGPLAN International Conference on Functional Programming* (Victoria, BC, Canada) *(ICFP '08)*. Association for Computing Machinery, New York, NY, USA, 143–156. https://doi.org/10.1145/1411204.1411226

[22] Duc-Hiep Chu and Joxan Jaffar. 2012. A Complete Method for Symmetry Reduction in Safety Verification. In *Computer Aided Verification*, P. Madhusudan and Sanjit A. Seshia (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 616–633.

[23] Edmund M Clarke, Thomas A Henzinger, Helmut Veith, Roderick Bloem, et al. 2018. *Handbook of model checking*. Vol. 10. Springer.

[24] Edmund M. Clarke and Somesh Jha. 1995. *Symmetry and induction in model checking*. Springer Berlin Heidelberg, Berlin, Heidelberg, 455–470. https://doi.org/10.1007/BFb0015260

[25] Ernesto Copello, Nora Szasz, and Álvaro Tasistro. 2021. Formalization of metatheory of the Lambda Calculus in constructive type theory using the Barendregt variable convention. *Mathematical Structures in Computer Science* 31, 3 (2021), 341–360. https://doi.org/10.1017/S0960129521000335

[26] Rob Cornish. 2025. Stochastic Neural Network Symmetrisation in Markov Categories. arXiv:2406.11814 [stat.ML] https://arxiv.org/abs/2406.11814

[27] Edsger W. Dijkstra. 1997. WLOG, or the misery of the unordered pair (EWD1223). In *Mathematical Methods in Program Development*, Manfred Broy and Birgit Schieder (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 33–34.

[28] Alastair F. Donaldson. 2007. *Automatic techniques for detecting and exploiting symmetry in model checking*. Ph. D. Dissertation. University of Glasgow, UK. http://theses.gla.ac.uk/1336/

[29] Gilles Dowek, Murdoch J. Gabbay, and Dominic P. Mulligan. 2010. Permissive nominal terms and their unification: an infinite, co-infinite approach to nominal techniques. *Logic Journal of the IGPL* 18, 6 (12 2010), 769–822. https://doi.org/10.1093/jigpal/jzq006 arXiv:https://academic.oup.com/jigpal/article-pdf/18/6/769/17505709/jzq006.pdf

[30] Gergo Érdi. 2018. Generic Description of Well-Scoped, Well-Typed Syntaxes. arXiv:1804.00119 [cs.PL] https://arxiv.org/abs/1804.00119

[31] Martín Hötzel Escardó. 1998. Effective and sequential definition by cases on the reals via infinite signed-digit numerals. *Electronic Notes in Theoretical Computer Science* 13 (1998), 53–68. https://doi.org/10.1016/S1571-0661(05)80214-2 Comprox III, Third Workshop on Computation and Approximation.

[32] Marcelo Fiore and Matías Menni. 2005. Reflective Kleisli subcategories of the category of Eilenberg-Moore algebras for factorization monads. *Theory and Applications of Categories [electronic only]* 15 (2005), 40–65. http://eudml.org/doc/125160

[33] Marcelo Fiore and Dmitrij Szamozvancev. 2022. Formal metatheory of second-order abstract syntax. *Proc. ACM Program. Lang.* 6, POPL, Article 53 (Jan. 2022), 29 pages. https://doi.org/10.1145/3498715

[34] Marcelo Fiore and Dmitrij Szamozvancev. 2025. Familial Model of Second-Order Abstract Syntax. (2025). unpublished.

[35] Marcelo P. Fiore, Gordon D. Plotkin, and Daniele Turi. 1999. Abstract Syntax and Variable Binding. In *14th Annual IEEE Symposium on Logic in Computer Science, Trento, Italy, July 2-5, 1999*. IEEE Computer Society, 193–202. https://doi.org/10.1109/LICS.1999.782615

[36] Marcelo P. Fiore and Sanjiv Ranchod. 2025. Substructural Abstract Syntax with Variable Binding and Single-Variable Substitution. In *2025 40th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. 196–208. https://doi.org/10.1109/LICS65433.2025.00022

[37] Yannick Forster and Kathrin Stark. 2020. Coq à la Carte — A Practical Approach to Modular Syntax with Binders. In *9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, USA*. ACM.

[38] Murdoch J. Gabbay and Andrew M. Pitts. 2002. A New Approach to Abstract Syntax with Variable Binding. *Formal Aspects Comput.* 13, 3-5 (2002), 341–363. https://doi.org/10.1007/S001650200016

[39] Andrew Gacek. 2009. *A Framework for Specifying, Prototyping, and Reasoning about Computational Systems.* Ph. D. Dissertation. University of Minnesota.

[40] Andrew Gacek, Dale Miller, and Gopalan Nadathur. 2012. A two-level logic approach to reasoning about computations. *Journal of Automated Reasoning* 49, 2 (2012), 241–273.

[41] Ian P. Gent, Karen E. Petrie, and Jean-François Puget. 2006. Symmetry in Constraint Programming. In *Handbook of Constraint Programming*, Francesca Rossi, Peter van Beek, and Toby Walsh (Eds.). Foundations of Artificial Intelligence, Vol. 2. Elsevier, 329–376. https://doi.org/10.1016/S1574-6526(06)80014-3

[42] Neil Ghani, Makoto Hamana, Tarmo Uustalu, and Varmo Vene. 2006. Representing Cyclic Structures as Nested Datatypes. (April 2006), 173–188.

[43] Georges Gonthier and Assia Mahboubi. 2010. An introduction to small scale reflection in Coq. *Journal of Formalized Reasoning* 3, 2 (Jan. 2010), 95–152. https://doi.org/10.6092/issn.1972-5787/1979

[44] Makoto Hamana. 2009. Initial Algebra Semantics for Cyclic Sharing Structures. In *Typed Lambda Calculi and Applications*, Pierre-Louis Curien (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 127–141.

[45] John Harrison. 2009. Without Loss of Generality. In *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings (Lecture Notes in Computer Science, Vol. 5674)*, Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel (Eds.). Springer, 43–59. https://doi.org/10.1007/978-3-642-03359-9_3

[46] Martin Hofmann. 1999. Semantical analysis of higher-order abstract syntax. In *Proceedings. 14th Symposium on Logic in Computer Science (Cat. No. PR00158)*. 204–213. https://doi.org/10.1109/LICS.1999.782616

[47] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. 2005. Handbook of Computational Group Theory. https://api.semanticscholar.org/CorpusID:116937731

[48] Mikoláš Janota, Markus Kirchweger, Tomáš Peitl, and Stefan Szeider. 2025. Breaking Symmetries in Quantified Graph Search: A Comparative Study. arXiv:2502.15078 [cs.LO] https://arxiv.org/abs/2502.15078

[49] Somesh Jha. 1996. *Symmetry and Induction in Model Checking.* Ph. D. Dissertation. Carnegie Mellon University.

[50] Edgar Kaucher. 1980. *Interval Analysis in the Extended Interval Space IR.* Springer Vienna, Vienna, 33–49. https://doi.org/10.1007/978-3-7091-8577-3_3

[51] Steven Keuchel. 2011. Generic Programming With Binders and Scope.

[52] Steven Keuchel and Johan T. Jeuring. 2012. Generic conversions of abstract syntax representations. In *Proceedings of the 8th ACM SIGPLAN Workshop on Generic Programming* (Copenhagen, Denmark) *(WGP '12)*. Association for Computing Machinery, New York, NY, USA, 57–68. https://doi.org/10.1145/2364394.2364403

[53] Steven Keuchel, Stephanie Weirich, and Tom Schrijvers. 2016. Needle & Knot: Binder Boilerplate Tied Up. In *Proceedings of the 25th European Symposium on Programming Languages and Systems - Volume 9632*. Springer-Verlag, Berlin, Heidelberg, 419–445. https://doi.org/10.1007/978-3-662-49498-1_17

[54] Gyesik Lee, Bruno C. D. S. Oliveira, Sungkeun Cho, and Kwangkeun Yi. 2012. GMeta: A Generic Formal Metatheory Framework for First-Order Representations. In *Programming Languages and Systems*, Helmut Seidl (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 436–455.

[55] Michael Leuschel, Michael Butler, Corinna Spermann, and Edd Turner. 2006. Symmetry Reduction for B by Permutation Flooding. In *B 2007: Formal Specification and Development in B*, Jacques Julliand and Olga Kouchnarenko (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 79–93.

[56] Anton Lorenzen, Daan Leijen, Wouter Swierstra, and Sam Lindley. 2025. First-Order Laziness. *Proc. ACM Program. Lang.* 9, ICFP (2025), 734–762. https://doi.org/10.1145/3747530

[57] Saunders Mac Lane. 1978. *Categories for the Working Mathematician* (2nd ed.). Springer New York, NY. https://doi.org/10.1007/978-1-4757-4721-8

[58] Conor Thomas McBride. 2014. How to keep your neighbours in order. In *Proceedings of the 19th ACM SIGPLAN International Conference on Functional Programming* (Gothenburg, Sweden) *(ICFP '14)*. Association for Computing Machinery, New York, NY, USA, 297–309. https://doi.org/10.1145/2628136.2628163

[59] Brendan D. McKay and Adolfo Piperno. 2014. Practical graph isomorphism, II. *Journal of Symbolic Computation* 60 (2014), 94–112. https://doi.org/10.1016/j.jsc.2013.09.003

[60] Vaibhav Mehta and Justin Hsu. 2025. A Hoare Logic for Symmetry Properties. *Proc. ACM Program. Lang.* 9, OOPSLA2, Article 302 (Oct. 2025), 25 pages. https://doi.org/10.1145/3763080

[61] Alice Miller, Alastair Donaldson, and Muffy Calder. 2006. Symmetry in temporal logic model checking. *ACM Comput. Surv.* 38, 3 (Sept. 2006), 8–es. https://doi.org/10.1145/1132960.1132962

[62] Peter Morris, Thorsten Altenkirch, and Conor McBride. 2006. Exploring the Regular Tree Types. In *Types for Proofs and Programs*, Jean-Christophe Filliâtre, Christine Paulin-Mohring, and Benjamin Werner (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 252–267.

[63] Michael Norrish. 2004. Recursive Function Definition for Types with Binders. In *Theorem Proving in Higher Order Logics*, Konrad Slind, Annette Bunker, and Ganesh Gopalakrishnan (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 241–256.

[64] F. Pfenning and C. Elliott. 1988. Higher-order abstract syntax. In *Proceedings of the ACM SIGPLAN 1988 Conference on Programming Language Design and Implementation* (Atlanta, Georgia, USA) *(PLDI '88)*. Association for Computing Machinery, New York, NY, USA, 199–208. https://doi.org/10.1145/53990.54010

[65] Brigitte Pientka. 2010. Beluga: Programming with Dependent Types, Contextual Data, and Contexts. In *Functional and Logic Programming*, Matthias Blume, Naoki Kobayashi, and Germán Vidal (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–12.

[66] Andrew M. Pitts. 2003. Nominal logic, a first order theory of names and binding. *Inf. Comput.* 186, 2 (2003), 165–193. https://doi.org/10.1016/S0890-5401(03)00138-X

[67] Andrew M. Pitts. 2006. Alpha-structural recursion and induction. *J. ACM* 53, 3 (May 2006), 459–506. https://doi.org/10.1145/1147954.1147961

[68] Andrew M. Pitts. 2013. *Nominal Sets: Names and Symmetry in Computer Science.* Cambridge University Press.

[69] Andrew M. Pitts. 2016. Nominal techniques. *ACM SIGLOG News* 3, 1 (2016), 57–72. https://doi.org/10.1145/2893582.2893594

[70] Andrew M. Pitts, Justus Matthiesen, and Jasper Derikx. 2015. A Dependent Type Theory with Abstractable Names. *Electronic Notes in Theoretical Computer Science* 312 (2015), 19–50. https://doi.org/10.1016/j.entcs.2015.04.003 Ninth Workshop on Logical and Semantic Frameworks, with Applications (LSFA 2014).

[71] G. D. Plotkin. 1973. *Lambda Definability and Logical Relations.* Memorandum SAI-RM-4. University of Edinburgh. https://homepages.inf.ed.ac.uk/gdp/publications/logical_relations_1973.pdf

[72] Emmanuel Polonowski. 2013. Automatically Generated Infrastructure for De Bruijn Syntaxes. In *Interactive Theorem Proving*, Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 402–417.

[73] Andrei Popescu. 2024. Nominal Recursors as Epi-Recursors. *Proc. ACM Program. Lang.* 8, POPL, Article 15 (Jan. 2024), 32 pages. https://doi.org/10.1145/3632857

[74] Andrei Popescu and Elsa L. Gunter. 2011. Recursion principles for syntax with bindings and substitution. In *Proceedings of the 16th ACM SIGPLAN International Conference on Functional Programming* (Tokyo, Japan) *(ICFP '11)*. Association for Computing Machinery, New York, NY, USA, 346–358. https://doi.org/10.1145/2034773.2034819

[75] Casper Bach Poulsen, Arjen Rouvoet, Andrew Tolmach, Robbert Krebbers, and Eelco Visser. 2018. Intrinsically-Typed Definitional Interpreters for Imperative Languages. *Proceedings of the ACM on Programming Languages* 2, POPL (10 Jan. 2018), 1–34. https://doi.org/10.1145/3158104

[76] John C. Reynolds. 1983. Types, Abstraction and Parametric Polymorphism. In *Information Processing 83, Proceedings of the IFIP 9th World Computer Congress, Paris, France, September 19-23, 1983*, R. E. A. Mason (Ed.). North-Holland/IFIP, 513–523.

[77] Steven Schäfer, Gert Smolka, and Tobias Tebbi. 2015. Completeness and Decidability of de Bruijn Substitution Algebra in Coq. In *Proceedings of the 2015 Conference on Certified Programs and Proofs, CPP 2015, Mumbai, India, January 15-17, 2015.* ACM, 67–73.

[78] Richard Schmoetten, Jake E. Palmer, and Jacques D. Fleuriot. 2021. Formalising Geometric Axioms for Minkowski Spacetime and Without-Loss-of-Generality Theorems. In *Proceedings of the 13th International Conference on Automated Deduction in Geometry, ADG 2021, Hagenberg, Austria/virtual, September 15-17, 2021 (EPTCS, Vol. 352)*, Predrag Janicic and Zoltán Kovács (Eds.). 116–128. https://doi.org/10.4204/EPTCS.352.13

[79] Richard Schmoetten, Jake E. Palmer, and Jacques D. Fleuriot. 2022. Towards Formalising Schutz' Axioms for Minkowski Spacetime in Isabelle/HOL. *J. Autom. Reason.* 66, 4 (2022), 953–988. https://doi.org/10.1007/S10817-022-09643-1

[80] John W Schutz. 1997. *Independent axioms for Minkowski space-time.* Vol. 373. CRC Press.

[81] Ákos Seress. 2003. *Permutation Group Algorithms.* Cambridge University Press.

[82] Peter Sewell, Francesco Zappa Nardelli, Scott Owens, Gilles Peskine, Thomas Ridge, Susmit Sarkar, and Rok Strniša. 2010. Ott: Effective tool support for the working semanticist. *Journal of Functional Programming* 20, 1 (2010), 71–122. https://doi.org/10.1017/S0956796809990293

[83] A. Prasad Sistla and Patrice Godefroid. 2004. Symmetry and reduced symmetry in model checking. *ACM Trans. Program. Lang. Syst.* 26, 4 (July 2004), 702–734. https://doi.org/10.1145/1011508.1011511

[84] Kathrin Stark. 2020. *Mechanising Syntax with Binders in Coq.* Ph. D. Dissertation. Saarland University.

[85] Kathrin Stark, Steven Schäfer, and Jonas Kaiser. 2019. Autosubst 2: Reasoning with Multi-Sorted de Bruijn Terms and Vector Substitutions. *8th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2019, Cascais, Portugal, January 14-15, 2019* (2019).

[86] Wouter Swierstra. 2008. Data types à la carte. *J. Funct. Program.* 18, 4 (2008), 423–436. https://doi.org/10.1017/S0956796808006758

[87] Dmitrij Szamozvancev. 2026. *Categorical models of second-order abstract syntax*. Ph. D. Dissertation. University of Cambridge.

[88] The mathlib Community. 2020. The Lean Mathematical Library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*. ACM, New Orleans, LA, USA. https://doi.org/10.1145/3372885.3373824

[89] Dominique Unruh. 2024. Without Loss of Generality. *Archive of Formal Proofs* (August 2024). https://isa-afp.org/entries/Wlog.html, Formal proof development.

[90] Christian Urban. 2008. Nominal Techniques in Isabelle/HOL. *J. Autom. Reason.* 40, 4 (2008), 327–356. https://doi.org/10.1007/S10817-008-9097-2

[91] Christian Urban and Stefan Berghofer. 2006. A Recursion Combinator for Nominal Datatypes Implemented in Isabelle/HOL. In *Automated Reasoning*, Ulrich Furbach and Natarajan Shankar (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 498–512.

[92] Philip Wadler. 1989. Theorems for Free!. In *Proceedings of the fourth international conference on Functional programming languages and computer architecture, FPCA 1989, London, UK, September 11-13, 1989*, Joseph E. Stoy (Ed.). ACM, 347–359. https://doi.org/10.1145/99370.99404

[93] Thomas Wahl. 2007. Adaptive Symmetry Reduction. In *Computer Aided Verification*, Werner Damm and Holger Hermanns (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 393–405.

[94] Thomas Wahl and Vijay Victor D'Silva. 2010. A lazy approach to symmetry reduction. *Formal Aspects Comput.* 22, 6 (2010), 713–733. https://doi.org/10.1007/S00165-009-0131-X

[95] Toby Walsh. 2012. Symmetry Breaking Constraints: Recent Results. In *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, July 22-26, 2012, Toronto, Ontario, Canada*, Jörg Hoffmann and Bart Selman (Eds.). AAAI Press, 2192–2198. https://doi.org/10.1609/AAAI.V26I1.8437

[96] Stephanie Weirich, Brent A. Yorgey, and Tim Sheard. 2011. Binders unbound. *SIGPLAN Not.* 46, 9 (Sept. 2011), 333–345. https://doi.org/10.1145/2034574.2034818

[97] Wikipedia contributors. 2026. Without loss of generality — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Without_loss_of_generality&oldid=1336885984 [Online; accessed 8-March-2026].

[98] Bo Zhao, Robin Walters, and Rose Yu. 2025. Symmetry in Neural Network Parameter Spaces. arXiv:2506.13018 [cs.LG] https://arxiv.org/abs/2506.13018

Supplementary material

We proceed as follows:

- Appendix A presents the theory of symmetric indexed data types, as it follows almost identical structure to its simply-typed counterpart.
- Appendix B contains further details about the simply-typed w.l.o.g. construction (§2).
- Appendix C contains further details about the dependently-typed w.l.o.g. construction (§3).
- Appendix D contains further details and proofs about symmetric simply typed data types (§4.1–§4.4). This material is a special case of its dependently-typed counterparts. Much of it can also be done more abstractly and categorically. Here we prove much of it more concretely and with fewer abstractions to help make the material more accessible.
- Appendix E contains further details and proofs about symmetric dependently typed data types (§4.5 and Appendix A). Here we give concrete descriptions of additional auxiliary results, and omitted details from concrete examples.
- Appendix F contains a more abstract category theoretic development that unifies parts of both theories of data types (cf. summary figure in §4.5).

A Indexed algebraic data types

In §4.5 we summarised the changes to the simply-typed development of symmetric data types. In this appendix, we spell the theory out in full detail, for completeness.

To extend the theory to indexed data types $\underline{\Gamma} \vdash \mathsf{D}$, we use endofunctors $F_{\mathsf{D}} : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\Gamma}$ over the category $\mathbf{Fam}_{\underline{\Gamma}}$ of families indexed by a set $\underline{\Gamma}$ and vertical maps between them. The data type D denotes an initial F_{D}-algebra $\underline{\Gamma} \vdash \mathbf{roll} : F_{\mathsf{D}}\mathsf{D} \to \mathsf{D}$. As in the non-indexed case, we equip those endofunctors with a symmetry strength relative to an ambient G-action $\Gamma = \langle \underline{\Gamma}, (\circledast) \rangle$ on the set of indices. This strength will be a certain natural transformation $\mathbf{st} : G \circledast F_{\mathsf{D}}X \to F_{\mathsf{D}}(G \circledast X)$, where $(G \circledast -)$ is the functor part of the *free* Γ*-indexed* G*-action* monad. Initial algebras for such endofunctors enjoy an indexed version of the parameterised initiality and representation theorems, and stating and establishing those is our main goal.

We'll use the indexed family $t : \mathsf{Tree} \vdash \mathsf{InPath}\, t$ as our running example, but unlike Example 3.2, we avoid the redundant cases through symmetric programming. As our endofunctor, we take:

$$(F_{\mathsf{InPath}}X)_{\mathsf{Leaf}} \coloneqq \emptyset \qquad (F_{\mathsf{InPath}}X)_{\mathsf{Node}\ \ell\, n\, r} \coloneqq \mathsf{Nil} \mid \mathsf{L} :: X_\ell \mid \mathsf{R} :: X_r$$
$$(F\,f)_u\mathsf{Nil} \coloneqq \mathsf{Nil} \qquad (F\,f)_u(\mathsf{L} :: x) \coloneqq \mathsf{L} :: f_\ell x \qquad (F\,f)_u(\mathsf{R} :: y) \coloneqq \mathsf{R} :: f_r y$$
$$(\text{where: } t : \mathsf{Tree} \vdash f : X \to Y,\ u = \mathsf{Node}\ \ell\, n\, r)$$

The initial algebra has as carrier $t : \mathsf{Tree} \vdash \mathsf{InPath}\, t$ from Example 3.1.

We denote the multiplication of the free Γ-indexed G-action monad P by:

$$(\boxtimes) : G \circledast (G \circledast X) \to G \circledast X \qquad \left\langle g, \left\langle h, x : X_{h^{-1} \circledast g^{-1} \circledast \gamma} \right\rangle \right\rangle \coloneqq \left\langle g * h, x : X_{(g*h)^{-1} \circledast \gamma} \right\rangle$$

It is the functor $(G \circledast)$ that generalises the notion of strength to the indexed setting:

Definition A.1. Let Γ be a G-action and $F : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$ be an endofunctor. A Γ*-indexed* G*-symmetry strength* is a natural transformation $\mathbf{st} : G \circledast FX \to F(G \circledast X)$, satisfying:

$$\mathbf{st}_\gamma(e, u) = F(x \mapsto \langle e, x \rangle)u \qquad F(\boxtimes) \circ \mathbf{st}(g, \mathbf{st}(h, x)) = \mathbf{st}(g * h, x)$$

Example A.2. We define an $\mathbf{S}_2$-symmetry strength for $t : \mathsf{Tree} \vdash \mathsf{InPath}\, t$. Only the F case is interesting, as the first strength axiom forces the definition for $\mathtt{I}$:

$$\mathtt{st}^{\mathsf{InPath}}\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)\left\langle \mathsf{F}, \mathsf{Nil} : \mathsf{InPath}\begin{array}{ccc} & n & \\ \mathsf{F} \circledast r & & \mathsf{F} \circledast \ell \end{array}\right\rangle \coloneqq \mathsf{Nil} : \mathsf{InPath}\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)$$

$$\mathtt{st}^{\mathsf{InPath}}\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)\langle \mathsf{F}, \mathsf{L} :: (x : X_{\mathsf{F}\circledast r})\rangle \coloneqq \mathsf{R} :: \langle \mathsf{F}, x : X_{\mathsf{F}\circledast r}\rangle \in (F_{\mathsf{InPath}}(G \circledast X))\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)$$

$$\mathtt{st}^{\mathsf{InPath}}\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)\langle \mathsf{F}, \mathsf{R} :: (x : X_{\mathsf{F}\circledast \ell})\rangle \coloneqq \mathsf{L} :: \langle \mathsf{F}, x : X_{\mathsf{F}\circledast \ell}\rangle \in (F_{\mathsf{InPath}}(G \circledast X))\left(\begin{array}{ccc} & n & \\ \ell & & r \end{array}\right)$$

To prove the second strength axiom, only the case $g \coloneqq h \coloneqq \mathsf{F}$ is interesting though straightforward:

$$\begin{aligned} F(\boxplus) \circ \mathbf{st}(\mathsf{F}, \mathbf{st}(\mathsf{F}, \mathsf{Nil})) &= F(\boxplus) \circ \mathbf{st}(\mathsf{F}, \mathsf{Nil}) = F(\boxplus)\mathsf{Nil} = \mathsf{Nil} \\ &= \mathtt{st}(\mathsf{F} * \mathsf{F}, \mathsf{Nil}) \\ F(\boxplus) \circ \mathbf{st}(\mathsf{F}, \mathbf{st}(\mathsf{F}, \mathsf{L} :: x)) &= F(\boxplus) \circ \mathbf{st}(\mathsf{F}, \mathsf{R} :: \langle \mathsf{F}, x\rangle) \\ &= F(\boxplus)(\mathsf{L} :: \langle \mathsf{F} * \mathsf{F}, x\rangle) = \mathsf{L} :: \langle \mathtt{I}, x\rangle = \mathbf{st}(\mathsf{F} * \mathsf{F}, \mathsf{L} :: x) \end{aligned}$$

and symmetrically for $\mathsf{R} :: x$. We cannot avoid this symmetric argument using wlog as we are setting up the symmetric action by defining the strength. Later uses of wlog will exploit this work. □

The appropriate category-theoretic concept that abstracts this notion of strength is a *monad-functor distributive law*, and we will use this perspective in our category theoretic development in Appendix F. As may be clear, when $\mathbb{1} \vdash X$ is a single-fibred family, $\mathbb{1} \vdash G \boxplus X$ is the single-fibred family $\underline{G} \times X$, subsuming the simply-typed case.

The following lemma justifies checking only the interesting cases, as we did in Example A.2:

Lemma A.3. *Let* $\mathbf{st}$ *be the structure of an indexed* G*-symmetric strength, satisfying the first axiom. Then the second axiom holds when either* $g = e$ *or* $h = e$*.*

Our main initiality theorem uses an indexed notion of equivariant algebras (cf. Definition 4.6):

Definition A.4. Let Γ be a G-action, $F : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$ an endofunctor equipped with a symmetry strength. For every indexed action A, the *lifted action* is given by:

$$\underline{F_{\mathbf{st}} A} \coloneqq \underline{FA} \qquad g \circledast_\gamma u \coloneqq F(\circledast)\, \mathbf{st}_{g\circledast\gamma}\, \langle g, t\rangle$$

An *equivariant* F*-algebra* $\langle A, f\rangle$ for an endofunctor equipped with a symmetry strength, consists of an indexed action A equipped with an equivariant algebra structure $\Gamma \vdash f : F_{\mathbf{st}} A \mathbin{\circledast\!\!\longrightarrow} A$. An equivariant F-algebra homomorphism is then a family map between the carrier families of two such algebras that is simultaneously equivariant and F-algebra homomorphic.

We generalise the Equivariant Initiality Theorem 4.8 to indexed families:

Theorem A.5 (indexed equivariant initiality)**.** *Let* $\mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ *be an initial algebra for a functor* F *over* Γ*-indexed families with a* G*-symmetry strength* $\mathbf{st} : G \boxplus FX \to F(G \boxplus X)$*. There is a unique map* $(\circledast) : G \boxplus \boldsymbol{\mu}F \to \boldsymbol{\mu}F$ *satisfying* $g \circledast (\mathbf{roll}\, u) = \mathbf{roll}(F(\circledast)(\mathbf{st}(g, u)))$*. It makes* $\langle \boldsymbol{\mu}f, \mathbf{roll}\rangle$ *into an initial equivariant* F*-algebra: for every equivariant* F*-algebra* $\langle A, f : F_{\mathbf{st}} A \mathbin{\circledast\!\!\longrightarrow} A\rangle$*, the* F*-homomorphism into* $\underline{A}$ *is equivariant:* $\mathbf{fold}\, f : \boldsymbol{\mu}F \mathbin{\circledast\!\!\longrightarrow} A$*.*

Like its simply-typed variant, the proof of this theorem uses an appropriate notion of parameterised initiality originally proposed by Bird and Paterson [13].

Example A.6. The action induced by the Indexed Equivariant Initiality Theorem A.5 satisfies:

$$\begin{aligned}\mathsf{F} \circledast (\mathsf{L} :: \mathsf{R} :: \mathsf{Nil}) &= \mathbf{roll} \circ F(\circledast)\, \mathbf{st}(\mathsf{F}, \mathsf{L} :: (\mathsf{R} :: \mathsf{Nil})) = \mathbf{roll} \circ F(\circledast)(\mathsf{R} :: \langle \mathsf{F}, \mathsf{R} :: \mathsf{Nil}\rangle) \\ &= \mathsf{R} :: (\mathsf{F} \circledast (\mathsf{R} :: \mathsf{Nil})) = \mathsf{R} :: \mathsf{L} :: (\mathsf{F} \circledast \mathsf{Nil}) = \mathsf{R} :: \mathsf{L} :: \mathsf{Nil}\end{aligned}$$

as we may expect from the example at the beginning of §3.2. □

Example A.7. Let's implement the dependently-typed node lookup function and simultaneously show its equivariance $\mathsf{lookup} : (t : \mathsf{Tree}) \times \mathsf{InPath}\, t \circledast\!\!\longrightarrow \mathbb{N}$. We'll construct an indexed equivariant map $t : \mathsf{Tree} \vdash \mathsf{lookup}_t : \mathsf{InPath}\, t \circledast\!\!\longrightarrow \mathbb{N}$. By the Indexed Equivariant Initiality Theorem A.5, it suffices to equip $\mathbb{N}$ with an equivariant F_{InPath}-algebra structure $\mathsf{lookup}^{\mathrm{Elim}} : F_{\mathsf{InPath}}\mathbb{N} \circledast\!\!\longrightarrow \mathbb{N}$. Informally, w.l.o.g., the path to the node is either empty or starts with the Left subtree, eliminating one symmetric case. Formally, define a canoniser by $c\mathsf{Nil} := c(\mathsf{L} :: n) := \mathtt{I}$ and $c(\mathsf{R} :: n) := \mathsf{F}$. Its canonical elements are Nil and $\mathsf{L} :: n$. This canoniser is equivariant, but not strictly:

$$\begin{aligned}c(\mathsf{F} \circledast \mathsf{Nil}) = c\mathsf{Nil} = \mathtt{I} \overset{\mathsf{Nil}}{\sim} \mathsf{F} = \mathtt{I} * \mathsf{F}^{-1} = \mathsf{F} \circledast c\,\mathsf{Nil} \\ c(\mathsf{F} \circledast (\mathsf{L} :: n)) = c(\mathsf{R} :: n) = \mathsf{F} = \mathtt{I} * \mathsf{F}^{-1} = \mathsf{F} \circledast c(\mathsf{L} :: n)\end{aligned}$$

and symmetrically for $\mathsf{R} :: n$. Again, we cannot avoid this symmetry with wlog since we are setting up the symmetric argument.

Let's define the core function for the eliminator $t : \mathsf{Tree} \vdash \mathsf{lookup}^{\mathrm{Core}} : \mathsf{Can}\, c \to \mathbb{N}$:

$$\mathsf{lookup}^{\mathrm{Core}}_{(\mathsf{Node}\ \ell\, n\, r)}\, \mathsf{Nil} := n \qquad \mathsf{lookup}^{\mathrm{Core}}_{(\mathsf{Node}\ \ell\, n\, r)}(\mathsf{L} :: p) := p$$

and we do not need to consider the symmetric case. The stabiliser subgroup for $\mathbb{N}$ is the whole of $\mathbf{S}_2$ since its action is trivial. Consequently, every core function is stable, and we don't need to work out the stabilisers for canonical elements. For completeness, here they are. The stabiliser subgroup for Nil is the whole of $\mathbf{S}_2$, and the stabiliser subgroup for $\mathsf{L} :: p$ is the trivial subgroup $\{\mathtt{I}\}$.

We use the Indexed Representation Theorem 3.12 to show the extended function is equivariant: $\mathsf{lookup}^{\mathrm{Elim}} := \mathsf{wlog}(c, f) : F_{\mathsf{InPath}}\mathbb{N} \circledast\!\!\longrightarrow \mathbb{N}$. □

As in the simply-typed case (cf. §4.3), we reuse the same canoniser for multiple traversals of the same symmetric indexed data type, and streamline the steps in Example A.7.

Definition A.8. Let Γ be a G-action, and F be a Γ-indexed G-strong. An *indexed canoniser* for F is a natural transformation $\underline{\Gamma} \vdash c : F \to \underline{G}$. Each such canoniser induces the *canonical elements* functor $\mathsf{Can}\, c : G\text{-}\mathbf{Act}_\Gamma \to \mathbf{Fam}_{\underline{\Gamma}}$ given by:

$$((\mathsf{Can}\, c)A)_\gamma := (\mathsf{Can}_{FA}\, c_{\underline{A}})_\gamma := \left\{ g \circledast^{FA}_{\delta} u \;\middle|\; \begin{array}{l} g = c_{\underline{A};\delta} u, g \circledast \delta = \gamma, \\ u \in (\underline{FA})_\delta \end{array} \right\} \qquad (\mathsf{Can}\, c)h : u \mapsto (\underline{Fh})u$$

An indexed canoniser is uniquely determined by its component at the terminal family $\underline{\Gamma} \vdash \mathbb{1}$.

Example A.9. The indexed $\mathbf{S}_2$-strong functor F_{InPath} has the canoniser (cf.Example 4.11)

$$\mathsf{goLeft}_{\mathsf{Node}\, n\, \ell\, r}\, \mathsf{Nil} := \mathtt{I} =: \mathsf{goLeft}_{\mathsf{Node}\, \ell\, n\, r}(\mathsf{L} :: p) \quad \mathsf{goLeft}_{\mathsf{Node}\, \ell\, n\, r}(\mathsf{R} :: p) := \mathsf{F}$$

The canonical elements are:

$$(\mathsf{Can}_A\, \mathsf{goLeft})_{\mathsf{Leaf}} := \emptyset \qquad (\mathsf{Can}_A\, \mathsf{goLeft})_{\mathsf{Node}\, \ell\, n\, r} := \left\{ \mathsf{Nil}, \mathsf{L} :: a \;\middle|\; a \in \underline{A}_{\mathsf{Node}\, \ell\, n\, r} \right\}$$ □

Continuing in tandem with the development of §4.5, we define the data we use to traverse an indexed symmetric data type:

Definition A.10. Let F be a Γ-indexed G-strong functor and $c : \underline{F} \to \underline{G}$ a canoniser for it. An *indexed c-core F-algebra* $\langle A, f\rangle$ consists of a Γ-indexed G-action A equipped with a vertical map $\underline{\Gamma} \vdash f : (\mathsf{Can}\ c)A \to \underline{A}$. It is *equivariant* when f is equivariant $\Gamma \vdash f : ((\mathsf{Can}\ c)A \subseteq FA) \circledast\!\!\longrightarrow A$. A *homomorphism* of equivariant indexed c-core F-algebras $h : \langle A, f\rangle \to \langle B, g\rangle$ is an equivariant map $\Gamma \vdash h : A \circledast\!\!\longrightarrow B$ satisfying: $h(f\,u) = g\,((\mathsf{Can}\ c)h\,u)$.

Example A.11. We have the following equivariant goLeft-core F_{InPath}-algebra:

$$\mathsf{lookup}^{\mathrm{Core}} : (\mathsf{Can}\ \mathsf{goLeft})(\mathsf{Triv}\mathbb{N}) \to \underline{\mathsf{Triv}\mathbb{N}} = \mathbb{N}$$
$$\mathsf{lookup}^{\mathrm{Core}}_{\mathsf{Node}\,\ell\,n\,r}\mathsf{Nil} := n \qquad \mathsf{lookup}^{\mathrm{Core}}_{\mathsf{Node}\,\ell\,n\,r}(\mathsf{L} :: (k \in \mathbb{N})) := k$$ □

Next, chain together the traversal and w.l.o.g. constructions:

$$\underline{\Gamma} \vdash \left(\mathsf{Can}_{FA}\ c_{\underline{A}} = (\mathsf{Can}\ c)A \xrightarrow{f} \underline{A}\right) \mapsto \left(F\underline{A} \xrightarrow{\mathsf{wlog}(c_{\underline{A}}, f)} \underline{A}\right) \mapsto \left(\mathbf{flog}_A(c, f) : \boldsymbol{\mu}\underline{F} \xrightarrow{\mathbf{fold}\ \mathsf{wlog}(c_{\underline{A}}, f)} \underline{A}\right)$$

And similarly chain Theorem 3.12 and the Indexed Equivariant Initiality Theorem A.5:

Theorem A.12 (indexed core initiality)**.** *Let F be a Γ-indexed G-strong functor, $\underline{\Gamma} \vdash \mathbf{roll} : \underline{F\boldsymbol{\mu}\underline{F}} \to \boldsymbol{\mu}\underline{F}$ an initial algebra of $\underline{F}$, and c a canoniser for F. Then restricting* **roll** *to canonical elements makes $\boldsymbol{\mu}F$ into the initial indexed c-core F-algebra* $\mathbf{roll} : (\mathsf{Can}\ c)\boldsymbol{\mu}F \circledast\!\!\longrightarrow \boldsymbol{\mu}F$*: for any equivariant indexed c-core F-algebra $f : (\mathsf{Can}\ c)A \circledast\!\!\longrightarrow A$, the unique equivariant indexed c-core F-algebra homomorphism into f is:* $\mathbf{flog}(c, f) : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$.

This theorem implies, by Example A.11, that we have an equivariant function:

$$t : \mathsf{Tree} \vdash \mathsf{lookup} := \mathbf{flog}(\mathsf{goLeft}, \mathsf{lookup}^{\mathrm{Core}}) : \mathsf{InPath}\ t \circledast\!\!\longrightarrow \mathsf{Triv}\mathbb{N}$$

B Simply-typed w.l.o.g.: further details

In this Appendix, we provide further details to §2. Our first proof obligation is a comment we immediately before Example 2.4:

Lemma B.1 (well-known)**.** *Let A and B be G-actions. The exponential $A \to B$ in G-***Act** *is given by the set of functions between their carriers:*

$$\underline{A \to B} := \underline{A} \to \underline{B} \qquad (g \circledast^{A\to B} f) := a \mapsto g \circledast^{B} f(g^{-1} \circledast^{A} a)$$
$$\mathrm{eval} : (A \to B) \times A \circledast\!\!\longrightarrow B \qquad \mathrm{eval}\,\langle f, a\rangle := f\,a$$

Proof
We indeed have an action. Unit preservation:

$$(\overset{G}{e} \circledast^{A\to B} f)a = \overset{G}{e} \circledast^{B} f(\overset{G}{e}{}^{-1} \circledast a) = f\,a \implies \overset{G}{e} \circledast^{A\to B} f = f$$

Action preservation:

$$(g \circledast^{A\to B} h \circledast^{A\to B} f)a = g \circledast^{B} (h \circledast^{A\to B} f)(g^{-1} \circledast^{A} a) = g \circledast^{B} (h \circledast^{B} f(h^{-1} \circledast^{A} (g^{-1} \circledast^{A} a)))$$
$$= (g \overset{G}{*} h) \circledast^{B} f\left((g \overset{G}{*} h)^{-1} \circledast^{A} a\right) = \left((g \overset{G}{*} h) \circledast^{A\to B} f\right) a$$
$$\implies (g \circledast^{A\to B} h \circledast^{A\to B} f) = (g \overset{G}{*} h) \circledast^{A\to B} f$$

Evaluation is equivariant. Calculate:

$$\mathrm{eval}(g \circledast^{(A\to B)\times A} \langle f, a\rangle) = \mathrm{eval}\left\langle g \circledast^{A\to B} f, g \circledast^{A} a\right\rangle = (g \circledast^{A\to B} f)\,(g \circledast^{A} a)$$
$$= g \circledast^{B} (f(g^{-1} \circledast^{A} (g \circledast^{A} a))) = g \circledast^{B} (f\,a) = g \circledast^{B} \mathrm{eval}\,\langle f, a\rangle$$

Given any equivariant map $h : C \times A \circledast\!\!\longrightarrow B$, its curried map is also equivariant:

$$(g \circledast^{A \Rightarrow B} \text{curry } hc)a = g \circledast^{B} \text{curry } h(c; g^{-1} \circledast^{A} a) = g \circledast^{B} h(c, g^{-1} \circledast^{A} a) \overset{\text{equivariance}}{\downarrow} = h(g \circledast^{C} c, g \circledast g^{-1} \circledast^{A} a)$$
$$= h(g \circledast^{C} c, a) = (\text{curry } h(g \circledast^{C} c))a$$
$$\implies \quad g \circledast^{A \to B} \text{curry } hc = \text{curry } h(g \circledast^{C} c)$$

and so curry $h : C \circledast\!\!\longrightarrow (A \to B)$. The curried function lifts h along evaluation. Now if we have an equivariant map $g : C \circledast\!\!\longrightarrow (A \to B)$ that lifts h along evaluation, then by the set-theoretic argument, it coincides with curry h. ■

Next, we characterise the canonical elements of canonisers of the form $\underline{A} \times \underline{B} \xrightarrow{\pi_1} A \xrightarrow{c} \underline{G}$:

Proof of Lemma 2.8

Take an arbitrary canonical element $(c \circ \pi_1)\langle a, b\rangle \circledast \langle a, b\rangle \in \mathsf{Can}\,(c \circ \pi_1)$. We then have

$$(c \circ \pi_1)\langle a, b\rangle \circledast \langle a, b\rangle = ca \circledast \langle a, b\rangle = \langle ca \circledast a, ca \circledast b\rangle \in \mathsf{Can}\, c \times \underline{B}$$

Conversely, given an arbitrary pair $\langle ca \circledast a, b\rangle \in \mathsf{Can}\, c \times \underline{B}$, let $b' = (ca)^{-1} \circledast b$. We then have:

$$\langle ca \circledast a, b\rangle = \left\langle ca \circledast a, (ca * (ca)^{-1}) \circledast b\right\rangle = ca \circledast \langle a, b'\rangle = ((c \circ \pi_1)\langle a, b'\rangle) \circledast \langle a, b'\rangle \in \mathsf{Can}\,(c \circ \pi_1)$$

Therefore $\mathsf{Can}\,(c \circ \pi_1) = \mathsf{Can}\, c \times \underline{B}$. ■

Next, we proof the main equivariance theorem for the w.l.o.g. construction:

Proof of Theorem 2.13

Let us first show that $\mathsf{wlog}(c, f)$ is equivariant. Take arbitrary $g \in \underline{G}$ and $a \in \underline{A}$. By definition and by the group and action axioms, we can rewrite:

$$\begin{aligned}\mathsf{wlog}(c, f)(g \circledast a) &= c(g \circledast a)^{-1} \circledast f(c(g \circledast a) \circledast (g \circledast a)) \\ &= c(g \circledast a)^{-1} \circledast f(c(g \circledast a) \circledast (g \circledast (ca)^{-1} \circledast ca \circledast a)) \\ &= c(g \circledast a)^{-1} \circledast f\big((c(g \circledast a) * g * (ca)^{-1}) \circledast (ca \circledast a)\big)\end{aligned}$$

Since both $ca \circledast a$ and $c(g \circledast a) \circledast (g \circledast a)$ belong to $\mathsf{Can}\, c$, equivariance of f allows us to rewrite:

$$\begin{aligned}&= c(g \circledast a)^{-1} \circledast \big((c(g \circledast a) * g * (ca)^{-1}\big) \circledast f(ca \circledast a)) \\ &= g \circledast ((ca)^{-1} \circledast f(ca \circledast a)) \\ &= g \circledast \mathsf{wlog}(c, f)\, a\end{aligned}$$

as desired.

Next, let us show that $\mathsf{wlog}(c, f)$ extends f. Take an arbitrary canonical element $a \in \mathsf{Can}\, c$. Since $ca \circledast a$ also lies in $\in \mathsf{Can}\, c$, the action axioms imply:

$$\mathsf{wlog}(c, f)\, a = (ca)^{-1} \circledast f(ca \circledast a) \overset{f \text{ is equivariant}}{\downarrow} = (ca)^{-1} \circledast ca \circledast fa = fa$$

Finally, take an arbitrary $\varphi : A \circledast\!\!\longrightarrow B$ that extends f along $\mathsf{Can}\, c \subseteq \underline{A}$. Then, for an arbitrary $a \in \underline{A}$, we have

$$\varphi a = \varphi((ca)^{-1} \circledast ca \circledast a) \overset{\varphi \text{ equivariant}}{\downarrow} = (ca)^{-1} \circledast \varphi(ca \circledast a) \overset{\varphi \text{ extends } f}{\downarrow} = (ca)^{-1} \circledast f(ca \circledast a) \overset{\text{by definition}}{\downarrow} = \mathsf{wlog}(c, f)\, a$$

as desired. ■

The order of the next few results differs from the order in which they appear in the main text. They concern the characterisation of strictly equivariant and immediate canonisers from §2.2. Strict equivariance seem to be a more natural concept to the audience when we present this work, so the main text starts there. Here we first characterise immediate canonisers, and use this characterisation as part of the proof. This order make it easier to see that we avoid circular reasoning.

We start with immediate canonisers as every strictly equivariant canoniser is also immediate:

Proof of Proposition 2.20

Calculate:

$$c(ca * a) \overset{\text{equivariance}}{=} ca * (ca)^{-1} = e$$

as desired. ∎

We characterise immediate canonisers via the condition $\mathsf{Can}\ c = c^{-1}[e]$:

Proof of Proposition 2.22

Take an arbitrary $ca \circledast a \in \mathsf{Can}\ c$. Since c is immediate, we have $c\ (ca \circledast a) = e$, and so $ca \circledast a \in c^{-1}[e]$, thus $\mathsf{Can}\ c \subseteq c^{-1}[e]$. The converse inclusion always holds. Indeed, if $a \in c^{-1}[e]$, then $ca = e$ and so $a = ca \circledast a \in \mathsf{Can}\ c$.

Conversely, let us show that c is immediate and take an arbitrary $a \in \underline{A}$. We have $ca \circledast a \in \mathsf{Can}\ c$ by definition, thus $ca \circledast a \in c^{-1}[e]$ by assumption, and so $c(ca \circledast a) = e$ as required. ∎

The next result characterises strict equivariance of a canoniser via the equivariance of every core function. The proof uses the concept of stabilisers that we introduce in §3.4. The proof is dependently-typed in nature, and it is best understood in the context of §3 and §3.4 in particular. However, we make the proof self-contained and re-introduce the concepts that are relevant for it.

Proof of Theorem 2.17

First, take a strictly equivariant canoniser $c : \underline{A} \to \underline{G}$, and let B be an arbitrary action. We need to show that every core function $f : \mathsf{Can}\ c \to \underline{B}$ is equivariant. Take $a, g \circledast a \in \mathsf{Can}\ c$. Since c is strictly equivariant, by Proposition 2.20, it is an immediate canoniser. So by Proposition 2.22, $ca = e = c(g \circledast a)$, therefore:

$$g^{-1} = ca * g^{-1} \overset{c \text{ strictly equivariant}}{=} c\ (g \circledast a) = e$$

and equivariance holds vacuously.

Conversely, assume that every core function is equivariant, and let us show that c is strictly equivariant. Recall that for every $a \in \underline{A}$, we define the stabiliser sub-group of a as the set of symmetries that fix a:

$$G_a \coloneqq \left\{ s \in \underline{G} \,\middle|\, s \circledast a = a \right\}$$

Take the following action over the the set of dependent pairs consisting of an element in $\underline{A}$ and one of its stabilising symmetries:

$$\underline{B} \coloneqq (a : \underline{A}) \times G_a \qquad g \circledast \langle a, s \rangle \coloneqq \left\langle g \circledast a, s * g^{-1} \right\rangle$$

Indeed, this definition is well-typed because:

$$(s * g^{-1}) * (g \circledast a) = s \circledast (g^{-1} * g) \circledast a = s \circledast a = a$$

It is also an action, since:

$$e \circledast \langle a, s \rangle = \left\langle e \circledast a, s \circledast e^{-1} \right\rangle = \langle a, s \rangle$$

$$g \circledast h \circledast \langle a, s \rangle = \left\langle g \circledast h \circledast a, s * h^{-1} * g^{-1} \right\rangle = \left\langle (g * h) \circledast a, s * (g * h)^{-1} \right\rangle = (g * h) \circledast \langle a, s \rangle$$

Define:

$$f : \mathsf{Can}\, c \to \underline{B} \qquad f\, a \coloneqq \langle a, e\rangle$$

By our assumption, its w.l.o.g. extension is equivariant: $\mathsf{wlog}(c, f) : A \circledast\!\!\longrightarrow B$. Note that this map is given by:

$$\mathsf{wlog}(f, c)a = (ca)^{-1} \circledast f\,(ca * a) = (ca)^{-1} \circledast \langle ca * a, e\rangle = \left\langle a, \left((ca)^{-1}\right)^{-1}\right\rangle = \langle a, ca\rangle$$

Now take any $a \in \underline{A}$ and $g \in \underline{G}$, and calculate:

$$\langle g \circledast a, c\,(g \circledast a)\rangle = \mathsf{wlog}(c, f)(g \circledast a) = g \circledast \mathsf{wlog}(c, f)a = g \circledast \langle a, ca\rangle = \left\langle g \circledast a, (ca) * g^{-1}\right\rangle$$

Comparing the two second components, we have $c\,(g \circledast a) = (ca) * g^{-1}$ and the canoniser is strictly equivariant. ■

The next result shows that actions that admit strictly equivariant canonisers must be semi-regular, which makes this condition too strong for some actions:

Proof of Lemma 2.18

Assume $g \circledast a = a$. By equivariance of the canoniser, we thus have $ca = c\,(g \circledast a) = ca * g^{-1}$ and by cancelling ca on the left, we get $e = g$. ■

The final result concerns inheriting strict equivariance and immediateness from a canoniser:

Proof of Lemma 2.21

To show strict equivariance, we have that the projection is an equivariant map $\pi_1 : A \times B \circledast\!\!\longrightarrow A$, and equivariant maps compose. For immediateness, we calculate

$$\begin{aligned} c \circ \pi_1\,((c \circ \pi_1\langle a, b\rangle) * \langle a, b\rangle) &= c \circ \pi_1\,(ca * \langle a, b\rangle) = c \circ \pi_1\,(\langle ca * a, ca * b\rangle) \\ &= c\,(ca * a) = e \end{aligned}$$

and so $c \circ \pi_1$ is immediate when c is. ■

C Dependent types: further details

We begin by establishing the correctness of the action over the Grothendieck construction $\coprod_{\underline{\Gamma}} A$, as we will use its properties pervasively, e.g., when extending contexts.

Proof of Proposition 3.7

Take a Γ-indexed action A and define an action on $\coprod_{\underline{\Gamma}} \underline{A}$ by:

$$g \circledast \left\langle \gamma : \underline{\Gamma}, a : \underline{A}_{\gamma}\right\rangle \coloneqq \left\langle g \circledast \gamma, g \circledast_{\gamma} a : \underline{B}(g \circledast \gamma)\right\rangle$$

Since $\pi_1(g \circledast \langle \gamma, a\rangle) = g \circledast \gamma = \pi_1\,\langle \gamma, a\rangle$, the projection is equivariant $\pi_1 : \coprod_{\Gamma} A \circledast\!\!\longrightarrow \Gamma$.

Conversely, given an action $\coprod_{\Gamma} A$ as in the assumption, define $g \circledast_{\gamma} a \coloneqq \pi_2(g \circledast \langle \gamma, a\rangle)$. This definition is a well-typed dependent function $\gamma : \Gamma \vdash (\circledast) : (g : \underline{G}) \to A\gamma \to A(g \circledast \gamma)$:

$$g \circledast_{\gamma} a \in A\,(\pi_1(g \circledast \langle \gamma, a\rangle)) = A\,(g \circledast \gamma)$$

It also satisfies the two conditions for an indexed action. The unit axiom:

$$e \circledast_{\gamma} a = \pi_2(e \circledast \langle \gamma, a\rangle) = \pi_2\,\langle \gamma, a\rangle = a$$

The multiplication axiom:

$$h \circledast_{g \circledast \gamma} (g \circledast_\gamma a) = \pi_2 (h \circledast \langle g \circledast \gamma, \pi_2 (g \circledast \langle \gamma, a \rangle) \rangle)$$

π_1 equivariant

$$\downarrow$$

$$= \pi_2 (h \circledast \langle \pi_1 (g \circledast \langle \gamma, a \rangle), \pi_2 (g \circledast \langle \gamma, a \rangle) \rangle)$$

extensionality of pairs

$$\downarrow$$

$$= \pi_2 (h \circledast (g \circledast \langle \gamma, a \rangle)) = \pi_2 ((h * g) \circledast \langle \gamma, a \rangle) = (h * g) \circledast_\gamma a$$

and so we have an indexed action. The two constructions are inverse to each other. ■

The following example lets us work more formally with concrete examples:

Example C.1. The Grothendieck construction extends equivariantly to equivariant terms and maps. It sends equivariant terms $\Gamma \vdash t : A$ to equivariant sections $(\gamma \mapsto \langle \gamma, t_\gamma \rangle) : \Gamma \circledast\!\!\longrightarrow \coprod_\Gamma A$. It sends a dependent equivariant function $\Gamma \vdash f : (x : A) \to B$ to the following equivariant map $(\langle \gamma, a \rangle \mapsto \langle \gamma, x \mapsto a, f_\gamma a \rangle) : \coprod_\Gamma A \circledast\!\!\longrightarrow \coprod_{\Gamma, x:A} B$. □

Next, we establish the indexed action axioms for the family of dependent functions, and the indexed equivariance of related operations.

Lemma C.2. *The indexed action structure over the family of dependent functions is an action, evaluation is equivariant, and currying and uncurrying preserve equivariance.*

Proof

Indeed, the action axioms hold by calculating with the correct indices as in the ordinary case. Similarly for evaluation:

$$\mathrm{eval}(g \circledast_\gamma f, x)_{g \circledast \gamma, x \mapsto g \circledast_\gamma a} = g \circledast f(g^{-1} \circledast g \circledast a) = g \circledast f a = g \circledast \mathrm{eval}(f, x)_{\gamma, x \mapsto a}$$

The bijective correspondence is given as in the set-theoretic case. If t is equivariant, then:

$$(x : A \mapsto t)_{g \circledast \gamma} a = g \circledast t_{g \circledast \gamma, x \mapsto a} = g \circledast t_{g \circledast \gamma, x \mapsto (g \circledast (g^{-1} \circledast a))}$$

equivariance

$$\downarrow$$

$$= g \circledast g \circledast t_{\gamma, x \mapsto (g^{-1} \circledast a)} = (g \circledast (x : A \mapsto t)_\gamma) a$$

Therefore $(x : A \mapsto t)_{g \circledast \gamma} = (g \circledast (x : A \mapsto t)_\gamma)$.

Conversely, if $(x : A) \mapsto t$ is equivariant, then since $\mathrm{eval}\,\langle -, x \rangle$ is equivariant, t is. ■

We now turn to prove the indexed counterpart to the w.l.o.g. Representation Theorem 2.13:

Proof of Theorem 3.12

We can prove this theorem directly, but it may be more interesting to reduce it to the ordinary representation theorem. Applying the Grothendieck construction to the situation, we have:

- G-actions $\coprod_\Gamma A$ and $\coprod_{\Gamma, x:A} B$;
- canoniser $c' \coloneqq \langle \gamma, a \rangle \mapsto c_\gamma a : \underline{\coprod_\Gamma A} \to \underline{G}$;
- below we show that $\mathsf{Can}\, c' = \{\langle \gamma, a \rangle \mid a \in \mathsf{Can}\, c, \gamma\} =: \coprod_\Gamma \mathsf{Can}\, c$;
- core function $f' \coloneqq (\langle \gamma, a \rangle \mapsto \langle (\gamma, x \mapsto a), f_\gamma a \rangle) : \mathsf{Can}\, c' \to \underline{\coprod_{\Gamma, x:A} B}$;
- we have that $\mathrm{wlog}(c', f'; \langle \gamma, a \rangle) = \langle (\gamma, x \mapsto a), \mathrm{wlog}(c, f)_\gamma a \rangle$;
- the core function f' is equivariant iff f is (by Example C.1);
- below we show that $\mathrm{wlog}(c', f')$ is equivariant iff $\mathrm{wlog}(c, f)$ is equivariant;
- below we show that the function term $\underline{\Gamma} \vdash g : (x : \underline{A}) \to \underline{B}$ extends f along $\Gamma \vdash \mathsf{Can}\, c \subseteq A$ iff the function $\langle \gamma, a \rangle \mapsto \langle (\gamma, x \mapsto a), g_\gamma a \rangle : \coprod_{\underline{\Gamma}} \underline{A} \to \coprod_{\underline{\Gamma}, x:\underline{A}} \underline{B}$ extends f' along $\mathsf{Can}\, c' \subseteq \coprod_{\underline{\Gamma}} \underline{A}$.

The theorem follows by unpacking and re-packing definitions in both directions. Let's discharge the outstanding proof obligations.

Let $\langle \gamma, a\rangle$ be canonical for c', so $\langle \gamma, a\rangle = (c_\gamma a') \circledast \langle \gamma', a'\rangle$. Then $\gamma' = (ca')^{-1} \circledast \gamma$ and $a' \in A_{(ca')^{-1}\circledast\gamma}$, so $a \in (\mathsf{Can}\, c)_\gamma$, and so $\langle \gamma, a\rangle \in \coprod_\Gamma \mathsf{Can}\, c$. These implications are invertible, proving the converse.

Next, we show that the Grothendieck construction preserves the w.l.o.g. extension:

$$\begin{aligned}
\mathsf{wlog}(c', f'; \langle \gamma, a\rangle) &= (c'\ \langle \gamma, a\rangle)^{-1} \circledast f'((c'\ \langle \gamma, a\rangle) \circledast \langle \gamma, a\rangle) \\
&= (c_\gamma a)^{-1} \circledast f'((c_\gamma a) \circledast \langle \gamma, a\rangle) \\
&= (c_\gamma a)^{-1} \circledast f' \left\langle (c_\gamma a) \circledast \gamma, (c_\gamma a) \circledast a \right\rangle \\
&= (c_\gamma a)^{-1} \circledast \left\langle ((c_\gamma a) \circledast \gamma, x{\mapsto}((c_\gamma a) \circledast a)), f_{(c_\gamma a)\circledast\gamma}(c_\gamma a) \circledast a \right\rangle \\
&= \left\langle (\gamma, x{\mapsto}a), (c_\gamma a)^{-1} \circledast f_{(c_\gamma a)\circledast\gamma}(c_\gamma a) \circledast a \right\rangle \\
&= \left\langle (\gamma, x{\mapsto}a), \mathsf{wlog}(c, f)_\gamma a \right\rangle
\end{aligned}$$

In addition, by Example C.1, one w.l.o.g. extension is equivariant iff the other is equivariant.

The final bullet point follows by functoriality of the Grothendieck construction. ∎

We now establish the bread-and-butter properties facilitating smooth dependently-typed symmetric programming and symmetric propositional reasoning. We start with dependent-function abstraction:

Lemma C.3 (abstraction)**.** *Function abstraction of an equivariant term* $\Gamma, x : A \vdash t : B$ *is both:*

- *an equivariant term* $\Gamma \vdash ((x : A) \mapsto t) : (x : A) \to B$.
- *an equivariant function* $\Gamma \vdash ((x : A) \mapsto t) : (x : A) \circledast\!\!\to B$.

Proof

Calculate, ignoring indices (as those type-check):

$$\begin{aligned}
(g \circledast (x : A \mapsto t))_\gamma\, a &\overset{\text{action on dep. functions}}{=} g \circledast ((x : A \mapsto t)(g^{-1} \circledast a)) \overset{\text{abstraction def}}{=} g \circledast t_{\gamma, x\mapsto(g^{-1}\circledast a)} \overset{t \text{ equivariant}}{=} t_{g\circledast\gamma, x\mapsto(g\circledast g^{-1}\circledast a)} \\
&= t_{g\circledast\gamma, x\mapsto a} = (x : A \mapsto t)_{g\circledast\gamma} a
\end{aligned}$$

showing abstraction is an equivariant term. It is also an equivariant function, for:

$$(x : A \mapsto t)_{g\circledast\gamma}(g \circledast a) \overset{\text{abstraction def}}{=} t_{g\circledast\gamma, x\mapsto g\circledast a} \overset{t \text{ equivariant}}{=} g \circledast t_{\gamma, x\mapsto a}$$

as we wanted. ∎

Substitution using an equivariant substitution preserves equivariance:

Lemma C.4 (reindexing and substitution)**.** *Reindexing by an equivariant function* $\theta : \Gamma \to \Delta$ *sends equivariant terms* $\Delta \vdash s : B$ *to equivariant terms* $\Gamma \vdash s\,[\theta] : B\,[\theta]$*, and moreover every equivariant term* $\Gamma \vdash t : B\,[\theta]$ *induces an equivariant substitution* $(\theta, y{\mapsto}t) : \Gamma \circledast\!\!\to (\Delta, y : B)$.

Proof

Calculate:

$$g \circledast s\,[\theta]_\gamma \overset{\text{reindexing def}}{=} g \circledast s_{\theta\gamma} \overset{s \text{ equivariant}}{=} s_{g\circledast\theta\gamma} \overset{\theta \text{ equivariant}}{=} s_{\theta(g\circledast\gamma)} = s\,[\theta]_{g\circledast\gamma}$$

and so $s\,[\theta]$ is equivariant. Next, calculate:

$$(\theta, y{\mapsto}t)(g \circledast \gamma) \overset{\text{substitution def}}{=} (\theta(g \circledast \gamma), y{\mapsto}t_{g\circledast\gamma}) \overset{t \text{ equivariant}}{=} (\theta(g \circledast \gamma), y{\mapsto}g \circledast t_\gamma) \overset{\text{action on context extension}}{=} g \circledast (\theta\gamma, y{\mapsto}t_\gamma)$$
$$= g \circledast ((\theta, y{\mapsto}t)\gamma)$$

and so $(\theta, y{\mapsto}t) : \Gamma \circledast{\longrightarrow} (\Delta, y : B)$. ■

Dependent pairing also preserves equivariant terms:

Lemma C.5 (dependent pairing). *Two equivariant terms $\Gamma \vdash t : A$ and $\Gamma \vdash s : B\,[x{\mapsto}t]$ induce an equivariant term $\Gamma \vdash t\,, s : (x : A) \times B$.*

Proof
Calculate:

$$(g \circledast (t\,, s))_\gamma = (g \circledast t_\gamma\,, g \circledast s_{\gamma, x{\mapsto}t_\gamma}) \overset{t,\, s \text{ equivariant}}{=} (t_{g\circledast\gamma}\,, s_{g\circledast\gamma, x{\mapsto}(g\circledast t_\gamma)})$$

as we wanted. ■

We now turn to propositions:

Lemma C.6 (subfamilies). *Each equivariant proposition $\Gamma, x : A \vdash \varphi : \mathsf{Prop}$ induces an indexed action on the subfamily $\Gamma \vdash \{x : A \mid \varphi\}$ that lifts A along the subset inclusions. Equivariant terms $\Gamma \vdash t : A$ satisfying φ lift to equivariant terms inhabiting the associated subspace i.e., $\Gamma \vdash \mathsf{lift}\, t : \{x : A \mid \varphi\}$.*

Proof
Equivariance means that if $a \in \underline{A}_\gamma$ satisfies φ, then so does $g \circledast a$. Therefore $g \circledast_\gamma a \in \{x : A \mid \varphi\}$, and the action lifts. For equivariance of the lifted term, use injectivity of the coercion function $\Gamma \vdash \mathsf{coerce} \coloneqq a \mapsto a : \{x : A \mid \varphi\} \circledast{\longrightarrow} A$:

$$\mathsf{coerce}_{g\circledast\gamma}(g \circledast (\mathsf{lift}\, t)_\gamma) \overset{\text{coerce equivariance}}{=} g \circledast \mathsf{coerce}_\gamma\, \mathsf{lift}\, t_\gamma \overset{\text{coercion}}{=} g \circledast t_\gamma \overset{t \text{ equivariant}}{=} t_{g\circledast\gamma} = \mathsf{coerce}_{g\circledast\gamma}(\mathsf{lift}\, t)_{g\circledast\gamma}$$

and so $g \circledast (\mathsf{lift}\, t)_\gamma = (\mathsf{lift}\, t)_{g\circledast\gamma}$. ■

We use these facts implicitly when conducting reasoning:

Lemma C.7. *The logical connectives are equivariant $(\wedge), (\vee) : \mathsf{Prop}^2 \circledast{\longrightarrow} \mathsf{Prop}$, $(\neg) : \mathsf{Prop} \circledast{\longrightarrow} \mathsf{Prop}$, as well as the quantifiers $\forall, \exists : (A \to \mathsf{Prop}) \circledast{\longrightarrow} \mathsf{Prop}$.*

Proof
The logical connectives operate between trivial actions hence equivariant. For the quantifiers, assume $\forall t = \mathsf{True}$, and so, for each $a \in \underline{A}_\gamma$, we have $t(g^{-1} \circledast a) = \mathsf{True}$, i.e.:

$$\forall(g \circledast t) = \forall x.t(g^{-1} \circledast x) = \mathsf{True}$$

Conversely, if $\forall(g \circledast t)$, then by instantiating with $g \circledast a$ we have that $ta = t(g^{-1} \circledast g \circledast a) = \mathsf{True}$. Therefore $\forall t = \forall g \circledast t$. A similar argument holds for $\exists$, or by use of de Morgan. ■

We conclude our treatment of propositions by explicating how symmetric reasoning w.l.o.g. often manifests—via a property invariant under the symmetry of interest:

Proof of Lemma 3.17
Take canonical a and $g \circledast_\gamma a$. By type-checking, $g \circledast f_\gamma a, f_\gamma(g \circledast a)$ prove the same proposition, namely $\varphi_{g\circledast\gamma, x{\mapsto}(g\circledast a)}$. Therefore, $g \circledast f_\gamma a = f_\gamma(g \circledast a)$. ■

In some concrete cases, working with the entire group of permutations incurs a combinatorial explosion. Group theorists often generate the group from a smaller set of symmetries, and then only work with those. As we briefly mentioned in the main text, a group G is *generated* by a subset $S \subseteq \underline{G}$ when G is the smallest subgroup of G containing S, equivalently, when every $\underline{G}$-element is the multiplication of $\underline{G}$-elements or their inverses. For example, the symmetry group $\mathbf{S}_3$ is generated by the two transpositions $(1\,2)$ and $(2\,3)$. We have an indexed variation of a well-known lemma:

Lemma C.8. *Let $\Gamma \vdash A$ and $\Gamma, x : A \vdash B$ be indexed G-actions. If S generates G and $\underline{\Gamma} \vdash f : \left(x : \underline{A}\right) \to \underline{B}$ is equivariant w.r.t. symmetries in S, then f is equivariant $\Gamma \vdash f : (x : A) \circledast\!\!\to B$. When $B = \mathsf{Prop}$ and $[S]^{-1} \subseteq S$, it suffices to show lax/oplax equivariance, i.e.:*

$$(\forall g \in S, \forall x. f(g \circledast x) \implies fx) \vee (\forall g \in S, \forall x. f(g \circledast x) \impliedby fx)$$

Proof of Lemma C.8
Let $H \subseteq \underline{G}$ be the set of symmetries that f respects. Then $S \subseteq H$. Since $f(e \circledast a) = fa = e \circledast (fa)$, we have: $e \in H$. Take $h \in H$ we have:

$$f(h \circledast a) = h \circledast (fa) \implies f(h^{-1} \circledast a) = h^{-1} \circledast f(h \circledast (h^{-1} \circledast a)) = h^{-1} \circledast (fa)$$

so $h^{-1} \in H$. Take $g, h \in H$ and then:

$$f((g * h) \circledast a) = f(g \circledast (h \circledast a)) = g \circledast (f(h \circledast a)) = g \circledast (h \circledast (fa)) = (g * h) \circledast (fa)$$

so $g * h \in H$. Thus $H \subseteq \underline{G}$ is a subgroup containing S, and so $H = \underline{G}$.

When $B = \mathsf{Prop}$ and $[S]^{-1} \subseteq S$, by substituting $x \mapsto g^{-1} \circledast a$ we have:

$$fx \iff f(g^{-1} \circledast (g \circledast x)) \overset{[S]^{-1} \subseteq S}{\implies} f(g \circledast x)$$

For the left disjunct, f is in fact equivariant for symmetries in S. Similarly for the right disjunct. ■

We now turn to study equivariant canonisers. It turns out that the indexed setting is fruitful for this purpose. We first show that the indexed action of *distinguishable symmetries* G/A from Definition 3.18 is well-defined:

Lemma C.9. *Let A be a G-action. The action over distinguishable symmetries G/A is congruent w.r.t. indistinguishability, hence is well-defined.*

Proof
Assume $s_1 \overset{a}{\sim} s_2$. Calculate:

$$(s_1 * g^{-1}) \circledast (g \circledast a) = s_1 \circledast a = s_2 \circledast a = (s_2 * g^{-1}) \circledast (g \circledast a)$$

and so $s_1 * g^{-1} \overset{g \circledast a}{\sim} s_2 * g^{-1}$, and the action is well-defined. ■

In §3.4 we mentioned in passing the stabiliser family alongside the indexed actions of the orbits and the indistinguishable symmetries. The stabilisers also form an indexed action:

Example C.10. The *stabiliser* family has all the symmetries fixing an index $a \in \underline{A}$ as the fibre over it: $a : \underline{A} \vdash G_a \coloneqq \left\{ s \in \underline{G} \,\middle|\, s \circledast a = a \right\}$. The stabiliser has an A-indexed action:

$$g \circledast_a s \coloneqq s * g^{-1} \in G_{g \circledast a} \quad \text{since} \quad s * g^{-1} \circledast (g \circledast a) = s \circledast a = a$$ □

We now prove our reformulation of the famous Orbit-Stabiliser Theorem 3.20:

Proof of Theorem 3.20

The bijectivity of φ is the well-known theorem. We show equivariance:

$$\begin{aligned}\varphi_{g \circledast x}(g \circledast_x [h]_{\underset{\sim}{x}}) &\overset{\text{action on } G/A}{=} \varphi_{g \circledast x}([h * g^{-1}]_{g \underset{\sim}{\circledast} x}) = (h * g^{-1}) \circledast (g \circledast x) = h \circledast x \overset{\text{action on } G \circledast [x]}{=} g \circledast_x (h \circledast x) \\ &= g \circledast_x \varphi_x [h]_{\underset{\sim}{x}}\end{aligned}$$

and we conclude as inverses of equivariant functions are equivariant. ∎

Next, we characterise equivariant canonisers as those for which stable and equivariant core functions coincide. First, an observation:

Lemma C.11. *Let $c : \underline{A} \to \underline{G}$ be an equivariant canoniser for a G-action A. For every canonical element $a \in \mathsf{Can}\, c$, we have $ca \overset{a}{\sim} e$.*

Proof

Since a is canonical, there is some $b \in \underline{A}$ such that $a = (cb) \circledast b$. Since c is equivariant, we have:

$$ca = c((cb) \circledast b) \overset{a}{\sim} (cb) * (cb)^{-1} = e \qquad \uparrow \text{ equivariance } (cb) \circledast b = a$$

as we wanted. ∎

Now, for the proof:

Proof Theorem 3.25

First, assume $c : (a : A) \circledast\!\!\longrightarrow (G/A)a$ is equivariant, and consider any stable core function $f : \mathsf{Can}\, c \to B$. We show that f is equivariant.

Consider any canonical $g \circledast a, a \in \mathsf{Can}\, c$. Since c is equivariant, by Lemma C.11, we have $ca \overset{a}{\sim} e$ and so $ca \in G_a$. By equivariance, we have:

$$g \circledast^{G/A} [ca]_{\underset{\sim}{a}} = [c(g \circledast a)]_{g \underset{\sim}{\circledast} a} \overset{\text{Lemma C.11 for } g \circledast a}{=} [e]_{g \underset{\sim}{\circledast} a} \implies [ca]_{\underset{\sim}{a}} = g^{-1} \circledast [e]_{g \underset{\sim}{\circledast} a} = [g]_{\underset{\sim}{a}}$$

and so $g \overset{a}{\sim} ca \in G_a$ and so $g \in G_a \subseteq G_{fa}$. Therefore:

$$f(g \circledast a) \overset{g \in G_a}{=} fa = g \circledast fa \qquad \uparrow g \in G_{fa}$$

and so f is equivariant.

Conversely, assume that every stable core function is equivariant. We need to show the canoniser is equivariant. The proof adapts the argument in Theorem 2.17. Since we now have the indexed action vocabulary, the proof simplifies somewhat.

Take the A-indexed action $B \coloneqq G/A$, and the following core function:

$$f : (x : \mathsf{Can}\, c) \to (G/A)x \qquad fa \coloneqq [e]_{\underset{\sim}{a}}$$

It is stable. Indeed, take any canonical $a \in \mathrm{Can}\, c$ and a stabilising symmetry $g \in G_a$. Since G_a is a sub-group, $g^{-1} \in G_a$, and so $[g^{-1}]_{\underline{a}} = [e]_{\underline{a}}$. Calculate:

$$g \circledast_a^{G/A} (fa) = g \circledast_a^{G/A} [e]_{\underline{a}} = \left[e * g^{-1}\right]_{g \circledast a} \overset{g \in G_a}{\underset{\downarrow}{=}} \left[g^{-1}\right]_{\underline{a}} = [e]_{\underline{a}} = fa$$

Therefore $g \in G_{fa}$, and so $G_a \subseteq G_{fa}$, and so f is stable.

By assumption, f is equivariant, and by the Indexed Representation Theorem 3.12 we have an equivariant $\mathrm{wlog}(c, f) : (x : A) \circledast\!\!\longrightarrow (G/A)x$. We will show that $\mathrm{wlog}(c, f) = \left(a \mapsto [ca]_{\underline{a}}\right)$ and therefore c is equivariant.

Take any $a \in \underline{A}$ and calculate:

$$\mathrm{wlog}(c, f)a = (ca)^{-1} \circledast f(ca \circledast a) = (ca)^{-1} \circledast [e]_{ca \circledast a} = \left[\left((ca)^{-1}\right)^{-1}\right]_{((ca)^{-1}) \circledast ca \circledast a} = [ca]_{\underline{a}}$$

Therefore $\mathrm{wlog}(c, f) = [ca]_{\underline{a}}$, as we wanted. ■

We conclude this section by proving that every action has an equivariant canoniser. Recall that a *transversal* of an action is a (dependent) function $t : (a : \underline{A}) \to G \circledast [a]$ that picks a representative for the orbit of its input: $ta = tb$ iff $G \circledast [a] = G \circledast [b]$.

Proof Theorem 3.26

Consider the family of orbits $x : A \vdash G \circledast [x]$, and use the axiom of choice to choose a transversal: $t : (x : A) \to G \circledast [x]$. For each $a \in \underline{A}$, the elements a and $t\, a \in G \circledast [a]$ are symmetric, and so there is some symmetry $g \in \underline{G}$ such that $g \circledast a = t\, a$. Use the axiom of choice to choose a canoniser $c : A \to \underline{G}$ such that $ca \circledast a = t\, a$. We will show this canoniser is equivariant.

Take any element $a \in \underline{A}$ and symmetry $g \in \underline{G}$. Then $g \circledast a$ and a are in the same orbit, and therefore $t(g \circledast a) = t\, a$. Calculate:

$$(c(g \circledast a) * g) \circledast a = c(g \circledast a) \circledast (g \circledast a) = t(g \circledast a) = t\, a = ca \circledast a$$

Therefore, $c(g \circledast a) * g \overset{a}{\sim} ca$, and so $[c(g \circledast a) * g]_{\underline{a}} = [ca]_{\underline{a}}$. Calculate:

$$[c(g \circledast a)]_{g \circledast a} = \left[c(g \circledast a) * g * g^{-1}\right]_{g \circledast a} = g \circledast [c(g \circledast a) * g]_{\underline{a}} = g \circledast [ca]_{\underline{a}}$$

and so c is equivariant. ■

D Algebraic data types: further details

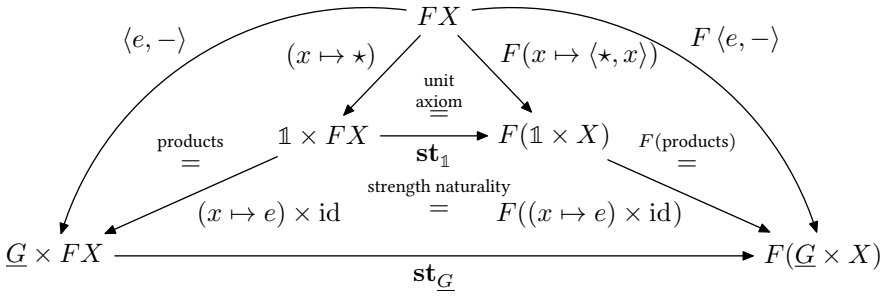
In some sense, the theoretical development in this section is a special case of the proceedings two sections. However, it requires some additional abstractions that make the material less accessible: indexed families (Appendix E), or monadic adjunctions and distributive laws (Appendix F). Therefore, we decided to include more specialised proofs for the simply-typed case, that use less categorical reasoning and mostly concern sets and functions.

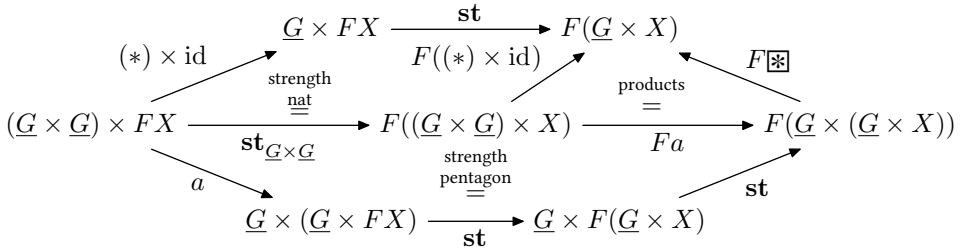
We start by proving that every Cartesian strength is a G-strength (cf. Remark 4.3).

Lemma D.1. *Let* $\mathbf{st} : X \times FY \to F(X \times Y)$ *be a Cartesian strength for a functor* $F : \mathbf{Set} \to \mathbf{Set}$. *Then* $\mathbf{st}_{\underline{G},X} : \underline{G} \times FX \to F(\underline{G} \times X)$ *is a* G*-strength.*

Proof

It's more natural to use diagrammatic reasoning here:





as we wanted. ∎

Next, we prove that a G-strength for F and an G-action A let us equip $F\underline{A}$ with a G-action:

Proof of Lemma 4.4

This definition is a G-action by straightforward calculation:

$$e \circledast t = F(\circledast)(\mathbf{st}(e, t)) \overset{\text{first axiom}}{=} F(\circledast)(F(x \mapsto \langle e, x \rangle)t) \overset{\text{map fusion}}{=} F(x \mapsto e \circledast x)t = F(x \mapsto e \circledast x)t = F(\mathrm{id})t = t$$

$$\begin{aligned}
g \circledast (h \circledast t) &= F(\circledast)(\mathbf{st}(g, F(\circledast)(\mathbf{st}(h, t)))) \\
&\overset{\text{strength nat.}}{=} F(\circledast)(F(\langle g', h', x \rangle \mapsto \langle g', h' \circledast x \rangle)(\mathbf{st}(g, (\mathbf{st}(h, t))))) \\
&\overset{\text{map fusion}}{=} F(\langle g', h', x \rangle \mapsto g' \circledast h' \circledast x)(\mathbf{st}(g, (\mathbf{st}(h, t)))) \\
&= F(\langle g', h', x \rangle \mapsto (g' * h') \circledast x)(\mathbf{st}(g, (\mathbf{st}(h, t)))) \\
&\overset{\text{map fusion}}{=} F(\circledast)(F(\langle g', h', x \rangle \mapsto \langle g' * h', x \rangle)(\mathbf{st}(g, (\mathbf{st}(h, t))))) \\
&\overset{\text{second axiom}}{=} F(\circledast)(\mathbf{st}(g * h, t)) =: (g * h) \circledast t
\end{aligned}$$

and so we have an action.

Let $h : A \circledast\!\!\longrightarrow B$ be equivariant. Calculate:

$$\begin{aligned} F\,h(g \circledast t) &= F\,h(F(\circledast)(\mathbf{st}(g,t))) \overset{\text{map fusion}}{=} F(\langle g', x\rangle \mapsto h(g' \circledast x))(\mathbf{st}(g,t)) \\ &= F(\langle g', x\rangle \mapsto g' \circledast h(x))(\mathbf{st}(g,t)) \overset{\text{map fusion}}{=} F(\circledast)\,F(\mathrm{id} \times h)(\mathbf{st}(g,t)) \\ &\overset{\text{strength nat.}}{=} F(\circledast)\,\mathbf{st}(g, F\,ht) = g \circledast F\,ht \end{aligned}$$

and so we have an equivariant map $F\,h : FA \circledast\!\!\longrightarrow FB$. ■

Next, we prove that G-strengths for each component functor induce a G-strength for the coproduct functor:

Proof Proposition 4.7

Follows by **Set**'s distributivity: the natural isomorphism $\underline{G} \times (X + Y) \cong (\underline{G} \times X) + (\underline{G} \times Y)$. ■

The following technical result is the workhorse that allows us to both derive the action on the data type from its strength, and to reason about properties of parameterised maps. It is prevalent in Fiore et al.'s work on abstract syntax [33, 34, 36], originally proposed by Bird and Paterson [13]. Here we use the following special case.

Theorem D.2 (parameterised initiality). *Let A be a set, $F : \mathbf{Set} \to \mathbf{Set}$ a functor, $\mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ an initial algebra, and $\mathbf{st} : A \times FX \to F(A \times X)$ a natural transformation in X. For every F-algebra $f : FX \to X$ there is a unique A-*parameterised *homomorphism $\mathbf{pfold}\ f : \langle \boldsymbol{\mu}F, \mathbf{roll}\rangle \to \langle X, f\rangle$, i.e., a function $\mathbf{pfold}\ f : A \times \boldsymbol{\mu}F \to X$ satisfying:*

$$\mathbf{pfold}\ f\ \langle a, \mathbf{roll}\ t\rangle = f(F(\mathbf{st}(a,t)))$$

Proof

Using both the given strength and the Cartesian-closed structure, define the following morphism:

$$\begin{array}{ccc} A \times F(X^A) & \xrightarrow{\ \mathbf{st}\ } & F(A \times X^A) \\ {\scriptstyle g}\downarrow & \coloneqq & \downarrow{\scriptstyle F\,\mathrm{eval}} \\ X & \xleftarrow[\ f\ ]{} & FX \end{array}$$

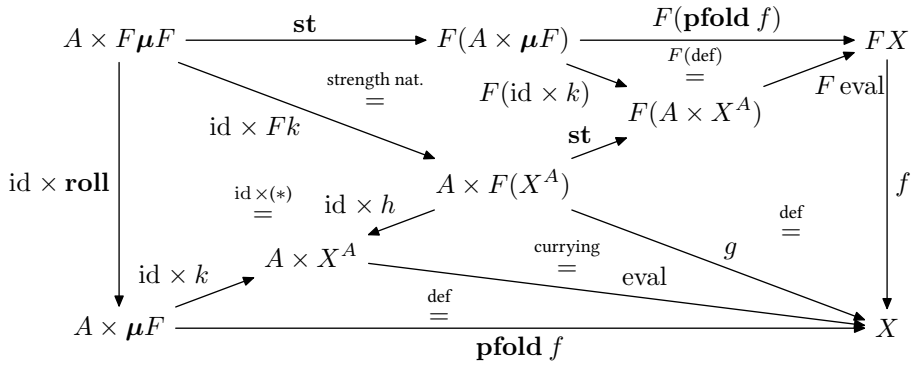
Currying, we have $h \coloneqq \mathrm{curry}\, g : F(X^A) \to X^A$, and so by ordinary initiality, there is a unique homomorphism into X^A:

$$\begin{array}{ccc} F\boldsymbol{\mu}F & \xrightarrow{\ Fk\ } & F(X^A) \\ {\scriptstyle \mathbf{roll}}\downarrow & \overset{(*)}{=} & \downarrow{\scriptstyle h} \\ \boldsymbol{\mu}F & \xrightarrow[\ k\ ]{} & X^A \end{array}$$

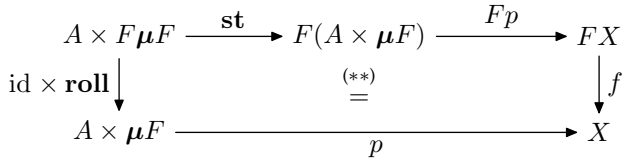
We define the required parameterised traversal as the uncurried function:

$$\mathbf{pfold}\ f \coloneqq \mathrm{uncurry}\ k : A \times \boldsymbol{\mu}F \xrightarrow{\mathrm{id}\times k} A \times X^A \xrightarrow{\mathrm{eval}} X$$

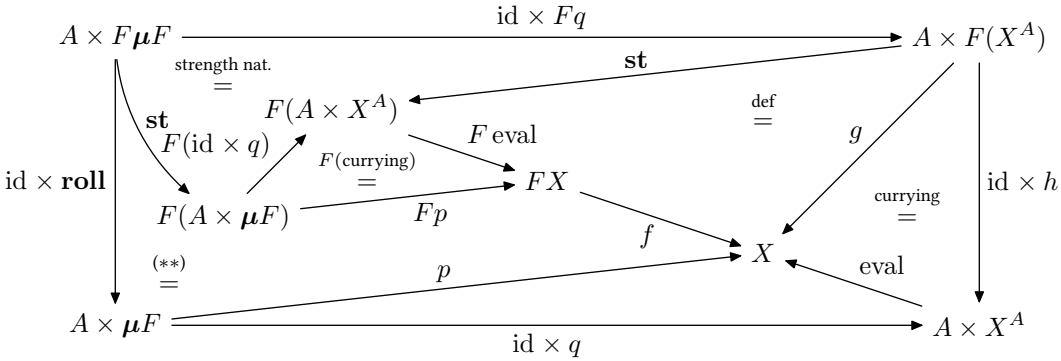
We need to show that it satisfies the required equation, and that it is the unique such function. Calculate:



Now, take any map $p : A \times \boldsymbol{\mu}F \to X$ that satisfies:



Let $q \coloneqq \mathrm{curry}\ p : \boldsymbol{\mu}F \to X^A$. Calculate:



and so, by the universal property of the exponential, q satisfies $(*)$, and so $q = k$, hence:

$$p = \mathrm{uncurry}\ q = \mathrm{uncurry}\ k = \mathbf{pfold}\ f$$

and we proved uniqueness. ■

We now lay the capstone in the theory of data types, the Equivariant Initiality Theorem 4.8:

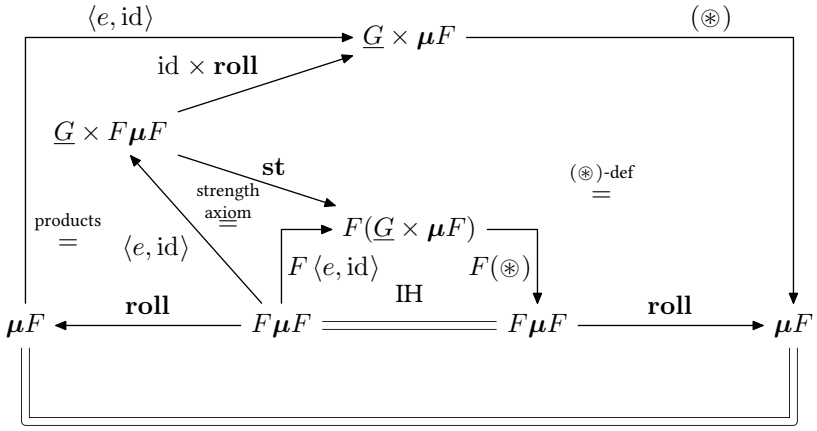
Proof of Theorem 4.8

We have three things to do:

- show the unit axiom for $(\circledast)$.
- show the associativity axiom for $(\circledast)$.
- show that $\mathbf{fold}\ f$ is equivariant when f is equivariant.

All three are straightforward calculations, appealing to initiality or parameterised initiality.

For the unit axiom, appeal to initiality:



and so, by initiality, $e \circledast t = t$.

For associativity, we appeal to parameterised initiality, for the composite strength:

$$\begin{array}{ccc} (\underline{G} \times \underline{G}) \times FX & \xrightarrow{a} & \underline{G} \times (\underline{G} \times X) \\ & & \downarrow \mathrm{id} \times \mathbf{st} \\ \mathbf{st}_2 \downarrow & \coloneqq & \underline{G} \times F(\underline{G} \times X) \\ & & \downarrow \mathbf{st} \\ F((\underline{G} \times \underline{G}) \times X) & \xleftarrow[Fa^{-1}]{} & F(\underline{G} \times (\underline{G} \times X)) \end{array}$$

via the calculation in Fig. 3. Therefore, $(g * h) \circledast t = g \circledast (h * t)$, and we have an action. Note that the defining property of $(\circledast)$ makes the initial algebra structure equivariant $\mathbf{roll} : F\boldsymbol{\mu}F \circledast\!\!\longrightarrow \boldsymbol{\mu}F$.

Finally, take any equivariant algebra $f : FA \circledast\!\!\longrightarrow A$, and consider the unique F-homomorphism $\mathbf{fold}\, f : \boldsymbol{\mu}F \to \underline{A}$. We appeal to parametrised initiality w.r.t. the G-strength, and calculate as in Fig. 4. Therefore $\mathbf{fold}\, f(g \circledast t) = g \circledast (\mathbf{fold}\, f)$, as we wanted. ■

The proofs from §4.3 are identical and special cases to their indexed variants, and do not use abstract categorical concepts. We therefore only prove them in the indexed case (cf. Appendix E).

E Indexed data types

The theory of indexed data types has a few more moving parts. So in this case we do most of our proofs more abstractly in Appendix F. In this appendix we establish the assumptions needed for that development, prove a result about canonisers, who do not feature in the abstract account, and state the indexed version of the Parameterised Initiality Theorem.

Proof Theorem 4.16

Let's start with the left adjoint. It is an action by direct calculation:

$$e \circledast_\gamma \langle g, x\rangle \coloneqq \langle e * g, x\rangle = \langle g, x\rangle \qquad g \circledast h \circledast \langle s, x\rangle \coloneqq \langle g * (h * s), x\rangle = \langle (g * h) * s, x\rangle = (g * h) \circledast \langle s, x\rangle$$

Given any Γ-indexed G-action A and a vertical map $h : X \to \underline{A}$, define:

$$h^\dagger : (g : G) \times g \circledast X \circledast\!\!\longrightarrow A \qquad h^\dagger_\gamma \langle g, x\rangle \coloneqq \left(g \circledast_{g^{-1} \circledast \gamma} x\right) \in X_\gamma$$

Indeed:

$$h^\dagger_{g \circledast \gamma}(g \circledast \langle s, x\rangle) = h^\dagger_{g \circledast \gamma}(\langle g * s, x\rangle) = (g * s) \circledast (hx) = g \circledast (s \circledast (hx)) = g \circledast h^\dagger_\gamma \langle s, x\rangle$$

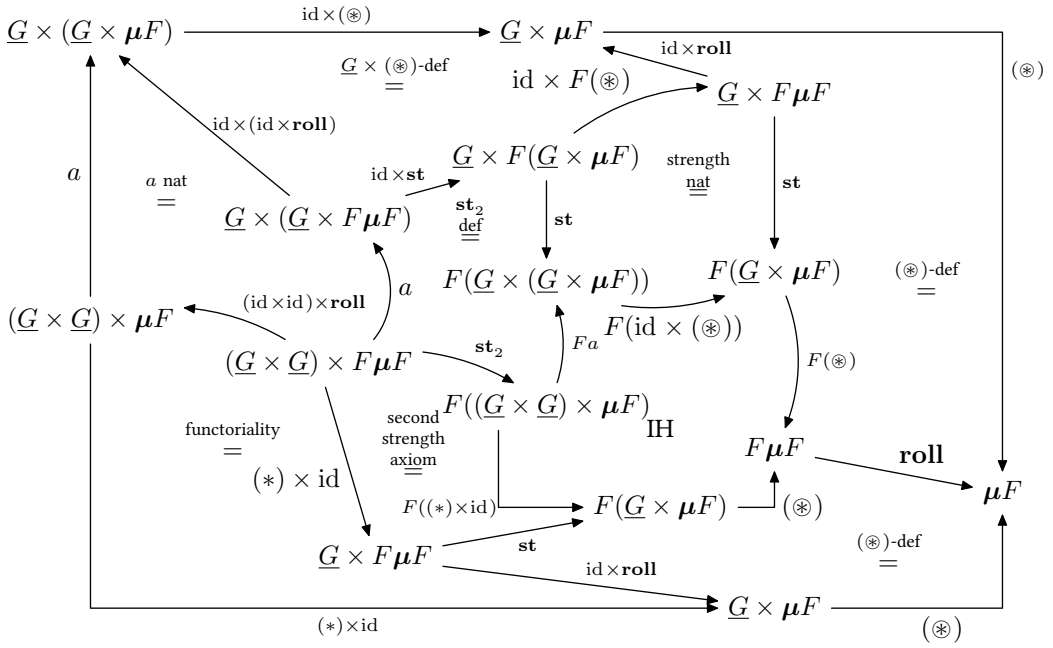


Fig. 3. associativity of the action over the initial algebra

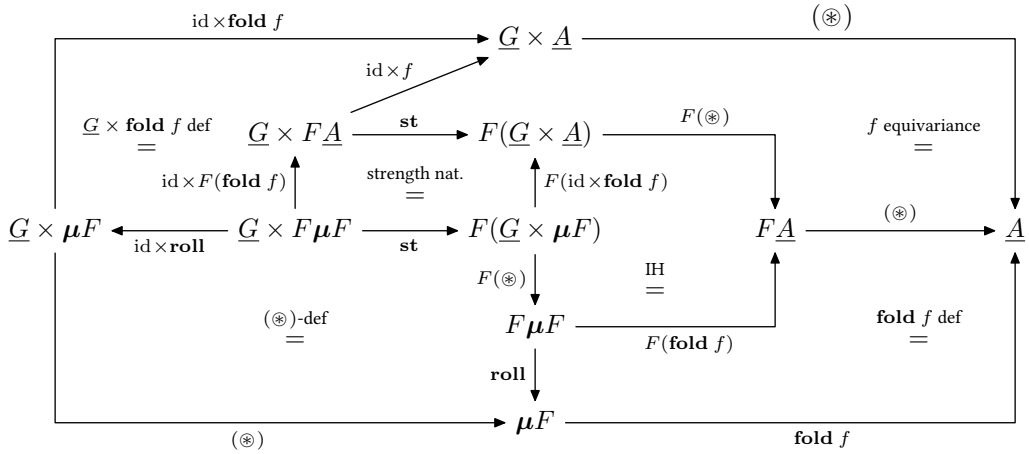


Fig. 4. equivariance of the homomorphism into an equivariant algebra

Now, $h^\dagger$ extends h along the unit, since:

$$h^\dagger \langle e, x \rangle = e \circledast hx = hx$$

If $\overline{h} : (g : G) \times g \circledast X \mathrel{\circledast\!\!\longrightarrow} A$ is any other such extension, we have:

$$\overline{h}_\gamma \langle g, x\rangle = \overline{h}_\gamma(g \circledast \langle e, x\rangle) \overset{\text{equivariance}}{=} g \circledast \overline{h}_{g^{-1}\circledast\gamma} \langle e, x\rangle \overset{\overline{h}\text{ extends the unit}}{=} g \circledast h_{g^{-1}\circledast\gamma} x = h^\dagger_\gamma \langle g, x\rangle$$

and so $\overline{h} = h^\dagger$, as we wanted.

The monadicity result follows by an application of Beck's monadicity theorem [57, Thm. VI.7.1]. Start with a split coequalier diagram, in which A and B are Γ-indexed actions, and $f, g : A \mathrel{\circledast\!\!\longrightarrow} B$ are equivariant:

$$\begin{array}{ccccc} \underline{B} & \xrightarrow[t]{} & \underline{A} & \xrightarrow[g]{} & \underline{B} \\ {\scriptstyle q}\downarrow & = & \downarrow{\scriptstyle f} & = & \downarrow{\scriptstyle q} \\ \underline{C} & \xrightarrow[s]{} & \underline{B} & \xrightarrow[q]{} & \underline{C} \end{array}$$

First, equip $\underline{C}$ with an indexed action: $h \circledast_\gamma c \coloneqq q_{g\circledast\gamma}(h \circledast_\gamma s_\gamma c)$. Indeed: $e \circledast_\gamma c = q(e \circledast_\gamma sc) = q(sc) = c$ and:

$$h \circledast k \circledast c = q(h \circledast s(q(k \circledast sc))) = q(h \circledast (k \circledast_\gamma sc)) = q((h * k) \circledast sc) = (h * k) \circledast c$$

The coequaliser $\underline{\Gamma} \vdash q : \underline{B} \to \underline{C}$ in $\mathbf{Fam}_{\underline{\Gamma}}$ is in fact equivariant $\Gamma \vdash q : B \mathrel{\circledast\!\!\longrightarrow} C$:

$$\begin{aligned} h \circledast (q\,b) &= q(h \circledast (s(q\,b))) = q(h \circledast (f(t\,b))) = q(f(h \circledast (t\,b))) = q(g(h \circledast (t\,b))) = q(h \circledast g(t\,b)) \\ &= q(h \circledast b) \end{aligned}$$

It is also a coequaliser in G-$\mathbf{Act}_\Gamma$. Given any coequalising equivariant map $\ell : B \mathrel{\circledast\!\!\longrightarrow} D$, the underlying family map $\ell : \underline{B} \to \underline{D}$ is also coequalising. Therefore, the unique extension in $\mathbf{Fam}_{\underline{\Gamma}}$ of ℓ along q is given by:

$$r : \underline{C} \overset{s}{\to} \underline{B} \overset{\ell}{\to} \underline{D}$$

It is an equivariant map $r : C \mathrel{\circledast\!\!\longrightarrow} D$. Indeed:

$$\begin{aligned} r(h \circledast c) &= \ell(s(h \circledast c)) = \ell(s(q(h \circledast s\,c)) = \ell(f(t(h \circledast s\,c)) = \ell(g(t(h \circledast s\,c))) = \ell(h \circledast s\,c) \\ &= h \circledast (\ell(s\,c)) = h \circledast (r\,c) \end{aligned}$$

Therefore $\underline{-}$ lifts split coequalisers of parallel pairs to coequalisers.

Now, if C already had an indexed A-action structure and q was equivariant, then necessarily $h \circledast c = h \circledast q(s\,c) = q(h \circledast (s\,c))$, and so the action on $\underline{C}$ must be the one we defined. Therefore, $\underline{-}$ reflects split coequalisers of parallel pairs as coequalisers.

By Beck's theorem, the free indexed action adjunction is monadic.

Turning to the right adjoint, we first prove it's an action:

$$e \circledast_\gamma \varphi \coloneqq (h \mapsto \varphi(h * e)) = (h \mapsto \varphi h) = \varphi$$

and:

$$(g \circledast k \circledast \varphi)h = (k \circledast \varphi)(h * g) = \varphi((h * g) * k) = \varphi(h * (g * k)) = ((g * k) \circledast \varphi)h$$

and so $g \circledast k \circledast \varphi = (g * k) \circledast \varphi$.

Next, take any Γ-indexed G-action A, and a vertical map $\underline{\Gamma} \vdash f : \underline{A} \to X$. Define:

$$\Gamma \vdash f^\dagger : A \mathrel{\circledast\!\!\longrightarrow} \big((g : G) \to g^{-1} \circledast X\big) \qquad f^\dagger_\gamma a \coloneqq (g \mapsto f(g \circledast a)) \in \big(g : \underline{G}\big) \to \big(X_{g\circledast\gamma}\big)$$

It is equivariant:

$$f^{\dagger}_{h \circledast \gamma}(h \circledast a) = g \mapsto f(g \circledast (h \circledast a)) = g \mapsto f((g * h) \circledast a) = h \circledast (g \mapsto f(g \circledast a)) = h \circledast f^{\dagger}_{\gamma} a$$

It lifts f along eval $\langle -, e \rangle$:

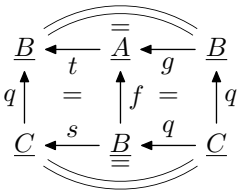
$$\text{eval} \left\langle f^{\dagger} a, e \right\rangle = (f^{\dagger} a) e = f(e \circledast a) = f\, a$$

Now if $\overline{f} : A \circledcirc\!\!\longrightarrow (g : G) \to g^{-1} \circledast X$ lifts f along eval $\langle -, e \rangle$, then:

$$(\overline{f} a) g = (\overline{f} a)(e * g) = (g \circledast (\overline{f} a))(e) = \text{eval} \left\langle g \circledast (\overline{f} a), e \right\rangle = \text{eval} \left\langle \overline{f}(g \circledast a), e \right\rangle = f(g \circledast a)$$

and so $\overline{f} = f^{\dagger}$, and we have a right adjoint.

We use Beck's theorem in its dual formulation. Consider a split equaliser, with A, B actions:



Equip $\underline{C}$ with the following indexed G-action structure: $k \circledast_{\gamma} c \coloneqq s(k \circledast_{\gamma} (q\, c))$. It is indeed an action, for $e \circledast c = s(e \circledast (q\, c)) = s(q\, c) = c$ and:

$$k \circledast h \circledast c = s(k \circledast (q(s(h \circledast (q\, c))))) = s(k \circledast h \circledast (q\, c)) = s((k * h) \circledast (q\, c)) = (k * h) \circledast c$$

We need to show the structure maps q and s (but not t!) are equivariant. For q:

$$q(k \circledast c) = q(s(k \circledast (q\, c))) = k \circledast (q\, c)$$

For s:

$$k \circledast s b = s(k \circledast (q(s\, b))) = s(k \circledast b)$$

Now, given an equalising equivariant map $\Gamma \vdash e : X \circledcirc\!\!\longrightarrow B$, by moving to families, we know the mediating map is $u : X \xrightarrow{e} B \xrightarrow{s} C$, and therefore equivariant. Therefore $\underline{-}$ lifts equalisers of split equalisers. Now, equip C with any action that makes $q : C \to B$ equivariant. We then have:

$$k \circledast c = s(q(k \circledast c)) = s(k \circledast (q\, c))$$

and so the action on C is the lifted one, making $q : C \to B$ a coequaliser, i.e., $\underline{-}$ reflects equalisers that split in $\underline{\Gamma}$-families. ■

Next, we justify not checking the second axiom of G-strengths in the cases $g = e$ or $h = e$:

Proof Lemma A.3

For $h = e$:

$$\begin{aligned}
F(\boxplus)(\mathbf{st}(g, \mathbf{st}(e, t))) &\overset{\text{first axiom}\ \downarrow}{=} F(\boxplus)(\mathbf{st}_X(g, F(x \mapsto \langle e, x \rangle) t)) \\
&\overset{\text{naturality}\ \downarrow}{=} F(\boxplus)(F(\langle g', x \rangle \mapsto \langle g', e, x \rangle)\, \mathbf{st}(g, t)) \\
&\overset{\text{map fusion}\ \downarrow}{=} (F(\langle g', x \rangle \mapsto \langle g' * e, x \rangle)\, \mathbf{st}(g, t)) \\
&= \mathbf{st}(g, t) = \mathbf{st}(g * e, t)
\end{aligned}$$

Next, for $g = e$:

$$\begin{aligned} F(\circledast)(\mathbf{st}(e, \mathbf{st}(h,t))) &\overset{\text{first axiom}}{=} F(\circledast)(F(\langle h', x\rangle \mapsto \langle e, h', x\rangle)(\mathbf{st}(h,t))) \\ &\overset{\text{map fusion}}{=} F(\langle h', x\rangle \mapsto \langle e * h', x\rangle)(\mathbf{st}(h,t)) \\ &= \mathbf{st}(h,t) = \mathbf{st}(e * h, t) \end{aligned}$$

as we wanted. ∎

Next, we state the indexed analogue to the Parameterised Initiality Theorem D.2 for the indexed setting:

Theorem E.1 (indexed parameterised initiality)**.** *Let Γ be a G-action, $F : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$ an endofunctor equipped with a symmetry strength, and $\underline{\Gamma} \vdash \mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ an initial F-algebra. For every F-algebra $f : FX \to X$, there is a unique* parameterised homomorphism *into $\langle X, f\rangle$, i.e., a map $\mathbf{pfold}\ f : G \circledast \boldsymbol{\mu}F \to X$ satisfying: $(\mathbf{pfold}\ f)(g, \mathbf{roll}\ u) = f \circ F(\mathbf{pfold}\ f)\ \mathbf{st}(g,u)$.*

We will prove this theorem and the Indexed Equivariant Initiality Theorem A.5 using the more abstract tools of the next section.

The remainder of this section establishes the results concerning canonisers for indexed G-strong functors, which do not have a general counterpart. By ignoring the indices, they also generalise the corresponding results from §4.3.

Lemma E.2. *Let Γ be a G-action, $F : \mathbf{Fam}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$ be a functor equipped with a symmetry strength $\mathbf{st} : G \circledast FX \to F(G \circledast X)$, and $c : F \to \underline{G}$ an indexed canoniser for F. The canonical elements extend to a functor $\mathsf{Can}\ c : G\text{-}\mathbf{Act}_{\underline{\Gamma}} \to \mathbf{Fam}_{\underline{\Gamma}}$ given for $\Gamma \vdash h : A \circledast\!\!\longrightarrow B$ by:*

$$(\mathsf{Can}\ c)\ h\ (g \circledast_\delta u) \coloneqq g \circledast_\delta (Fhu) \qquad (g = c_{\underline{A};\delta} u, g \circledast \delta = \gamma, u \in (F\underline{A})_\delta)$$

Consequently, we have an equivariant function $\Gamma \vdash ((\mathsf{Can}\ c)\ h : (\mathsf{Can}\ c)A \circledast\!\!\longrightarrow (\mathsf{Can}\ c)A$. The inclusions $\mathsf{Can}\ c \hookrightarrow F$ are natural.

Proof

First, since $h : A \circledast\!\!\longrightarrow B$ is equivariant, $Fh : FA \circledast\!\!\longrightarrow FB$ is equivariant. Therefore:

$$(\mathsf{Can}\ c)h(g \circledast_\delta u) \coloneqq Fh(g \circledast_\delta u) = g \circledast_\delta (Fhu)$$

and so the equation in the lemma statement defines a family map $k : (\mathsf{Can}\ c)A \to FB$, independently of the representatives used.

The crux of the proof is that, by c's naturality, $c_{\underline{B};\delta}(F\,hu) = c_{\underline{A};\delta}(u) = g$. Therefore, $g \circledast_\delta (F\,hu)$ is canonical, and $(\mathsf{Can}\ c)h$ is well-defined by lifting $k : (\mathsf{Can}\ c)A \to FB$ along the inclusion $(\mathsf{Can}\ c)B \hookrightarrow FB$. Functoriality follows by routine calculation. For equivariance, take:

$$\begin{aligned} g \circledast_\delta u &\in ((\mathsf{Can}\ c)A)_\gamma & (g = c_{\underline{A};\delta} u, g \circledast \delta = \gamma, u \in (F\underline{A})_\delta) \\ p \circledast_\xi v &\in ((\mathsf{Can}\ c)A)_\gamma & (p = c_{\underline{A};\xi} v, p \circledast \xi = \gamma, v \in (F\underline{A})_\xi) \end{aligned}$$

and $r \in G_\gamma \subseteq \underline{G}$ such that:

$$r \circledast_\gamma g \circledast_\delta u = p \circledast_\xi v$$

We then have:

$$\begin{aligned} (\mathsf{Can}\ c)\ h\ (p \circledast_\xi v) = p \circledast_\xi (F\,h\,v) &\overset{Fh : FA \circledast\!\!\longrightarrow FB}{=} F\,h\,(p \circledast_\xi v) = F\,h\,(r \circledast_\gamma g \circledast_\delta u) = r \circledast_\gamma g \circledast_\delta (F\,h\,u) \\ &= r \circledast_\gamma ((\mathsf{Can}\ c)\ h\ (g \circledast_\delta u)) \end{aligned}$$

and so $(\mathsf{Can}\ c)\ h$ is equivariant.

The naturality of the inclusions $\mathsf{Can}\ c \hookrightarrow F$ amounts to the calculation:

$$(\mathsf{Can}\ c)h(g \circledast_\delta u) \coloneqq g \circledast_\delta (Fhu) = Fh(g \circledast_\delta u)$$

which holds by equivariance of $Fh : FA \circledast\!\!\longrightarrow FB$. ∎

The following transformation lets us simultaneously work with canonical elements in a symmetric fibre while carrying around their canonising symmetry.

Proposition E.3. *The transformation* $\gamma : \underline{\Gamma} \vdash \mathsf{canonise}_c \coloneqq u \mapsto \langle (cu)^{-1}, cu \circledast_\gamma u \rangle : F \Rightarrow G \boxtimes (\mathsf{Can}\ c)$ *is natural.*

Proof

More generally, for every $g \in \underline{G}$, we have transformation:

$$\gamma : \underline{\Gamma} \vdash (g \circledast_\gamma \eta -) : \underline{A} \to G \boxtimes \underline{A} \qquad g \circledast_\gamma \eta a \coloneqq \langle g, g^{-1} \circledast_\gamma a \rangle = g \overset{G \boxtimes \underline{A}}{\circledast_{g^{-1} \circledast \gamma}} \langle e, g^{-1} \circledast_\gamma a \rangle$$

Given an equivariant family map $\Gamma \vdash f : A \circledast\!\!\longrightarrow B$, we indeed have:

$$\begin{array}{ccc} \underline{A} \ni a & \xmapsto{(g \circledast_\gamma)} & \langle g, g^{-1} \circledast_\gamma a \rangle \in G \boxtimes \underline{A} \\ \Big\downarrow{\scriptstyle f_\gamma} & f \text{ equivariant} = & \Big\downarrow{\scriptstyle (G \boxtimes f)_\gamma} \\ \underline{B} \ni f_\gamma a & \xmapsto[(g \circledast_\gamma)]{} & \langle g, g^{-1} \circledast_\gamma f a \rangle = \langle g, f(g^{-1} \circledast_\gamma a) \rangle \in G \boxtimes \underline{B} \end{array}$$

We now use the canoniser's naturality:

$$\begin{aligned} \mathsf{canonise}(Ffu) &\coloneqq \left\langle (c(Ffu))^{-1}, (c(Ffu)) \circledast (Ffu) \right\rangle \overset{c : F \to \underline{G}\ \text{natural}}{=} \left\langle (cu)^{-1}, (cu) \circledast (Ffu) \right\rangle \\ &\overset{Ff : FA \circledast\!\!\to FB}{=} \left\langle (cu)^{-1}, Ff\left((cu) \circledast (u)\right) \right\rangle \overset{((cu)^{-1} \circledast \eta -) : \underline{C} \to G \boxtimes \underline{C}\ \text{natural}}{=} Ff\left(\left\langle (cu)^{-1}, (cu) \circledast u \right\rangle\right) \\ &=: Ff(\mathsf{canonise}\ u) \end{aligned}$$

as we wanted. ∎

We can use this transformation to express the w.l.o.g. construction:

Lemma E.4. *We have:*

$$\underline{\Gamma} \vdash \mathsf{wlog}(c, f) : F\underline{A} \xrightarrow{\mathsf{canonise}_c} \underline{G \boxtimes ((\mathsf{Can}\ c)A)} \xrightarrow{G \boxtimes f} \underline{G \boxtimes \underline{A}} \xrightarrow{(\circledast)} \underline{A}$$

Proof

Calculate:

$$\begin{aligned} u \xmapsto{\mathsf{canonise}_c} \left\langle (cu)^{-1}, (cu) \circledast u \right\rangle \xmapsto{G \boxtimes f} \left\langle (cu)^{-1}, f\left((cu) \circledast u\right) \right\rangle \xmapsto{(\circledast)} (cu)^{-1} \circledast f\left((cu) \circledast u\right) \\ = \mathsf{wlog}(c, f) \end{aligned}$$

as we wanted. ∎

The next result establishes a universal property for the intermediate step in the **flog** construction: the extension of a core algebra to an F-algebra.

Theorem E.5 (indexed equivariant algebra representation)**.** *Let Γ be a G-action, F a Γ-indexed G-strong functor, and $c : F \Rightarrow \underline{G}$ an indexed canoniser for F, and consider an indexed equivariant core-F algebra $\Gamma \vdash f : (\mathsf{Can}\, c)A \circledast\!\!\longrightarrow A$. Then the w.l.o.g. construction is the unique equivariant F-algebra $\Gamma \vdash \mathsf{wlog}(c, f) : FA \circledast\!\!\longrightarrow A$ extending f along the inclusion $\mathsf{Can}\, c \hookrightarrow F$.*

Given two equivariant F-algebras (A, f) and (B, g) and an equivariant function $\Gamma \vdash h : A \circledast\!\!\longrightarrow B$, it is an equivariant F-homomorphism $\Gamma \vdash h : (A, f) \circledast\!\!\longrightarrow (B, g)$ iff it is an equivariant core-$\mathsf{Can}\, c$ algebra homomorphism.

Proof

Assume $f : (\mathsf{Can}\, c)A \circledast\!\!\longrightarrow A$ is a core algebra. By the naturality of $\mathsf{Can}\, c$, f is a core function for the canoniser $c_A : F\underline{A} \to \underline{G}$. This function is equivariant w.r.t. c_A in the sense of the main paper iff it is equivariant w.r.t. the canoniser c for F in the sense of Definition A.10.

If f is equivariant, then by the Indexed Representation Theorem 3.12, $\mathsf{wlog}(c, f) = \mathsf{wlog}(c_{\underline{A}}, f)$ is equivariant extending f. Covnersely, if $h : FA \circledast\!\!\longrightarrow A$ is an equivariant algebra, then by the representation theorem, $h = \mathsf{wlog}(c_{\underline{A}}, f) = \mathsf{wlog}(c, f)$, as we wanted.

Given another such equivariant algebra $g : FB \circledast\!\!\longrightarrow B$, and an equivariant map $h : A \to B$. The naturality and injectivity of the embedding $\mathsf{Can}\, c \hookrightarrow F$ show that h is an F-algebra homomorphism iff it is a $\mathsf{Can}\, c$-algebra homomorphism. Indeed, consider the composite square:

$$\begin{array}{ccccc} (\mathsf{Can}\, c)A & \hookrightarrow & FA & \xrightarrow{f} & A \\ {\scriptstyle (\mathsf{Can}\, c)h}\downarrow & \overset{\text{naturality}}{=} & {\scriptstyle Fh}\downarrow & (**) & \downarrow{\scriptstyle h} \\ (\mathsf{Can}\, c)B & \hookrightarrow & FB & \xrightarrow[g]{} & B \end{array} \qquad (*)$$

Our goal is to show that the inner square $(**)$ commutes—h is an F-algebra homomorphism—iff the outer square $(*)$ commutes—h is a $\mathsf{Can}\, c$-algebra homomorphism. If $(**)$ commutes, the whole diagram commutes. Assume $(*)$ commutes. We have that f, g, and h are equivariant, and the latter also implies that Fh is equivariant. Therefore, the two sides of $(**)$ are equivariant extensions of the outer face $(*)$ along the embedding $(\mathsf{Can}\, c)A \hookrightarrow FA$. By the indexed representation theorem, they coincide, i.e., $(**)$ commutes. ■

We conclude by proving the representation theorem for the indexed **flog** construction:

Proof

The proof assembles the previous results. First, by the indexed equivariant initiality theorem, the initial algebra is equivariant $\mathbf{roll} : F\boldsymbol{\mu}F \circledast\!\!\longrightarrow \boldsymbol{\mu}F$. By the algebra representation Theorem E.5, its restriction along the embedding $\mathsf{Can}\, c \hookrightarrow F$ is an equivariant algebra $\mathbf{roll} : (\mathsf{Can}\, c)\boldsymbol{\mu}F \to \boldsymbol{\mu}F$.

Now, given any equivariant core algebra $f : (\mathsf{Can}\, c)A \circledast\!\!\longrightarrow A$, by the algebra representation Theorem E.5, its w.l.o.g. construction is an equivariant algebra $g \coloneqq \mathsf{wlog}(c, f) : FA \circledast\!\!\longrightarrow A$. By the equivariant initiality theorem, the unique F-homomorphism out of the initial algebra is equivariant $\mathbf{flog}\, f \coloneqq \mathbf{fold}\, g : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$. By the algebra representation Theorem E.5, it is also a $(\mathsf{Can}\, c)$-homomorphism.

Conversely, if $h : \boldsymbol{\mu}F \circledast\!\!\longrightarrow A$ is any equivariant core algebra homomorphism, then by Theorem E.5, it is an equivariant F-homomorphism. By the equivariant initiality theorem, $h = \mathbf{fold}\, g = \mathbf{flog}\, f$. ■

F Category theoretic development

The amount of details in the theory of indexed symmetric data types is high, but a few categorical abstractions keep the development relatively clean. We start by recasting the parameterised initiality

theorems in this setting. Much of this is known but appears in different places in the work of Fiore et al. [35], and especially in the more recent work with Szamozvancev [33, 34, 87]. We provide references where available.

Lemma F.1. *Let $P, F : C \to C$ be two endofunctors, and* $\mathbf{st} : PF \to FP$ *a natural transformation. Then F lifts along the forgetful functor $\langle x, a\rangle \mapsto x$ to an endofunctor over P-algebras:*

$$\langle x, a : Px \to x\rangle \mapsto \left\langle Fx, a_F : PFx \xrightarrow{\mathbf{st}} FPx \xrightarrow{Fa} Fx \right\rangle$$
$$\left(\langle x, a\rangle \xrightarrow{h} \langle y, b\rangle\right) \mapsto \left(\langle Fx, a_F\rangle \xrightarrow{Fh} \langle Fy, b_F\rangle\right)$$

The proof is by direct calculation, see Prop. 3.1.2 in Szamozvancev's thesis. This type of result is known from the early days of the concept, as in Beck's work [11].

When P is a left adjoint $P \dashv E$, we can swap P-strengths for an endofunctor F with E-costrengths for the same endofunctor[7]:

Lemma F.2 (strength-costrength)**.** *Consider endofunctors $P, E, F : C \to C$. Let $P \dashv E$ with unit $\eta : \mathrm{Id} \to EP$ and counit $\varepsilon : PE \to \mathrm{Id}$. TFAE:*

- *P-strengths for F, i.e., natural transformations* $\mathbf{st} : PF \to FP$.
- *E-costrengths for F, i.e., natural transformations* $\mathrm{costrength} : FE \to EF$.

The equivalence is given by the following relationships:

$$\begin{array}{ccc} FEx & \xrightarrow{\eta} & EPFEx \\ {\scriptstyle \mathrm{costrength}}\downarrow & := & \downarrow{\scriptstyle E\,\mathbf{st}} \\ EFx & \xleftarrow[EF\varepsilon]{} & EFPEx \end{array} \qquad \begin{array}{ccc} FPx & \xleftarrow{\varepsilon} & PEFPx \\ {\scriptstyle \mathbf{st}}\uparrow & := & \uparrow{\scriptstyle P\,\mathrm{costrength}} \\ PFx & \xrightarrow[PF\eta]{} & PFEPx \end{array}$$

and moreover satisfy:

$$\begin{array}{ccc} Fx & \xrightarrow{F\eta} & FEPx \\ {\scriptstyle \eta}\downarrow & = & \downarrow{\scriptstyle \mathrm{costrength}} \\ EPFx & \xrightarrow[E\,\mathbf{st}]{} & EFPx \end{array} \qquad \begin{array}{ccc} Fx & \xleftarrow{F\varepsilon} & FPEx \\ {\scriptstyle \varepsilon}\uparrow & = & \uparrow{\scriptstyle \mathbf{st}} \\ PEFx & \xleftarrow[P\,\mathrm{costrength}]{} & PFEx \end{array}$$

Proof

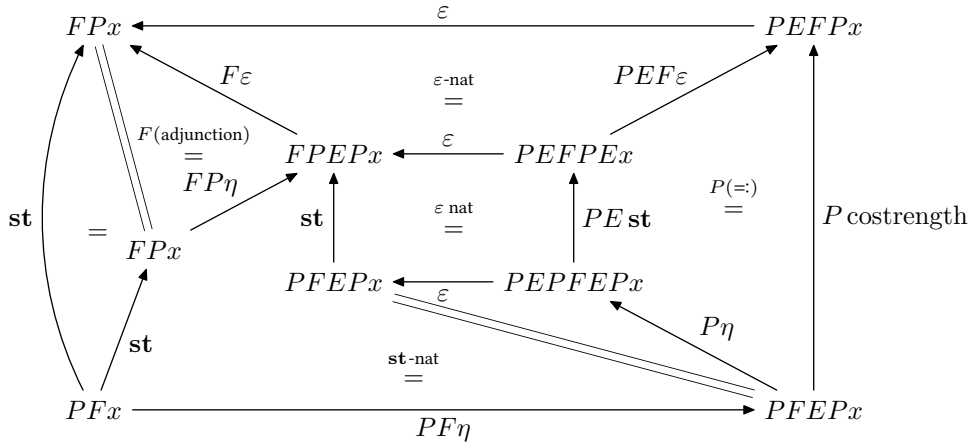
By duality, we only need to show:

- That costrength is natural.
- That the strength associated with costrength is **st**.
- The diagram involving the units only (η and $F\eta$).

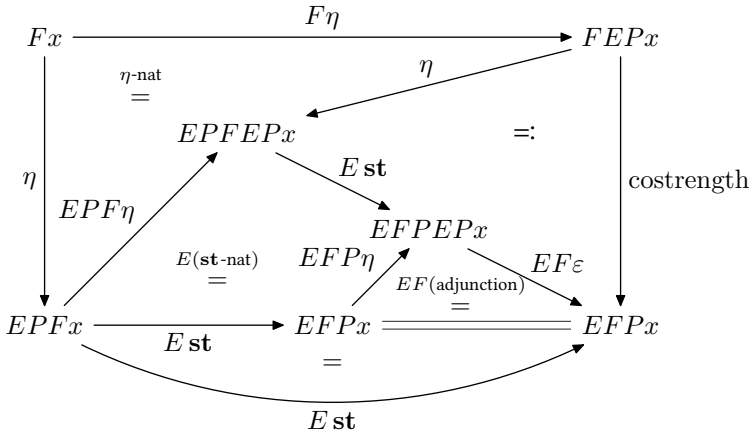
The costrength is natural: it is a composition of natural transformations.

We substitute the definition of costrength into the definition of **st** and show it recovers **st**:

[7] We learned this fact from Marcelo P. Fiore in private communication.



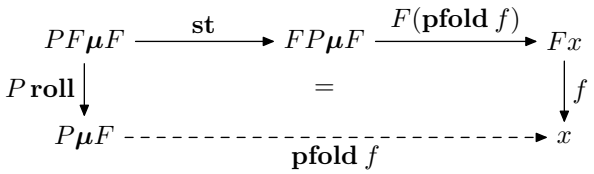
The diagram involving units only amounts to straightforward calculation:



■

We now prove a general version of parameterised initiality, already prevalent in Fiore et al.'s work on abstract syntax [33, 34, 36], originally proposed by Bird and Paterson [13].

Definition F.3. Let $P, F : C \to C$ be endofunctors. An initial F-algebra $\mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ is *P-initial* when every F-algebra $f : Fx \to x$ has a unique morphism $\mathbf{pfold}\ f : P\boldsymbol{\mu}F \to x$ satisfying:



Theorem F.4 (generalised parameterised initiality)**.** *Let $P \dashv (E : C \to C)$ be an adjunction over a category C, with unit $\eta : \mathrm{Id} \to EP$ and counit $\varepsilon : PE \to \mathrm{Id}$. Every initial algebra $\mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$, for an endofunctor $F : C \to C$ equipped with a natural transformation $\mathbf{st} : PF \to FP$, is P-initial.*

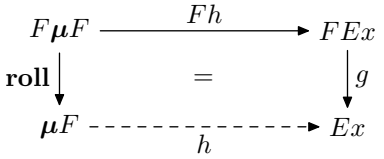
For completeness, we include the proof of this result in this formulation.

Proof

Let $f : Fx \to x$ be any F-algebra. We equip Ex with an F-algebra structure. It is more direct to work with the costrength:

$$g : FEx \xrightarrow{\text{costrength}} EFx \xrightarrow{Ef} Ex$$

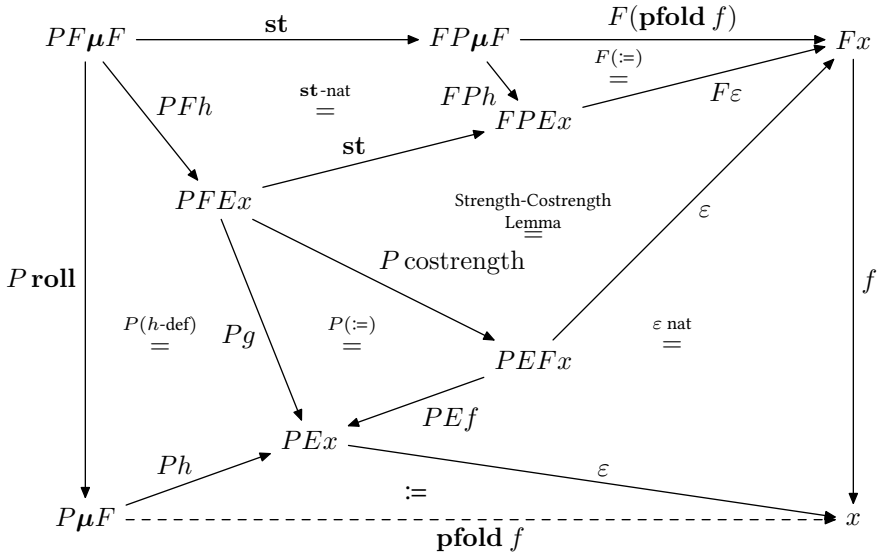
and so, by initiality, we have a unique morphism $h \coloneqq \mathbf{fold}\, g : \boldsymbol{\mu}F \to Ex$ satisfying:



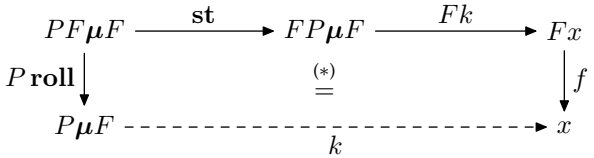
Now take the mate of this morphism:

$$\mathbf{pfold}\, f : P\boldsymbol{\mu}F \xrightarrow{Ph} PEx \xrightarrow{\varepsilon} x$$

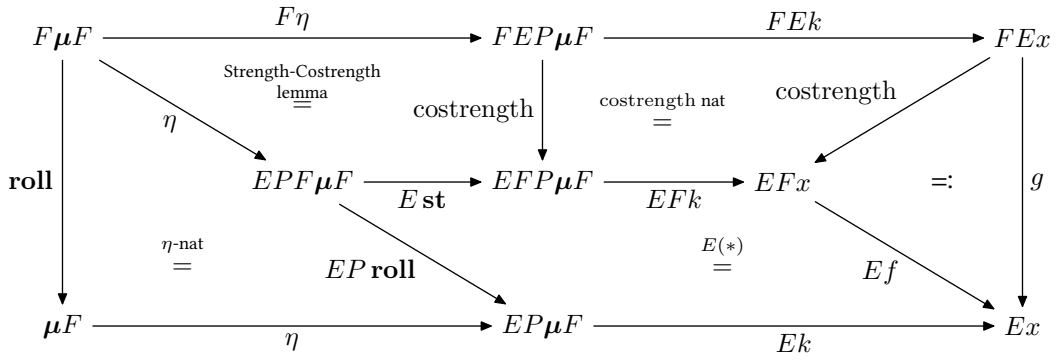
This morphism satisfies the required property:



Now consider any morphism $k : P\boldsymbol{\mu}F \to x$ making the following diagram commute:



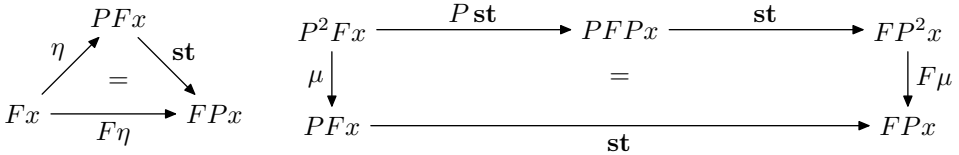
We will show that its mate must be h, i.e.: $h : \boldsymbol{\mu}F \xrightarrow{\eta} EP\boldsymbol{\mu}F \xrightarrow{Ek} Ex$. Calculate:



By universality, h is the mate of k, and so $k = \mathbf{pfold}\ f$. ■

Therefore, if an endofunctor F over $\underline{\Gamma}$-indexed families has a $(G \circledast -)$-strength, then its initial algebras are both $(G \circledast -)$-initial and $(G \circledast G \circledast -)$-initial.

Definition F.5. Let $P = \langle P : C \to C, \eta, \mu \rangle$ be a monad, and $F : C \to C$ an endofunctor over C. A *P-strength for F* is a natural transformation $\mathbf{st} : PF \to FP$ satisfying:



This notion is sometimes called: a *distributive law* between a monad and a functor; a *module*; or a *monad endomorphism*.

The following notion generalises equivariant F-algebras as algebras of the lifting of F to P-algebras:

Definition F.6. Let $P = \langle P : C \to C, \eta, \mu \rangle$ be a monad over C, and $F : C \to C$ an endofunctor equipped with a P-strength $\mathbf{st}\ P : PF \to FP$. A *$P$-linear F-algebra* $\langle x, f, a \rangle$ consists of:

- an F-algebra $f : Fx \to x$; and
- a P-algebra $a : Pa \to a$;

such that f is P-linear $f : \langle Fx, a_F \rangle \to \langle x, a \rangle$. A *homomorphism* $h : \langle x, f, a \rangle \to \langle y, g, b \rangle$ of P-linear F-algebras is a morphism $h : x \to y$ that is simultaneously an F-algebra homomorphism and a P-algebra homomorphism.

Since a $(G \circledast -)$-algebra is precisely a Γ-indexed G-action and a $(G \circledast -)$-linear map between them is precisely an equivariant function, we have that the $(G \circledast -)$-linear F-algebras are precisely the equivariant F-algebras. The capstone of this development is the following theorem:

Theorem F.7 (general representation theorem)**.** *Let $P = \langle P : C \to C, \eta, \mu \rangle$ be a monad over C, and $F : C \to C$ an endofunctor equipped with a P-strength $\mathbf{st} : PF \to FP$. If an initial F-algebra $\mathbf{roll} : F\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ is both P-initial and P^2-initial, then it is also the initial P-linear F-algebra. Its P-algebra structure is given by P-initiality as $\mathbf{alg} \coloneqq \mathbf{pfold}\ \mathbf{roll} : P\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ and the unique F-homomorphism $\mathbf{fold}\ f : \boldsymbol{\mu}F \to x$ into any other P-linear F-algebra $\langle x, f, a \rangle$ is P-linear.*

We chose this formulation as its proof follows our proof in the simply-typed case more closely, which itself follows the argument in abstract syntax with binding and substitution [35]. Our situation is semantically well-behaved, and there are alternative theorems we could use. For example, since Γ-indexed G-actions are $E \coloneqq (G \multimap\!\!\circledast -)$-algebras, we could use Szamozvancev's Prop. 3.3.1

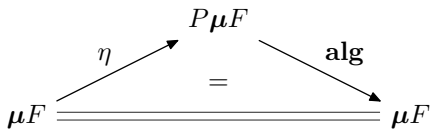
instead [34]. Whichever formulation we use, it is clear it proves the Indexed Representation Theorem A.5.

Proof

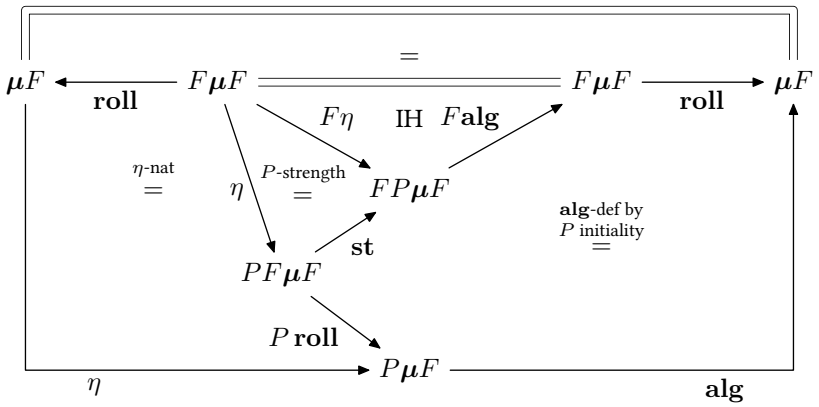
We show that:

- **alg** : $P\boldsymbol{\mu}F \to \boldsymbol{\mu}F$ is a P-algebra;
- **roll** is P-linear by the defining property of P-initiality;
- each **fold** f is P-linear.

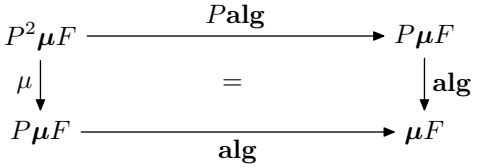
We show the P-algebra unit axiom:



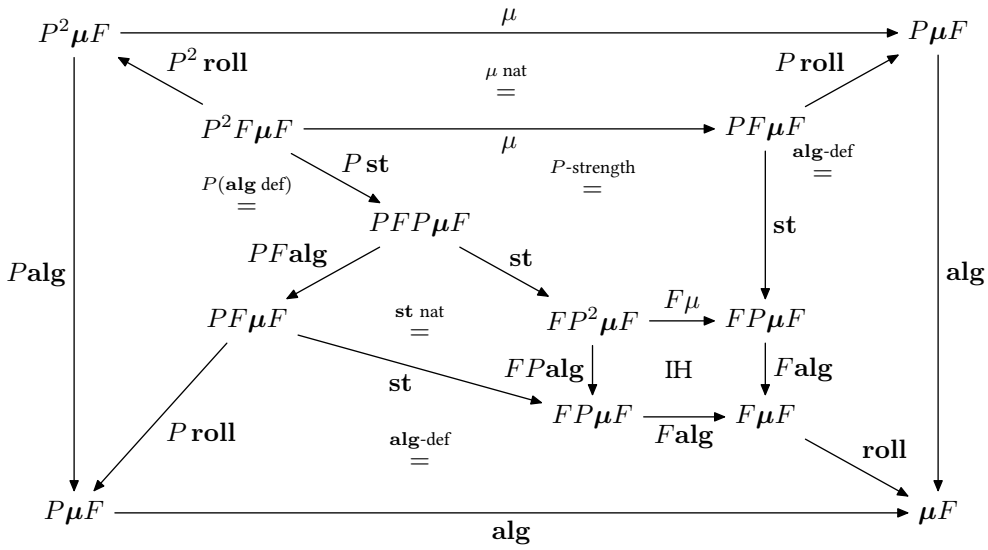
by recourse to mere initiality:



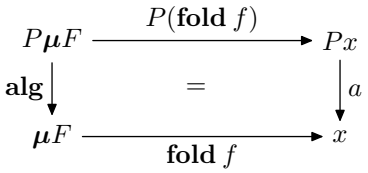
We show the P-algebra multiplication axiom:



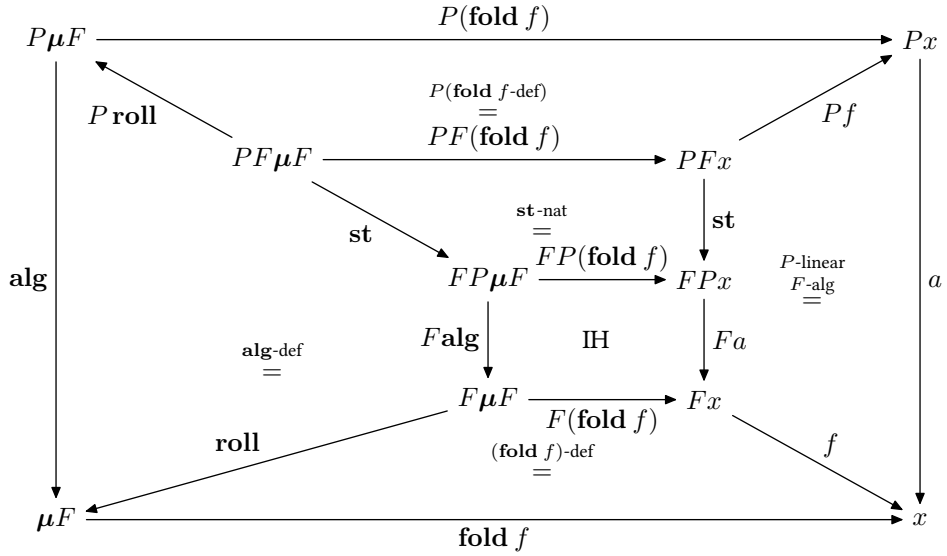
by recourse to P^2 initiality:



Finally, take any P-linear F-algebra $\langle x, f, a\rangle$. By initiality there is at most one P-linear F-homomorphism, and exactly one F-homomorphism, into it. We show:



by recourse to P-initiality:



concluding the proof. ■