Skript zur Vorlesung

Nominal Sets

von *Thorsten Wißmann*
im Sommersemester 2024
an der FAU Erlangen-Nürnberg

Danksagungen
Ich bin folgenden Personen für das aufmerksame Lesen und das finden von Fehlern dankbar; sie haben zur Verbesserung dieses Skripts beigetragen:

- Florian Frank
- Lorena Kretzschmar
- Silas Kuder

Die Präsentation in Abschnitt 8.1 folgt handschriftlichen Notizen von Florian Frank.

Aktuelle Version
Die vorliegende Version hat den Stand:
`11. Oktober 2024, 07:23 Uhr`

Inhaltsverzeichnis

1 Übersicht

Ein zentraler Aspekt in der Semantik von Programmiersprachen und allgemein der Informatik ist das Binden von (Variablen-)Namen, also die Frage: *Was bezieht sich auf was?*

Operationen auf Programmen und anderen Strukturen mit Variablen-Bindung (z. B. logischen Formeln) sind dabei leichter implementierbar und deren Korrektheit beweisbar, wenn die Strukturen nur bis auf Umbenennung von gebundenen Variablen zu betrachtet werden, d. h. modulo α-Äquivalenz. Das ist besonders der Fall, wenn die Operationen Variablen durch andere Terme ersetzen, die selber wieder freie Variablen haben; beispielsweise:

- β-Reduktion im λ-Kalkül (vgl. Theorie der Programmierung)
- Allquantor-Elimination in Prädikatenlogik (vgl. Grundlagen der Logik in der Informatik)

Bei solchen Operationen muss man nämlich Verhindern, dass die freien Variablen im eingesetzten Term fälschlicherweise gebunden, weil sie zufällig so heißen wie eine (eigentlich andere) lokale Variable. Bei diesem bekannten Beispiel im λ-Kalkül zeigt der erste Pfad die fehlerhafte β-Reduktion, die y einfängt und darunter die Reduktion, die das Einfangen vermeidet (engl.: capture avoiding):

$$\begin{tikzcd}
(\lambda x.\, \lambda y.\, x\, y)\, y \arrow[r, dashed, "\beta", "/" marking] \arrow[d, "\alpha"'] & \lambda y.\, y\, y \arrow[d, dashed, "\alpha", "/" marking] \\
(\lambda x.\, \lambda z.\, x\, z)\, y \arrow[r, "\beta"] & \lambda z.\, y\, z
\end{tikzcd}$$

Eine bekannte Technik des Abstrahierens von Variablennamen sind *de Bruijn Indizes* [4] (gesprochen: *Braun*). Hierbei wird statt Variablennamen lediglich eine natürliche Zahl (d. h. Index) verwendet, die die Distanz zum zugehörigen Binder (also der Variablendefinition) angibt. Im λ-Kalkül bedeutet Distanz die Anzahl der Binder (λ) zwischen einer Variable und ihrem zugehörigen Binder, siehe z. B. Abbildung 1. Nachdem es ja keine Namen mehr gibt (sondern nur noch Indizes), sind im Beispiel auch keine Namen mehr an den Bindern, und es kann somit auch keine Namenskollisionen mehr geben. Diese Angabe der Distanz hat allerdings zur Folge, dass Index 0 für unterschiedliche Variablen steht, je nach dem wo der Index eben vorkommt. Und umgekehrt muss beim Ersetzen einer Variable durch eine andere (z. B. während β-Reduktion) dieser Index passend berechnet werden, je nach dem, wie *tief* im Term die neue Variable eingesetzt wird. Dadurch unterscheidet sich also der mathematische Formalismus davon, wie wir als Menschen intuitiv mit Variablen umgehen.

$$\lambda x.\, x\, (\lambda x.\, x)\, (\lambda y.\, x\, y) \quad \Longleftrightarrow \quad \lambda\ 0\ (\lambda\ 0)\ (\lambda\ 1\ 0)$$

Abbildung 1: Beispiel von de Bruijn Indizes im λ-Kalkül

Diese Lücke wird durch nominale Mengen geschlossen: Der Grundstein dafür wurde im LICS-Paper von Jamie Gabbay und Andrew Pitts [5] gelegt, in dem allerdings noch nicht der Begriff *Nominal Sets* sondern *FM-sets* verwendet wurde. Dieser bezieht sich auf ein Mengentheorie von Fraenkel und Mostowski aus den 1920ern, die Mengen mit *Atomen* betrachteten. Einer der Beträge des Papers ist es, dass sich diese Atome ähnlich wie Variablennamen verhalten: man kann sie vertauschen (Umbenennung) und man kann sie auf Gleichheit überprüfen. Durch die Mengentheoretische Sichtweise sind nominale Mengen leichter zu verstehen als andere Formalismen für Namensbindung, die beispielsweise mit speziellen Funktor-Kategorien arbeiten.

Letztendlich ist die mengentheoretische Sichtweise der nominalen Mengen eine Repräsentation von einem dieser kategoriellen Modelle (einer Kategorie namens *Schanuel-topos*) und der Betrag von Gabbay und Pitts war es, Variablenbindung (bzw. α-Äquivalenz) mengentheoretisch elegant zu formulieren.

Intuitiv ist eine Nominale Menge (urspr. *FM-set* [5]) eine Menge X, in der jedes Element $x \in X$ eine *endliche* Menge $\mathsf{supp}(x)$ von Atomen (also freien Variablen) trägt und außerdem eine Operation bereitstellt, diese Atome (bijektiv) umzubenennen. Im Falle von λ-Termen modulo α-Äquivalenz ist der Support $\mathsf{supp}(t)$ genau die Menge aller freien Variablen von t.

Um nominale Konzepte mit der üblichen Mengentheorie besser vergleichen und katalogisieren zu können, werden wir trotzdem bei Bedarf auf Begriffe aus der Kategorientheorie zurückgreifen und einführen.

Weiteres Material kann optional hier nachgeschlagen werden:

- Das Buch von Andrew Pitts [13] zu *Nominal Sets*: hieran wird sich die Veranstaltung maßgeblich orientieren. Das Buch ist aus dem Uni-Netz als PDF unter der DOI `https://doi.org/10.1017/CBO9781139084673` abrufbar.
- Das Paper von Jamie Gabbay und Andrew Pitts [5], das den Startschuss für die heutige Theorie der Nominalen Mengen gegeben hat.
- Alles was an Kategorientheorie verwendet wird, wird bei Bedarf hier vollständig definiert. Weitere Grundlagen sind in der Vorlesungsmitschrift von *Algebra des Programmierens* [16] (auf Deutsch) zu finden. An englischsprachiger Einführungsliteratur zu Kategorientheorie gibt es die Bücher von Awodey [2] und von Adámek, Herrlich, Strecker [1] (beide online verfügbar).
- Automatentheorie [3, 14]: mittels nominalen Mengen lassen sich Konzepte von *endlichen* Automaten definieren, die in der Lage sind, Eingaben über einem *unendlichen* Eingabealphabet verarbeiten können. Das Paper [3] von Bojanczyk, Klin und Lasota verallgemeinert gleichzeitig den Begriff von nominalen Mengen auf andere Symmetrien als nur Vertauschung und Gleichheitsprüfung von Namen, z. B. auf eine linear geordnete Menge von Atomen.
- Die *bijektive* Umbenennung stellt sicher, dass zwei unterschiedliche Namen nie durch Umbenennung gleichgemacht werden können. Erlaubt man das jedoch explizit, erhält man *Nominal Renaming Sets* von Gabbay und Hofmann [6]. Nominal Renaming Sets stehen in starker Beziehung zu den üblichen nominalen Mengen und dienen auch als Grundlage für Automatentheorie (siehe Moerman und Rot [12]).
- Die gängige Definition von nominalen Mengen betrachtet zuerst die Kategorie der Gruppenoperationen und schränkt dann auf solche mit endlichem Support ein. Die oben angeführte Intuition von endlich vielen Variablen, die sich dann Umbenennen lassen lässt sich mathematisch genauso realisieren (auch für andere Symmetrien und

für Renaming Sets). Man betrachtet zuerst die Kategorie der *Supported Sets* [15] und erhält dann nominale Mengen als *algebraische Kategorie* darüber. Das ist analog zu Theorien wie Gruppen, Verbände, etc. die algebraische Kategorien über Mengen sind. Nominale Mengen sind selbst nicht algebraisch über (gewöhnlichen) Mengen, aber über Supported Sets.

2 Gruppenoperationen

Die Idee von nominalen Mengen ist es, dass die Strukturen X, die (Variablen-)Namen enthalten, opak sind und lediglich eine Operation bereitstellen: das bijektive Umbenennen (also Vertauschen) von Namen. Dies ist eine bekannte algebraische Struktur, nämlich die Operation einer Gruppe auf einer Menge X. Alle anderen Konzepte auf nominalen Mengen, z. B. welche Namen in einer Struktur vorkommen und wie sie zu binden sind, werden dann auf Gruppenoperationen reduziert:

Definition 2.1. Eine *Gruppe* $(G, \cdot)$ ist eine Menge G zusammen mit einer binären Operation '$\cdot$': $G \times G \to G$ (*Verknüpfung*), sodass gilt:

(a) $\cdot$ is assoziativ: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (für alle $x, y, z \in G$)

(b) es gibt ein neutrales Element $e \in G$: $x \cdot e = x = e \cdot x$ (für alle $x \in G$)

(c) jedes Element $x \in G$ hat ein Inverses x^{-1}: $x \cdot x^{-1} = e = x^{-1} \cdot x$

Ein *Gruppenhomomorphismsus* $f\colon (G, \cdot) \to (H, \cdot)$ ist eine Abbildung $f\colon G \to H$ mit $f(x \cdot y) = f(x) \cdot f(y)$. Eine *Untergruppe* von $(H, \cdot)$ ist durch einen injektiven Gruppenhomomorphismus $f\colon (G, \cdot) \to (H, \cdot)$ repräsentiert.

Beispiel 2.2. Für uns sind in erster Linie diese Permutationengruppen von Bedeutung:

(a) Für eine Menge A sei $(\mathsf{Sym}(A), \cdot)$ die Gruppe aller bijektiven Abbildungen auf A:

$$\mathsf{Sym}(A) = \{\pi\colon A \to A \mid \pi \text{ bijektiv}\}$$

Die Verknüpfung $\cdot$ ist Funktionskomposition (in der üblichen Reihenfolge):

$$(\pi \cdot \sigma) := (\pi \circ \sigma) = (a \mapsto \pi(\sigma(a)))$$

Das neutrale Element ist die Identität $\mathrm{id}_A\colon A \to A$, $\mathrm{id}_A(x) := x$.

(b) Der *Support* (auch *Träger*) einer (Endo-)Funktion $\pi\colon A \to A$ ist

$$\mathsf{supp}(\pi) := \{a \in A \mid \pi(a) \neq a\}$$

Eine Bijektion $\pi \in \mathsf{Sym}(A)$ heißt *endlich*, wenn $\mathsf{supp}(\pi)$ endlich ist; also wenn sie nur für nur endlich viele Elemente von A nicht konstant ist. Die endlichen Bijektionen bilden die Untergruppe $\mathfrak{S}_{\mathsf{f}}(A) \subseteq \mathsf{Sym}(A)$ der *(endlichen) Permutationen*:

$$\mathfrak{S}_{\mathsf{f}}(A) = \{f\colon A \to A \mid f \text{ bijektiv und endlich}\}$$

Notation 2.3. Wir verwenden den Begriff *Permutation* nur für endliche Bijektionen. Pitts [13] verwendet den Begriff für endliche und unendliche Bijektionen, verwendet aber die Notationen Sym und Perm $:= \mathfrak{S}_{\mathsf{f}}$.

Lemma 2.4. *Für jede Permutation $\pi \in \mathfrak{S}_{\mathsf{f}}(A)$ gibt es $n \in \mathbb{N}$ mit $n > 0$ und $\pi^n = id$.*

Beweis. Sei $S := \mathsf{supp}(\pi)$ und damit $\mathfrak{S}_\mathsf{f}(S)$ eine Untergruppe von $\mathfrak{S}_\mathsf{f}(A)$, die π enthält. Da S und damit auch $\mathfrak{S}_\mathsf{f}(S)$ endlich ist, ist die Menge

$$\{\pi^k \mid k \in \mathbb{N}\} \subseteq \mathfrak{S}_\mathsf{f}(S)$$

auch endlich. Folglich gibt es *unterschiedliche* $k, m \in \mathbb{N}$ (sei $k < m$ o.B.d.A.) mit $\pi^k = \pi^m$. Somit ist $n := m - k \in \mathbb{N}$ und

$$\mathrm{id} = \pi^0 = \pi^m \cdot (\pi^k)^{-1} = \pi^{m-k}. \qquad \square$$

Eine spezielle Art von Permutationen sind *zyklische Permutationen* $(a_1 \;\; a_2 \;\; \cdots \;\; a_k)$ (für paarweise verschiedene a_i, $1 \leq i \leq k$), definiert durch:

$$(a_1 \;\; a_2 \;\; \cdots \;\; a_k) \in \mathfrak{S}_\mathsf{f}(A) \qquad x \mapsto \begin{cases} a_{\ell+1} & \text{falls } x = a_\ell \text{ für } \ell < k \\ a_1 & \text{falls } x = a_\ell \text{ für } \ell = k \\ x & \text{sonst.} \end{cases}$$

Ein Spezialfall davon sind *Transpositionen*: sie vertauschen lediglich zwei Elemente $a_1, a_2 \in A$ (nicht zwingend verschieden):

$$(a_1 \;\; a_2) \in \mathfrak{S}_\mathsf{f}(A) \qquad (a_1 \;\; a_2)(x) := \begin{cases} a_2 & \text{falls } x = a_1 \\ a_1 & \text{falls } x = a_2 \\ x & \text{sonst.} \end{cases}$$

Die Transpositionen erzeugen alle endlichen Permutationen:

Theorem 2.5 (Übungsaufgabe)**.** *Jede endliche Permutation $\pi \in \mathfrak{S}_\mathsf{f}(A)$ lässt sich als Komposition von Transpositionen schreiben.*

2.1 Struktur

Definition 2.6. Die *Aktion* einer Gruppe $(G, \circ)$ *auf* einer Menge X (auch *Gruppenoperation*, *Wirkung*, engl.: *G-set*) ist eine Abbildung '$\cdot$': $G \times X \to X$ (in Infix-Schreibweise), sodass:

(a) $e \cdot x = x$, für alle $x \in X$ und das neutrale Element e.

(b) $(\pi \circ \sigma) \cdot x = \pi \cdot (\sigma \cdot x)$, für alle $x \in X$ und $\pi, \sigma \in G$.

Bemerkung 2.7. Zur besseren Unterscheidbarkeit haben in Definition 2.6 die Verknüpfung der Gruppe und die Aktion unterschiedliche Symbole. In Zukunft werden wir beides mit $\cdot$ bezeichnen, selbst wenn wir Gruppenoperationen auf unterschiedlichen Trägern haben.

Bemerkung 2.8 (Übungsaufgabe)**.** Eine Abbildung $h\colon G \times X \to X$ ist genau dann eine Gruppenoperation, wenn $\bar{h}\colon G \to (X \to X)$, $\bar{h}(g)(x) := h(g, x)$ ein Gruppenhomomorphismus $(G, \cdot) \to \mathsf{Sym}(X)$ ist.

Wie eben schon verwendet bezeichnet $Y \to Z$ die Menge aller Abbildungen von Y nach Z. Je nach Kontext schreiben wir synonym $Z^Y := (Y \to Z)$.

Beispiel 2.9. Beispiele für Aktionen:

(a) Für $G := \mathfrak{S}_{\mathsf{f}}(A)$ (sowie für $G := \mathsf{Sym}(A)$) und $X := A$: definiere $\pi \cdot a := \pi(a)$.

(b) Für $G := \mathfrak{S}_{\mathsf{f}}(A)$ und $X := A^2$: definiere $\pi \cdot (a, b) := (\pi(a), \pi(b))$.

(c) Für $(G, \circ)$ und $X := G$: definiere $\pi \cdot g := \pi \circ g$.

(d) Für $(G, \circ)$ und $X := G$: definiere die Aktion '$\star$': $G \times G \to G$ (genannt: *Konjugation* und hier üblicherweise mit $\star$ notiert) durch

$$\pi \star g := \pi \circ g \circ \pi^{-1}.$$

(e) Für $(G, \circ)$ und X beliebig: definiere $\pi \cdot x := x$; genannt die *diskrete Gruppenoperation*.

In Gruppenoperationen lässt sich fast so rechnen wie in der Gruppe G selbst, z. B.:

$$\pi \cdot x = y \qquad \Longleftrightarrow \qquad x = \pi^{-1} \cdot y$$

Definition 2.10. Der *Orbit* von $x \in X$ in einer Gruppenoperation auf X ist die Menge:

$$\mathsf{orb}(x) := \{g \cdot x \mid g \in G\}$$

Wenn X nur endlich viele verschiedene orbits hat, so heißt es *orbit-endlich*.

Intuitiv lassen sich von einem Element $x \in X$ über die Gruppenoperation nur Elemente innerhalb dessen Orbits erreichen. In Abbildung 2 sind die zwei Orbits von A^2 visualisiert (vgl. Beispiel 2.9.(b)). Da G Inverse hat, gilt:

Lemma 2.11. *Die Orbits zweier Elemente $x, y \in X$ sind entweder disjunkt oder identisch.*

Beweis. Fallunterscheidung, ob $g \in G$ mit $x = g \cdot y$ existiert:

1. Es gibt $g \in G$ mit $x = g \cdot y$: Die Orbits sind identisch ($\mathsf{orb}(x) = \mathsf{orb}(y)$), denn

$$x' \in \mathsf{orb}(x) \Rightarrow \exists g' \colon x' = g' \cdot x \Rightarrow x' = g' \cdot (g \cdot y) \Rightarrow x' = (g' \cdot g) \cdot y \Rightarrow x' \in \mathsf{orb}(y).$$

Die andere Richtung $\mathsf{orb}(y) \subseteq \mathsf{orb}(x)$ folgt aus dem gleichen Argument für $y = g^{-1} \cdot x$.

2. Es gibt kein $g \in G$ mit $x = g \cdot y$: Die Orbits sind disjunkt, denn gäbe es $z \in \mathsf{orb}(x) \cap \mathsf{orb}(y)$, dann gäbe es $g_x, g_y \in G$ mit $g_x \cdot x = z = g_y \cdot y$ und damit $x = (g_x^{-1} \cdot g_y) \cdot y$, Widerspruch. □

Lemma 2.12 (Übungsaufgabe). *Eine Gruppenoperation auf X ist genau dann diskret, wenn jeder Orbit genau ein Element hat.*

Beispiel 2.13. Bezeichne $\mathcal{P}X$ die *Potenzmenge* einer Menge X. Eine Aktion von G auf X erweitert sich punktweise zu einer Operation

$$\text{'}\cdot\text{'} \colon G \times \mathcal{P}X \to \mathcal{P}X \qquad \pi \cdot S = \{\pi \cdot x \mid x \in S\}.$$

Für $G := \mathfrak{S}_{\mathsf{f}}(A)$ haben zwei Mengen $S, T \in \mathcal{P}A$ genau dann den selben Orbit, wenn sie die gleiche Mächtigkeit haben. Wenn A unendlich ist, dann ist $\mathsf{orb}(\varnothing) = \{\varnothing\}$ der einzige endliche Orbit in $\mathcal{P}A$.

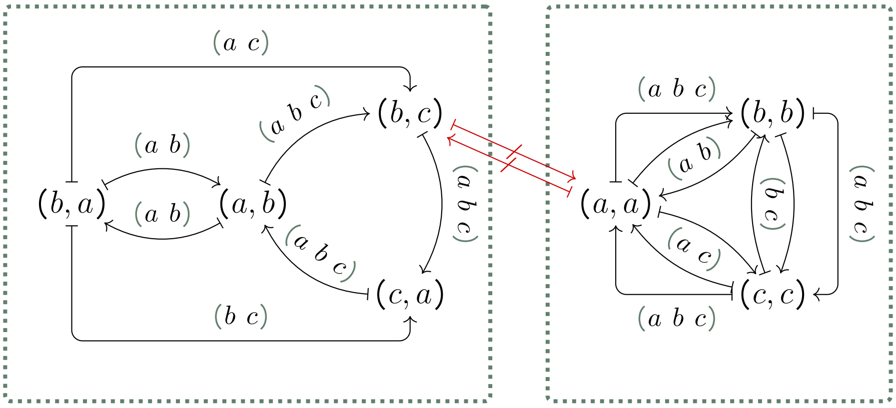


Abbildung 2: Die Gruppenoperation aus Beispiel 2.9.(b) auf A^2 hat zwei Orbits

Beispiel 2.14. Die Operation auf $\mathcal{P}X$ erhält Endlichkeit: wenn $S \in \mathcal{P}X$ endlich ist, so ist auch $\pi \cdot S$ für beliebiges $\pi \in G$ endlich. Daraus ergibt sich eine Gruppenoperation auf der *endlichen Potenzmenge*

$$\mathcal{P}_{\mathsf{f}}(X) := \{S \in \mathcal{P}X \mid S \text{ ist endlich}\},$$

die ebenfalls punktweise definiert ist:

$$`\cdot\text{'}\colon G \times \mathcal{P}_{\mathsf{f}}X \to \mathcal{P}_{\mathsf{f}}X \qquad \pi \cdot S = \{\pi \cdot x \mid x \in S\}.$$

2.2 Strukturerhaltung

Definition 2.15. Eine Abbildung $f\colon X \to Y$ zwischen Gruppenoperationen $(X, \cdot)$ und $(Y, \cdot)$ ist *äquivariant*, wenn gilt:

$$f(\pi \cdot x) = \pi \cdot f(x) \qquad \text{für alle } \pi \in G \text{ und } x \in X.$$

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi\cdot(-)"'] & Y \arrow[d, "\pi\cdot(-)"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

Beispiel 2.16. Die Identität $\mathrm{id}_X\colon (X, \cdot) \to (X, \cdot)$ ist äquivariant. Außerdem sind äquivariante Abbildungen unter Komposition abgeschlossen.

Das kommutierende Quadrat zu Äquivarianz sieht nicht nur aus wie *Natürlichkeit* (siehe Abschnitt 3.4 später), sondern erzwingt ein gewisses Maß an Natürlichkeit (im informellen Sinne) in der Definition äquivarianter Abbildungen:

Beispiel 2.17. Betrachte $G := \mathfrak{S}_{\mathsf{f}}(A)$ und die Gruppenoperationen auf A und A^2 (aus Beispiel 2.9). Die folgenden Abbildungen sind äquivariant:

(a) $\mathsf{pr}_1\colon A^2 \to A$, $\mathsf{pr}_1(a, b) = a$ (die *Projektion*).

(b) $\mathsf{pr}_2\colon A^2 \to A$, $\mathsf{pr}_2(a, b) = b$.

(c) $\Delta\colon A \to A^2$, $\Delta(a) = (a, a)$ (die *Diagonale*).

(d) $\eta\colon A \to \mathcal{P}(A)$, $\eta(a) = \{a\}$.

Lemma 2.18. *Wenn A mindestens drei Elemente hat, dann*

(a) ist id_A die einzige äquivariante Abbildung $A \to A$,

(b) *ist Δ die einzige äquivariante Abbildung $A \to A^2$.*

Beweis.

1. Sei $f\colon A \to A$ äquivariant. Wir zeigen $f = \mathrm{id}_A$ per Extensionalität und per Widerspruch: sei $a \in A$ mit $f(a) \neq a$. Da A mindestens drei Elemente hat, gibt es $b \in A \setminus \{a, f(a)\}$ und damit:

$$b = (f(a)\ \ b) \cdot f(a) = f\big((f(a)\ \ b) \cdot a\big) \overset{a \notin \{f(a), b\}}{=} f(a) \neq b$$

2. Sei $f\colon A \to A^2$ äquivariant und $a \in A$. Da $\mathsf{pr}_1 \circ f\colon A \to A$ äquivariant ist, gilt $\mathsf{pr}_1(f(a)) = \mathrm{id}(a) = a$ wegen Lemma 2.18.(a). Da analog $\mathsf{pr}_2 \circ f\colon A \to A$ äquivariant ist, gilt $\mathsf{pr}_2(f(a)) = \mathrm{id}(a) = a$. Also folgt $f(a) = (a, a) = \Delta(a)$. □

Um zu zeigen, dass auch die beiden Projektionen die einzigen Abbildungen $A^2 \to A$ sind, ist es hilfreich zu untersuchen, wie sich Orbits mit Äquivarianz verträgt. Jede äquivariante Abbildung $f\colon (X, \cdot) \to (Y, \cdot)$ erhält Orbits, denn für alle $x \in X$ gilt:

$$\begin{aligned} \mathsf{orb}(f(x)) &= \{\pi \cdot f(x) \mid \pi \in G\} = \{f(\pi \cdot x) \mid \pi \in G\} \\ &= \{f(y) \mid y \in \mathsf{orb}(x)\} = f[\mathsf{orb}(x)] \end{aligned} \tag{2.1}$$

Außerdem sind äquivariante Abbildungen bereits durch ihr Verhalten auf einem Element pro Orbit eindeutig festgelegt:

Lemma 2.19. *Äquivariante Abbildungen $f, g\colon (X, \cdot) \to (Y, \cdot)$ sind genau dann gleich ($f = g$), wenn es pro Orbit $O \subseteq X$ von X ein $x \in O$ gibt mit $f(x) = g(x)$.*

Beweis. Nachdem Orbits nicht leer sind, ist die Richtung „genau dann" trivial. Betrachte $z \in X$ für die umgekehrte Richtung. Per Annahme gibt es ein $x \in \mathsf{orb}(z)$ mit $f(x) = g(x)$, also $x = \pi \cdot z$ für ein $\pi \in G$ und damit:

$$f(z) = f(\pi^{-1} \cdot x) = \pi^{-1} \cdot f(x) = \pi^{-1} \cdot g(x) = g(\pi^{-1} \cdot x) = g(z).$$ □

Lemma 2.20. *Wenn A mindestens vier Elemente hat, dann sind pr_1 und pr_2 die einzigen äquivarianten Abbildungen $A^2 \to A$.*

Beweis. Sei $f\colon A^2 \to A$ äquivariant. Da A^2 zwei Orbits hat, genügt es nach Lemma 2.19, je ein Element pro Orbit zu betrachten:

- $(a, a) \in A^2$: Hier ist zwingend $f(a, a) = a$, da $f \circ \Delta\colon A \to A$ äquivariant ist und daher zwingend $f \circ \Delta = \mathrm{id}_A$ (Lemma 2.18.(a)) und $f(a, a) = \mathsf{pr}_1(a, a) = \mathsf{pr}_2(a, a)$.
- $(a, b) \in A^2$ mit $a \neq b$:
  - Wenn $f(a, b) = a$, so ist $f(a, b) = \mathsf{pr}_1(a, b)$ und damit $f = \mathsf{pr}_1$.
  - Wenn $f(a, b) = b$, so ist $f(a, b) = \mathsf{pr}_2(a, b)$ und damit $f = \mathsf{pr}_2$.
  - Für $f(a, b) \notin \{a, b\}$ leiten wir einen Widerspruch her: Für $c := f(a, b)$ existiert $d \in A \setminus \{a, b, c\}$ weil A mindestens vier Elemente hat.

$$d \neq c = f(a, b) = f\big((c\ \ d) \cdot (a, b)\big) = (c\ \ d) \cdot f(a, b) = (c\ \ d) \cdot c = d.$$ □

Lemma 2.21. *Sei $P := \big\{\{a,b\} \mid a,b \in A, a \neq b\big\}$ die Menge der ungeordneten Paare. Wenn es eine äquivariante Abbildung $X \to A$ gibt, dann ist $|A| \in \{0,1,3\}$.*

Beweis. Sei $f\colon X \to A$ äquivariant. Angenommen, A hat mehr als nur ein Element: $a \neq b$, dann gilt für $c := f(\{a,b\})$:

$$(a\,b) \cdot c = (a\,b) \cdot f\big(\{a,b\}\big) = f\big((a\,b) \cdot \{a,b\}\big) = f\big(\{a,b\}\big) = c.$$

Das ist nur möglich, wenn $a \neq c \neq b$, also wenn A mindestens drei Elemente hat. Dass A mehr als drei Elemente hat, ist hingegen nicht möglich, denn die Existenz eines vierten $d \in A \setminus \{a,b,c\}$ führt zum Widerspruch

$$d = (c\,d) \cdot c = f\big((c\,d) \cdot \{a,b\}\big) = f\big(\{a,b\}\big) = c \qquad \square$$

Bemerkung 2.22. Für Mächtigkeiten 0, 1 und 3 gibt es in der Tat äquivariante Abbildungen:

- Für $A = \varnothing$ und $|A| = 1$ ist P schlicht leer.
- Für $|A| = 3$ schickt $f\colon P \to A$ jede zweielementige Menge $S \subseteq A$, $|S| = 2$ auf das einzige Element $f(S) \in A$ mit $f(S) \notin S$.

Definition 2.23. Für Gruppenoperationen $(X, \cdot)$ und $(Y, \cdot)$ trägt die Menge *aller* Abbildungen $X \to Y$, geschrieben Y^X, eine kanonische Gruppenoperation $(Y^X, \star)$:

$$Y^X := \{f\colon X \to Y \mid f \text{ beliebige Abbildung}\} \qquad \pi \star f \;:=\; \big(x \mapsto \pi \cdot f(\pi^{-1} \cdot x)\big)$$

Überraschenderweise enthält Y^X alle Abbildungen, und nicht nur die äquivarianten:

Lemma 2.24 (Übungsaufgabe). *Eine Abbildung $f \in (Y^X, \star)$ ist genau dann äquivariant, wenn $\mathsf{orb}(f) = \{f\}$.*

Beispiel 2.25. Betrachtet man $n \in \mathbb{N}$ als Menge $n = \{0, \ldots, n-1\}$ mit diskreter Gruppenoperation, so ist

$$\underbrace{(X, \cdots) \times \cdots \times (X, \cdots)}_{n\text{-viele}} \;\cong\; (X, \cdots)^n$$

3 Kategorientheorie

Im folgenden werden einige Konzepte aus der Kategorientheorie erklärt, anhand derer sich Unterschiede und Gemeinsamkeiten zwischen Mengen, G-Sets und nominalen Mengen aufzeigen lassen. In der Definition von *Kategorie* ist eines der Daten (im Allgemeinen) keine Menge, sondern eine *Klasse*, deshalb kommt hier ein kleiner Exkurs zum Thema Mengenlehre:

3.1 Axiomatische Mengenlehre

Mengenlehre ist lediglich eine Theorie zu Prädikatenlogik (erster Stufe; FOL) zur Signatur bestehend (neben Gleichheit =) aus nur einem zweistelligen Prädikat:

$$\in$$

Alle Axiome und alle bewiesenen Sätze sind also strenggenommen einfach nur prädikatenlogische Formeln über genau dieser Signatur. Die heutzutage übliche Axiomatisierung von Ernst Zermelo und Abraham Frankel (ZF bzw. ZFC = ZF + Auswahlaxiom) besteht aus 8 Axiomen. Davon sind zwei eigentlich Axiom-Schemata (Axiome, die parametrisch in einer FO-Formel sind). Das Extensionalitäts-Axiom besagt, dass zwei Mengen genau dann gleich sind, wenn sie die gleichen Elemente haben:

$$\forall x.\forall y.\ x = y \ \leftrightarrow\ \forall e.\ e \in x \leftrightarrow e \in y.$$

Die meisten anderen Axiome beschreiben, wie man neue Mengen bauen kann und verwenden dabei implizit Extensionalität, indem sie lediglich spezifizieren, welche Elemente die neu gebauten Mengen haben. Beispielsweise ist das Axiom der (ungeordneten) Paarmenge (engl.: pairing):

$$\forall a, b.\exists p.(x \in p \leftrightarrow (x = a \lor x = b))$$

Für den Zeugen von p schreibt man üblicherweise $\{a, b\}$. Das Axiom der Existenz von Potenzmengen ist die Formel:

$$\forall x.\exists p.\forall s.(s \in p \leftrightarrow \forall e.e \in s \to e \in x)$$

Für den Zeugen von p schreibt man $\mathcal{P}(x)$. Eines der Axiom-Schemata ist die Mengen-*Komprehension* (oder *Aussonderung*), das besagt, dass wann immer man eine Menge x gegeben hat, dann gibt es auch eine Teilmenge $y \subseteq x$, die ein gewünschtes Prädikat φ erfüllen:

$$\forall x.\ \exists y.\ \forall e.\ e \in y \ \leftrightarrow\ e \in x \land \varphi(e) \qquad \text{für beliebige FO-Formel } \varphi.$$

Für y schreibt man üblicherweise:

$$\{e \in x \mid \varphi(e)\}$$

Hierbei schreiben wir $\varphi(e)$, um anzudeuten, dass φ von e abhängt und dass wir statt e auch mal andere Variablennamen verwenden werden.

Bemerkung 3.1 (Mengen vs. Klassen)**.** Alles im Modell der Mengentheorie ist eine Menge; deshalb bezeichnen alle Variablen *immer* Mengen (z. B. x, p, s, e im Axiom oben). Im Umkehrschluss bedeutet das: es ist nicht möglich, in ZF(C) explizit über (echte) Klassen zu quantifizieren. Stattdessen verstehen wir Klassen φ einfach als Formel mit einem Parameter

$\varphi(x)$, die angibt, welche Mengen in der Klasse enthalten sind. Also $e \in \varphi$ genau dann, wenn $\varphi(e)$ gilt, und man schreibt

$$\{e \mid \varphi(e)\}$$

für die entsprechende Klasse. Beispiele:

(a) Die Klasse aller Mengen (also **obj** Set später) ist geben durch $\varphi(x) := \top$.

(b) Die Klasse aller Paare von Mengen: $\varphi(x) := \exists \ell. \exists r. x = (\ell, r)$. Hier ist (ℓ, r) nur die übliche Notation für $(\ell, r) := \{\{\ell\}, \{\ell, r\}\}$ (vgl. [7, „Pairing"]).

(c) Für jede Menge s erhält man auch eine Klasse $\varphi(x) := (x = s)$.

(d) Die Klasse aller Gruppenoperation zu G:

$$\varphi(x) \;:=\; \exists X. \exists m.\; x = (X, m) \;\wedge\; m \in (G \times X \to X) \;\wedge\; \cdots$$

(e) Die Klasse aller Mengen aus höchstens zwei Elementen:

$$\varphi(x) \;:=\; \exists a, b.\, \forall e.\; e \in x \quad \to \quad e = a \vee e = b$$

(f) Die Klasse aller natürlichen Zahlen:

$$\varphi(x) \;:=\; x \in \mathbb{N}$$

(g) Die Klasse aller endlichen Mengen:

$$\varphi(x) \;:=\; \exists n, R.\; n \in \mathbb{N} \;\wedge\; R \in (x \rightarrowtail n)$$

3.2 Kategorien

Definition 3.2. Eine *Kategorie* $\mathcal{C}$ enthält die folgenden Daten:

(a) Eine Klasse **obj** $\mathcal{C}$, genannt *Objekte* von $\mathcal{C}$. Wir schreiben vereinfacht $X \in \mathcal{C}$ statt $X \in$ **obj** $\mathcal{C}$.

Eine Kategorie $\mathcal{C}$ heißt *klein*, wenn **obj** $\mathcal{C}$ eine Menge ist.

(b) Für je zwei Objekte $X, Y \in$ **obj** $\mathcal{C}$ eine Menge $\mathcal{C}(X, Y)$, genannt *Hom-Menge*. Die Elemente von $\mathcal{C}(X, Y)$ heißen *Morphismen* (oder auch *Pfeile*)

(c) Für jedes Objekt $X \in$ **obj** $\mathcal{C}$ ein Element $\mathrm{id}_X \in \mathcal{C}(X, X)$, genannt *Identität* auf X.

(d) Für Objekte $X, Y, Z \in$ **obj** $\mathcal{C}$ eine Komposition:

$$\circ\colon \mathcal{C}(Y, Z) \times \mathcal{C}(X, Y) \longrightarrow \mathcal{C}(X, Z)$$

... und hat folgende Eigenschaften:

(e) Für alle $X, Y \in$ **obj** $\mathcal{C}$ und $f \in \mathcal{C}(X, Y)$ gilt:

$$\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X$$

(f) Komposition ist assoziativ: Für alle $W, X, Y, Z \in$ **obj** $\mathcal{C}$, $f \in \mathcal{C}(W, X)$, $g \in \mathcal{C}(X, Y)$ und $h \in \mathcal{C}(Y, Z)$ gilt:

$$(h \circ g) \circ f = h \circ (g \circ f)$$

$$\underbrace{\begin{array}{c} X \xrightarrow{\quad f \quad} X' \xrightarrow{\quad f' \quad} X'' \\ Y \xrightarrow{\quad g \quad} Y' \xrightarrow{\quad g' \quad} Y'' \end{array}} \qquad \begin{array}{l} \text{in } \mathcal{C} \\ \text{in } \mathcal{D} \end{array}$$

$$\begin{tikzcd} (X,Y) \arrow[r, "{(f,g)}"] \arrow[rr, bend right, "{(f',g')\circ(f,g) \,:=\, (f'\circ f,g'\circ g)}"'] & (X',Y') \arrow[r, "{(f',g')}"] & (X'',Y'') & \text{in } \mathcal{C} \times \mathcal{D} \end{tikzcd}$$

Abbildung 3: Komposition in der Produktkategorie $\mathcal{C} \times \mathcal{D}$

Notation 3.3. In der Regel schreiben wir $\cdot$ statt $\circ$. Wenn $\mathcal{C}$ aus dem Kontext hervorgeht, schreiben wir

$$f\colon X \to Y \qquad \text{statt} \qquad f \in \mathcal{C}(X,Y)$$

Beispiel 3.4. Beispiele für Kategorien:

(a) Set: **obj** Set ist die Klasse der Mengen (also die größte Klasse). Und $\mathsf{Set}(X,Y)$ ist die Menge der Abbildungen $X \to Y$. Komposition ist die übliche Funktionskomposition, mit der Identitätsabbildung als neutrales Element.

(b) Jede Gruppe G ist gleichzeitig eine Kategorie bestehend aus:

- **obj** $= \{\bullet\}$ – eine beliebige einelementige Menge
- $\hom(\bullet,\bullet) = G$ – die (Endo-)Hom-Menge auf dem einzigen Objekt $\bullet$ enthält genau die Gruppenelemente
- $\mathrm{id}_\bullet = e$ – die Identität auf dem einzigen Objekt $\bullet$ ist das neutrale Element von G

(c) G-Set: **obj** G-Set enthält Tupel $(X,\cdot)$ bestehend aus einer Menge X und einer Gruppenoperation $\cdot$ von G auf X. Die Hom-Menge $G\text{-}\mathsf{Set}\big((X,\cdot),(Y,\cdot)\big)$ ist die Menge der äquivarianten Abbildungen $(X,\cdot) \to (Y,\cdot)$. Komposition und neutrales Element sind Funktionskomposition und Identität (vgl. Beispiel 2.16).

Beispiel 3.5. Konstruierte Kategorien:

(a) Für jede Kategorie $\mathcal{C}$ ist die *duale Kategorie* $\mathcal{C}^{\mathsf{op}}$ gegeben durch

- **obj** $\mathcal{C}^{\mathsf{op}}$:= **obj** $\mathcal{C}$
- $\mathcal{C}^{\mathsf{op}}(X,Y) := \mathcal{C}(Y,X)$
- Identität und Komposition sind wie in $\mathcal{C}$: id_X in $\mathcal{C}^{\mathsf{op}}$ ist identisch zu id_X in $\mathcal{C}$. Für $f \in \mathcal{C}^{\mathsf{op}}(X,Y)$, $g \in \mathcal{C}^{\mathsf{op}}(Y,Z)$ ist $g \circ f$ in $\mathcal{C}^{\mathsf{op}}$ gegeben durch $f \circ g$ in $\mathcal{C}$.

(b) Für Kategorien $\mathcal{C}$ und $\mathcal{D}$ ist die *Produktkategorie* $\mathcal{C} \times \mathcal{D}$ gegeben durch:

- **obj**$(\mathcal{C} \times D) := \{(X,Y) \mid X \in \mathcal{C}, Y \in \mathcal{D}\}$ (Wenn **obj** $\mathcal{C}$ durch $\varphi_{\mathcal{C}}$ und **obj** $\mathcal{D}$ durch $\varphi_{\mathcal{D}}$ beschrieben werden, dann ist die Klasse **obj**$(\mathcal{C} \times D)$ durch die Formel $\varphi(t) = \exists x,y.t = \{\{x\},\{x,y\}\} \wedge \varphi_{\mathcal{C}}(x) \wedge \varphi_{\mathcal{D}}(y)$ beschrieben)
- $(\mathcal{C} \times \mathcal{D})\big((X,Y),(X',Y')\big) := \mathcal{C}(X,X') \times \mathcal{D}(Y,Y')$
- $\mathrm{id}_{(X,Y)} := (\mathrm{id}_X, \mathrm{id}_Y)$
- $(f',g') \circ (f,g) := (f' \circ f, g' \circ g)$ (siehe Abbildung 3)

Duale Kategorien und Produktkategorien geben für sich alleine eher selten Einsichten, sondern werden eher dafür genutzt, unterschiedliche Kategorien miteinander in Beziehung zu setzen:

3.3 Funktoren

Die strukturerhaltenden Abbildungen zwischen Kategorien sind Funktoren:

Definition 3.6. Ein *Funktor* $F\colon \mathcal{C} \to \mathcal{D}$ enthält die Daten:

(a) Einer Klassenfunktion $\mathbf{obj}\,\mathcal{C} \to \mathbf{obj}\,\mathcal{D}$, die jedes Objekt $X \in \mathcal{C}$ auf ein Objekt $FX \in \mathcal{D}$ abbildet.

(b) Für Objekte $X, Y \in \mathcal{C}$ eine Funktion $\mathcal{C}(X,Y) \to \mathcal{D}(FX, FY)$, üblicherweise auch mit F bezeichnet:

$$\big(f\colon X \to Y \text{ in } \mathcal{C}\big) \quad \mapsto \quad \big(Ff\colon FX \to FY \text{ in } \mathcal{D}\big)$$

... und hat folgende Eigenschaften:

(c) $F\mathrm{id}_X = \mathrm{id}_{FX}$ für alle $X \in \mathcal{C}$.

(d) $F(g \circ f) = Fg \circ Ff$ für alle $f\colon X \to Y$ und $g\colon Y \to Z$ in $\mathcal{C}$.

Beispiel 3.7. (a) Der *Vergissfunktor* $U\colon G\text{-}\mathsf{Set} \to \mathsf{Set}$ schickt jede Gruppenoperation $(X, \cdot)$ auf ihre unterliegende Menge X und *vergisst* die Äquivarianz der Morphismen:

$$U(X,\cdot) = X \qquad U(\overbrace{f}^{(X,\cdot)\to(Y,\cdot)}) = f \in \mathsf{Set}(X,Y)$$

(b) Für jedes $(Y,\cdot) \in G\text{-}\mathsf{Set}$ erhalten wir einen Funktor

$$(Y,\cdot) \times (-)\colon G\text{-}\mathsf{Set} \to G\text{-}\mathsf{Set} \qquad (Y,\cdot) \times (X,\cdot) := (X \times Y, \cdot)$$

mit der Komponentenweisen Gruppenaktion

$$\pi \cdot (y,x) := (\pi \cdot y, \pi \cdot x)$$

(c) Das kartesische Produkt $\times$ ist funktoriell, also ein Funktor von der Produktkategorie nach Set:

$$`\times\text{'}\colon \mathsf{Set} \times \mathsf{Set} \to \mathsf{Set} \qquad `\times\text{'}(A,B) = A \times B$$

Abbildungen werden komponentenweise angewandt:

$$`\times\text{'}((f,g)\colon (A,B) \to (C,D)) = \underbrace{\big((a,b) \mapsto (f(a), f(b))\big)}_{\in\ (A\times B \to C \times D)}$$

(d) Für jede Kategorie $\mathcal{C}$ gibt es einen *Identitätsfunktor* $\mathrm{Id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ mit $\mathrm{Id}_{\mathcal{C}}(X) = X$ und $\mathrm{Id}_{\mathcal{C}}(f\colon X \to Y) = f$.

(e) Für jedes Objekt $X \in \mathcal{C}$ ist $\mathcal{C}(X,-)\colon \mathcal{C} \to \mathsf{Set}$ ein Funktor, genannt (kovarianter) *Hom-Funktor*. Der Hom-Funktor schickt ein Objekt $Y \in \mathcal{C}$ auf das Objekt $\mathcal{C}(X,Y) \in \mathsf{Set}$ und jeden Morphismus $f\colon Y \to Z$ in $\mathcal{C}$ auf die Abbildung

$$\mathcal{C}(X,f)\colon\ \mathcal{C}(X,Y) \to \mathcal{C}(X,Z) \qquad g \mapsto g \circ f$$

Theorem 3.8. *Wenn man eine Gruppe G als Kategorie betrachtet, dann sind die Gruppenoperationen (also G-Sets) genau die Funktoren $G \to \mathsf{Set}$.*

Beweis. Die Daten eines Funktors $F\colon G \to \mathsf{Set}$ sind in 1:1-Korrespondenz zu den Daten einer Gruppenoperation $(X, \cdot)$:

1. Da die Kategorie G nur ein Objekt $\bullet$ hat, entspricht die Wahl $F(\bullet) \in \mathbf{obj}\,\mathsf{Set}$ genau der Wahl einer Trägermenge X. (Im Folgenden: $X = F(\bullet)$)
2. Die Abbildung
$$\underbrace{\hom_G(\bullet, \bullet)}_{= G} \to \hom_{\mathsf{Set}}(X, X)$$
eines solchen Funktors entspricht genau einer Abbildung
$$G \times X \to X.$$
In die eine Richtung setzt man
$$g \cdot x := \underbrace{F(g\colon \bullet \to \bullet)}_{F\bullet \to F\bullet}(x)$$
und in die andere entsprechend $Fg := (x \mapsto g \cdot x)$.
3. Die (einzige) Identität $\mathrm{id}_\bullet\colon \bullet \to \bullet$, also das neutrale Element der Gruppe $\mathrm{id}_\bullet \in G$ erhält ($F\mathrm{id}_\bullet = \mathrm{id}_X$) ist äquivalent dazu, dass $\mathrm{id}_\bullet \cdot x = x$ für alle $x \in X$.
4. Dass der Funktor die Komposition von Morphismen erhält, also $F(g \cdot h) = Fg \circ Fh$, ist äquivalent zum Axiom der Gruppenoperation $(g \cdot h) \cdot x = g \cdot (h \cdot x)$ für alle $x \in X$:
$$\begin{aligned} & F(g \cdot h) = Fg \circ Fh \\ \iff \quad & F(g \cdot h)(x) = Fg(Fh(x)) \quad \text{für alle } x \in X \\ \iff \quad & (g \cdot h) \cdot x = g \cdot (h \cdot x) \quad \text{für alle } x \in X \end{aligned}$$ □

Definition 3.9. Zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ heißen *isomorph*, $\mathcal{C} \cong \mathcal{D}$, wenn es Funktoren $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{C}$ gibt mit $G \circ F = \mathrm{Id}_{\mathcal{C}}$ und $F \circ G = \mathrm{Id}_{\mathcal{D}}$.

3.4 Natürliche Transformationen

Die strukturerhaltenden Abbildungen zwischen Funktoren sind natürliche Transformationen:

Definition 3.10. Für Funktoren $F, G\colon \mathcal{C} \to \mathcal{D}$ besteht eine *natürliche Transformation* $\alpha\colon F \to G$ aus eine ($\mathbf{obj}\,\mathcal{C}$-indizierten) Familie von $\mathcal{D}$-Morphismen

$$\alpha_X\colon FX \to GX \qquad \text{in } \mathcal{D} \qquad \text{für jedes } X \in \mathbf{obj}\,\mathcal{C}$$

sodass für jeden Morphismus $h\colon X \to Y$ in $\mathcal{C}$ das folgende Diagramm in $\mathcal{D}$ kommutiert:

$$\begin{tikzcd} FX \arrow[r, "\alpha_X"] \arrow[d, "Fh"'] & GX \arrow[d, "Gh"] \\ FY \arrow[r, "\alpha_Y"] & GY \end{tikzcd} \qquad (\text{in } \mathcal{D})$$

Beispiel 3.11. Auf Set (und G-Set) ist das Produkt einer Menge mit sich selbst ein Funktor $Q\colon \mathsf{Set} \times \mathsf{Set} \to \mathsf{Set}$ (auch genannt *Quadratfunktor*): $Q(X) = X \times X$ und $Q(f) = f \times f$ für Abbildungen $f\colon X \to X'$. Die Projektionen und die Diagonale sind natürliche Transformationen:

$$\Delta\colon \mathrm{Id}_{\mathsf{Set}} \longrightarrow Q \qquad \mathsf{pr}_1, \mathsf{pr}_2\colon Q \longrightarrow \mathrm{Id}_{\mathsf{Set}}.$$

Definition 3.12. Die *Funktorkategorie* $[\mathcal{C}, \mathcal{D}]$ (für Kategorien $\mathcal{C}$, $\mathcal{D}$, wobei $\mathcal{C}$ klein) enthält:

(a) Die Objekte $\mathbf{obj}[\mathcal{C}, \mathcal{D}]$ sind die Funktoren $\mathcal{C} \to \mathcal{D}$.

(b) Die Morphismen $[\mathcal{C}, \mathcal{D}](F, G)$ (zwischen Funktoren $F, G\colon \mathcal{C} \to \mathcal{D}$) sind die natürlichen Transformationen $\alpha\colon F \to G$.

Theorem 3.13 (Übungsaufgabe)**.** *Die Kategorien G-Set und $[G, \mathsf{Set}]$ sind isomorph.*

Daraus ergibt sich:

Beispiel 3.14. Die äquivarianten Abbildungen $(X, \cdot) \to (Y, \cdot)$ zwischen G-Sets $(X, \cdot)$ und $(Y, \cdot)$ entsprechen genau den natürlichen Transformationen $(X, \cdot) \to (Y, \cdot)$ zwischen den Funktoren $(X, \cdot), (Y, \cdot)\colon G \to \mathsf{Set}$.

4 Nominale Mengen

Annahme 4.1. Von nun an sei eine unendliche Menge $\mathbb{A}$ (üblicherweise abzählbar) gegeben, die wir als *Atome* bezeichnen. Wenn nicht anders vermerkt, betrachten wir Gruppenoperationen zur Gruppe $G := \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$ der endlichen Permutationen.

4.1 Support

Definition 4.2. Sei X eine Menge mit Gruppenoperation. Eine Menge $S \subseteq \mathbb{A}$ ist ein *Support* eines Elements $x \in X$, wenn für alle $\pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$ gilt:

$$\pi(a) = a \quad \text{für alle } a \in S \qquad \Longrightarrow \qquad \pi \cdot x = x$$

Da wir die linke Seite der Implikation häufiger brauchen, definieren wir die Abkürzung:

$$\mathsf{Fix}\colon \mathcal{P}\mathbb{A} \to \mathcal{P}(\mathfrak{S}_{\mathsf{f}}(\mathbb{A})) \qquad \mathsf{Fix}(S) = \{\pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A}) \mid \pi(a) = a \text{ für alle } a \in S\}.$$

Somit ist S ein Support von x, wenn $\pi \cdot x = x$ für alle $\pi \in \mathsf{Fix}(S)$.

Definition 4.3. Eine Gruppenoperation $(X, \cdot)$ heißt *nominal*, wenn jedes Element einen endlichen Support hat.

Definition 4.4. Die Kategorie der *nominalen Mengen* (Nom) ist die volle Unterkategorie von $\mathfrak{S}_{\mathsf{f}}(\mathbb{A})$-$\mathsf{Set}$, erzeugt durch die nominalen Gruppenoperationen.

Explizit ausgeschrieben bedeutet das:

- $\mathbf{obj}\,\mathsf{Nom}$ enthält genau die Gruppenoperationen $(X, \cdot)$, in der jedes $x \in X$ einen endlichen Support hat.
- $\mathsf{Nom}\big((X, \cdot), (Y, \cdot)\big)$ ist die Menge der äquivarianten Abbildungen $(X, \cdot) \to (Y, \cdot)$.

Beispiel 4.5. Die Menge $(\mathbb{A}, \cdot)$ ist nominal, denn für $a \in \mathbb{A}$ ist $\{a\}$ ein endlicher Support: für alle $\pi \in \mathsf{Fix}(\{a\})$ gilt $\pi \cdot a = a$. Es ist auch jede Obermenge von $\{a\}$ ein Support von a, da Fix antiton ist:

$$S \subseteq T \quad \Longrightarrow \quad \mathsf{Fix}(S) \supseteq \mathsf{Fix}(T) \quad \text{für alle } S, T \in \mathcal{P}\mathbb{A}$$

Insbesondere ist die gesamte Menge $\mathbb{A}$ stets ein Support eines jeden Elements $x \in X$ einer Gruppenoperation auf X.

Beispiel 4.6. Für $(\mathbb{A}^2, \cdot)$ hat $(a, b) \in \mathbb{A}^2$ die Menge $\{a, b\}$ (und jede ihrer Obermengen) als Support: für alle $\pi \in \mathsf{Fix}(\{a, b\})$ gilt sowohl $\pi \cdot a = a$ als auch $\pi \cdot b = b$ und damit

$$\pi \cdot (a, b) = (\pi \cdot a, \pi \cdot b) = (a, b).$$

Nicht alle Gruppenoperationen sind nominal: in der Menge der Streams $\mathbb{A}^\omega$ (für $\omega := \mathbb{N}$) mit der punktweisen Operation hat ein Stream genau dann einen endlichen Support, wenn in ihm (genauer: seinem Bild) nur endlich viele verschiedene Atome vorkommen.

Notation 4.7. Das *Bild* einer Abbildung $f\colon X \to Y$ wird mit $\mathrm{Im}(f)$ bezeichnet:

$$\mathrm{Im}(f) = \{y \in Y \mid \exists x \in X\colon y = f(x)\}$$

Lemma 4.8. *$f \in \mathbb{A}^\omega$ hat genau dann einen endlichen Support, wenn $\mathrm{Im}(f)$ endlich ist.*

Beweis. Wenn $\mathrm{Im}(f)$ endlich ist, dann ist $\mathrm{Im}(f)$ ein Support von f, denn für alle $\pi \in \mathsf{Fix}(\mathrm{Im}(f))$ gilt:

$$\pi \cdot f = \pi \cdot (k \mapsto f(k)) = (k \mapsto \pi \cdot f(k)) \overset{\pi \in \mathsf{Fix}(\mathrm{Im}(f))}{=} (k \mapsto f(k)) = f.$$

Wenn $\mathrm{Im}(f) \subseteq \mathbb{A}$ unendlich ist, dann kann es keinen endlichen Support $S \subseteq \mathbb{A}$ von f geben: Gäbe es einen solchen, dann ist $\mathrm{Im}(f) \setminus S$ unendlich und insbesondere nichtleer. Sei also $k \in \mathbb{N}$ mit $f(k) \notin S$ und sei $b \in \mathbb{A} \setminus (S \cup \{f(k)\})$. Dann ist $(f(k)\ \ b) \in \mathsf{Fix}(S)$ und damit

$$f = (f(k)\ \ b) \cdot f$$

und weiter

$$f(k) = ((f(k)\ \ b) \cdot f)(k) = (f(k)\ \ b) \cdot f(k) = b \neq f(k) \qquad \square$$

Wenn ein Element $x \in (X, \cdot)$ (irgend)einen endlichen Support, dann lässt sich daraus ein *kleinster* endlicher Support konstruieren, indem man mögliche endliche Supports miteinander schneidet, denn endliche Supports sind unter Schnitt abgeschlossen:

Lemma 4.9. *Wenn $S, T \subseteq \mathbb{A}$ endliche Supports von $x \in X$ sind, dann ist auch $S \cap T$ ein Support von x.*

Die Beweisidee ist: wir werden ein gegebenes $\pi \in \mathsf{Fix}(S \cap T)$ so mit einer weiteren Permutation $\sigma \in \mathsf{Fix}(T)$ konjugieren, dass die Komposition in $\mathsf{Fix}(S)$ liegt:

Beweis. Sei $\pi \in \mathsf{Fix}(S \cap T)$. Da π eine endliche Permutation ist, ist $\mathsf{supp}(\pi)$ (wie explizit in Beispiel 2.2 definiert) eine endliche Menge. Da $\mathbb{A}$ unendlich ist, gibt es eine injektive Abbildung:

$$S \setminus T \overset{m}{\rightarrowtail} \mathbb{A} \setminus (\mathsf{supp}(\pi) \cup S \cup T)$$

Diese erweitern wir auf $\mathbb{A}$:

$$\sigma\colon \mathbb{A} \to \mathbb{A} \qquad \sigma(a) = \begin{cases} m(a) & \text{falls } a \in S \setminus T \\ b & \text{falls } a \in \mathrm{Im}(m) \text{ und } m(b) = a \\ a & \text{sonst.} \end{cases}$$

Da $S \setminus T$ und $\mathrm{Im}(m)$ disjunkt sind und da m injektiv ist, ist σ wohldefiniert. Aus der Injektivität von m folgt außerdem die Bijektivität von σ; und das Inverse ist sogar σ selbst: $\sigma \cdot \sigma = \mathrm{id}_{\mathbb{A}}$. Da $S \setminus T$ endlich ist, hat σ endlichen Support, also $\sigma \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$. Die Definition von σ wurde so gewählt, dass gilt:

1. $\sigma \in \mathsf{Fix}(T)$: Sei $a \in T$, so ist $a \notin S \setminus T$ und $a \notin \mathrm{Im}(m)$, also $\sigma(a) = a$.
2. $\sigma\pi\sigma \in \mathsf{Fix}(S)$: Sei $a \in S$. Fallunterscheidung, ob a auch in T ist:
   - Falls $a \in T$ und damit $a \in S \cap T$, so ist direkt $\sigma(a) = a$ und
     $$\sigma \cdot \pi \cdot \sigma a = \sigma \cdot \pi \cdot a \overset{\pi \in \mathsf{Fix}(S \cap T)}{=} \sigma \cdot a = a$$
   - Falls $a \notin T$, so ist $\sigma(a) = m(a) \notin \mathsf{supp}(\pi)$ und damit $\pi(\sigma(a)) = \sigma$. Schließlich:
     $$\sigma \cdot \pi \cdot \sigma a = \sigma \cdot \sigma a = \mathrm{id} \cdot a = a$$

Damit können wir jetzt $\pi \cdot x = x$ verifizieren:

$$\begin{array}{rcrcr} \sigma \in \mathsf{Fix}(T) & \& & T \text{ ist Support von } x & \Longrightarrow & \sigma \cdot x = x \\ \sigma \cdot \pi \cdot \sigma \in \mathsf{Fix}(S) & \& & S \text{ ist Support von } x & \Longrightarrow & \sigma \cdot \pi \cdot \sigma \cdot x = x \end{array}$$

$$\pi \cdot x = \sigma \cdot \sigma \cdot \pi \cdot \sigma \cdot \sigma \cdot x = \sigma \cdot \sigma \cdot \pi \cdot \sigma \cdot x = \sigma \cdot x = x$$

Also ist $S \cap T$ ein Support von x. □

Definition 4.10. Für eine nominale Menge $(X, \cdot)$ sei $\mathsf{supp}_X\colon X \to \mathcal{P}_{\mathsf{f}}(A)$ definiert durch:

$$\begin{aligned} \mathsf{supp}_X(x) &= \bigcap \{S \in \mathcal{P}_{\mathsf{f}}(\mathbb{A}) \mid S \text{ ist Support von } x\} \\ &= \{a \in \mathbb{A} \mid \text{für alle endlichen Supports } S \text{ von } x \text{ gilt } a \in S\} \end{aligned}$$

Wenn X aus dem Kontext klar ist, schreiben wir supp statt supp_X. Die Menge $\mathsf{supp}_X(x) \subseteq \mathbb{A}$ ist stets endlich, da der Schnitt nie leer ist, da jedes $x \in X$ (mindestens) einen endlichen Support hat.

Üblicherweise heißt $\mathsf{supp}_X(x)$ schlicht ***der*** *Support* von x:

Theorem 4.11. *In nominalen Mengen X ist $\mathsf{supp}_X(x)$ der kleinste endliche Support von x.*

Beweis. Es sind zwei Eigenschaften zu überprüfen:

1. $\mathsf{supp}(x)$ ist ein endlicher Support von x: Da $(X, \cdot)$ nominal ist, hat x einen endlichen Support $T \in \mathcal{P}_\mathsf{f}(\mathbb{A})$. Damit vereinfacht sich der Schnitt in der Definition von $\mathsf{supp}(x)$ zu:

$$\mathsf{supp}_X(x) = \bigcap \{S \in \mathcal{P}_\mathsf{f}(\mathbb{A}) \mid S \subseteq T, S \text{ ist Support von } x\}$$

   Da T endlich ist, gibt es nur endlich viele Teilmengen $S \subseteq T$, die Support von x sind. Nach Lemma 4.9 ist deren Schnitt $\mathsf{supp}(x) \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ ebenfalls ein Support von x.

2. $\mathsf{supp}(x)$ ist Teilmenge eines jeden endlichen Support von x: Das folgt direkt aus der Definition von $\mathsf{supp}(x)$ als Schnitt. □

Äquivariante Abbildungen erhalten Supports:

Lemma 4.12. *Sei $f\colon (X, \cdot) \to (Y, \cdot)$ eine äquivariante Abbildung zwischen Gruppenoperationen. Wenn $S \subseteq \mathbb{A}$ ein Support von $x \in X$ ist, dann ist S auch ein Support von $f(x)$.*

Beweis. Sei $x \in X$ und $S \subseteq \mathbb{A}$ ein Support von $x \in X$. Dann folgt für alle $\pi \in \mathsf{Fix}(S)$, dass $\pi \cdot x = x$ und damit auch:

$$\pi \cdot f(x) = f(\pi \cdot x) = f(x)$$ □

Korollar 4.13. *Wenn $f\colon (X, \cdot) \to (Y, \cdot)$ eine äquivariante Abbildung zwischen nominalen Mengen ist, dann gilt $\mathsf{supp}_Y(f(x)) \subseteq \mathsf{supp}_X(x)$ für alle $x \in X$.*

$$\begin{tikzcd}
(X, \cdot) \arrow[rr, "f"] \arrow[dr, "\mathsf{supp}_X"'] & \supseteq & (Y, \cdot) \arrow[dl, "\mathsf{supp}_Y"] \\
& (\mathcal{P}_\mathsf{f}(\mathbb{A}), \cdot) &
\end{tikzcd}$$

Umgekehrt heißen Atome $a \in \mathbb{A} \setminus \mathsf{supp}(x)$ außerhalb des Supports von x *frisch für* x:

Definition 4.14. Ein Element $x \in (X, \cdot)$ heißt *frisch* für $y \in (Y, \cdot)$, notiert $x \mathrel{\#} y$, wenn

$$\mathsf{supp}_X(x) \cap \mathsf{supp}_Y(y) = \varnothing.$$

Äquivariante Abbildungen erhalten ebenso Frische:

Korollar 4.15. *Für äquivariante Abbildungen $f\colon (X, \cdot) \to (Y, \cdot)$ zwischen nominalen Mengen und alle $a \in \mathbb{A}$, $x \in X$ gilt: wenn $a \mathrel{\#} x$, dann auch $a \mathrel{\#} f(x)$.*

Beweis. Nach Korollar 4.13: $\{a\} \cap \mathsf{supp}(f(x)) \subseteq \{a\} \cap (\mathsf{supp}(x)) \overset{a\#x}{=} \varnothing$. □

Beispiel 4.16. Werfen wir erneut einen Blick auf Lemma 2.18 (a) und (b):

(a) $\mathrm{id}_\mathbb{A}$ ist die einzige äquivariante Abbildung $\mathbb{A} \to \mathbb{A}$: Wenn $f\colon \mathbb{A} \to \mathbb{A}$ äquivariant ist, dann folgt für $a \in \mathbb{A}$ mittels $\mathsf{supp}(a) = \{a\}$ sofort $\mathsf{supp}(f(a)) \subseteq \{a\}$. In der Tat ist $a = f(a)$ das einzige in $\mathbb{A}$ dessen Support eine Teilmenge von $\{a\}$ ist.

(b) Δ ist die einzige Äquivalenz Abbildung $\mathbb{A} \to \mathbb{A}^2$: Ganz analog gilt für ein äquivariantes $f\colon \mathbb{A} \to \mathbb{A}^2$ und für $a \in \mathbb{A}$ sofort $\mathsf{supp}(f(a)) \subseteq \{a\}$. Wieder ist $(a, a) \in \mathbb{A}^2$ das einzige Element, deren Support eine Teilmenge von $\{a\}$ ist

Wenn $\mathsf{supp}(x)$ die Atome enthält, die irgendwo in x vorkommen, dann gilt für Tupel $t \in X_1 \times \cdots \times X_n$, dass ein Atom genau dann in $\mathsf{supp}(t)$ enthalten ist, wenn es im Support von einer der Komponenten von t ist:

Lemma 4.17 (Übungsaufgabe). *Für nominale Mengen $X_1, \dots, X_n$ ist der Support in $X_1 \times \cdots \times X_n$ beschrieben durch:*

$$\mathsf{supp}_{X_1 \times \cdots \times X_n}(x_1, \dots, x_n) = \mathsf{supp}_{X_1}(x_1) \cup \cdots \cup \mathsf{supp}_{X_n}(x_n).$$

Die Intuition besagt, dass $\mathsf{supp}(x)$ die Atome sind, die in einem Element $x \in X$ eingebaut sind und dass $\pi \cdot x$ diese Atome gemäß $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ umbenennt. Folglich gilt, dass $\pi \cdot x$ nur davon abhängt, wie sich π auf $\mathsf{supp}(a)$ verhält:

Lemma 4.18. *Für nominale Mengen $(X, \cdot)$ und $x \in X$ gilt für alle $\pi, \sigma \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$:*

$$\textit{wenn } \pi(a) = \sigma(a) \textit{ für alle } a \in \mathsf{supp}(x), \textit{ dann } \pi \cdot x = \sigma \cdot x.$$

Beweis. Wenn $\pi(a) = \sigma(a)$ für alle $a \in \mathsf{supp}(x)$, so folgt $\sigma^{-1} \cdot \pi \in \mathsf{Fix}(\mathsf{supp}(x))$. Da $\mathsf{supp}(x)$ ein Support von x ist, folgt $\sigma^{-1} \cdot \pi \cdot x = x$ und damit $\pi \cdot x = \sigma \cdot x$. □

Wenn man die Atome in x gemäß π ersetzt, um $\pi \cdot x$ zu erhalten, dann sollten nach der Intuition in $\pi \cdot x$ genau die Atome $\pi[\mathsf{supp}(x)]$ vorkommen. Dafür zeigen wir zuerst, dass sich Supports ganz allgemein mit der Gruppenoperation vertragen:

Lemma 4.19. *Wenn $S \subseteq \mathbb{A}$ ein Support von x in einer Gruppenoperation $(X, \cdot)$ ist, dann ist $\pi \cdot S$ ein Support von $\pi \cdot x$.*

Hier ist $\pi \cdot S := \pi[S]$ die punktweise Gruppenwirkung auf $\mathcal{P}_\mathsf{f}(\mathbb{A})$ (Beispiel 2.13).

Beweis. Sei $\sigma \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ mit $\sigma(a) = a$ für alle $a \in \pi \cdot S = \pi[S]$; also explizit $\sigma(\pi(b)) = \pi(b)$ für alle $b \in S$. Damit gilt $(\pi^{-1} \cdot \sigma \cdot \pi)(b) = b$ für alle b in S. Da S ein Support von x ist, folgt:

$$\pi^{-1} \cdot \sigma \cdot \pi \cdot x = x \qquad \iff \qquad \sigma \cdot \pi \cdot x = \pi \cdot x$$ □

Die Eigenschaft, dass die Menge der Atome in $\pi \cdot x$ genau $\pi[\mathsf{supp}(x)]$ ist, bedeutet, dass supp eine äquivariante Abbildung ist:

Lemma 4.20. *Für alle nominalen Mengen X ist $\mathsf{supp}_X \colon (X, \cdot) \to (\mathcal{P}_\mathsf{f}(\mathbb{A}), \cdot)$ äquivariant.*

Beweis. Da die Gruppenoperation auf $\mathcal{P}_\mathsf{f}(\mathbb{A})$ punktweise definiert ist, müssen wir für alle $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ überprüfen, dass

$$\mathsf{supp}(\pi \cdot x) = \pi[\mathsf{supp}(x)].$$

- Nach Lemma 4.19 ist $\pi \cdot \mathsf{supp}(x)$ ein Support von $\pi \cdot x$ – und außerdem natürlich endlich.
- Sei $S \subseteq \mathbb{A}$ ein endlicher Support von $\pi \cdot x$. Dann ist $\pi^{-1} \cdot S$ ein endlicher Support von $\pi^{-1} \cdot \pi \cdot x = x$. Also gilt notwendigerweise

  $$\mathsf{supp}(x) \subseteq \pi^{-1} \cdot S,$$

  das äquivalent zu $\pi \cdot \mathsf{supp}(x) \subseteq S$ ist. □

Es ist nicht schwer zu sehen, dass $(\mathcal{P}_\mathsf{f}\mathbb{A}, \cdot)$ auch eine nominale Menge ist; schließlich ist jedes $M \in \mathcal{P}_\mathsf{f}\mathbb{A}$ ein endlicher Support von M selbst. Obendrein gilt, dass M tatsächlich auch der *kleinste* endliche Support von M ist:

Lemma 4.21 (Übungsaufgabe)**.** *Für alle $M \in \mathcal{P}_\mathsf{f}X$ und $(X, \cdot)$ nominal ist $\bigcup_{x\in M} \mathsf{supp}(x)$ der kleinste endliche Support von M.*

Wir schreiben $\rightarrowtail$ für injektive Abbildungen:

Lemma 4.22 (Übungsaufgabe)**.** *Für eine äquivariante Injektion $f\colon (X, \cdot) \rightarrowtail (Y, \cdot)$ ist $S \subseteq \mathbb{A}$ genau dann ein Support von $x \in X$, wenn S ein Support von $f(x)$ ist.*

Insbesondere: ist $(Y, \cdot)$ nominal, so ist auch $(X, \cdot)$ nominal und $\mathsf{supp}_X = \mathsf{supp}_Y \circ f$.

$$\begin{tikzcd}
(X,\cdot) \arrow[rr, tail, "f"] \arrow[dr, "\mathsf{supp}_X"'] & \circlearrowleft & (Y,\cdot) \arrow[dl, "\mathsf{supp}_Y"] \\
& (\mathcal{P}_\mathsf{f}(\mathbb{A}), \cdot) &
\end{tikzcd}$$

Definition 4.23. Für eine Familie von nominalen Mengen $(X_i, \cdot)$, $i \in I$, bezeichne

$$\coprod_{i\in I} X_i = \{\mathsf{in}_i(x) \mid x \in X_i, i \in I\}$$

die *disjunkte Vereinigung* der Mengen (auch: *Koprodukt*). Die Injektion wird mit in bezeichnet. Für $I = 2$ schreiben wir $X_0 + X_1$.

Da die Injektionen in_k injektiv und äquivariant sind, folgt aus Lemma 4.22:

Korollar 4.24. *Der Support auf der disjunkten Vereinigung von nominalen Mengen ist gegeben durch:*

$$\mathsf{supp}(\mathsf{in}_k(x)) = \mathsf{supp}_{X_k}(x) \qquad \textit{für alle } \mathsf{in}_k(x) \in \coprod_{i\in I} X_i$$

Beweis. $\mathsf{supp}(x)$ ist ein endlicher Support von $\mathsf{in}_k(x)$. Damit ist $\coprod_{i\in I} X_i$ nominal und $\mathsf{supp}(\mathsf{in}_k(x)) = \mathsf{supp}_{X_k}(x)$. ☐

Die Implikation in der Definition von Support gilt im allgemeinen nicht in die umgekehrte Richtung. Falls doch, spricht man von *starkem* Support:

Definition 4.25. Eine Menge $S \subseteq \mathbb{A}$ heißt *starker Support* von $x \in X$, wenn für alle $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ gilt:

$$\pi \in \mathsf{Fix}(S) \qquad \Longleftrightarrow \qquad \pi \cdot x = x.$$

Eine nominale Menge ist *stark*, wenn alle ihre Elemente einen starken Support haben.

Intuitiv hat ein Element einer nominalen Menge dann einen starken Support, wenn die Atome in einer festen Reihenfolge vorkommen.

Beispiel 4.26. Tupel (von Atomen) haben starken Support: $\{a, b\}$ ist ein starker Support von $(a, b) \in \mathbb{A}^2$. Mengen (von Atomen) haben keinen starken Support: für $\{a, b\} \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ gilt zwar $(a\ \ b) \cdot \{a, b\} = \{a, b\}$, jedoch $(a\ \ b) \notin \mathsf{Fix}(\{a, b\})$.

Lemma 4.27. *Jeder starke und endliche Support $S \subseteq \mathbb{A}$ eines Elements $x \in X$ einer Gruppenoperation $(X, \cdot)$ ist notwendigerweise der kleinste endliche Support $\mathsf{supp}(x) = S$.*

Beweis. Sei $S \subseteq \mathbb{A}$ ein starker und endlicher Support von $x \in X$ und sei $M \subseteq \mathbb{A}$ ein weiterer endlicher Support von x. Angenommen, es gäbe ein $a \in S \setminus M$, so würde für frisches $b \in \mathbb{A} \setminus S \cup M \cup \{a\}$ zum Widerspruch führen: $(a\ \ b) \in \mathsf{Fix}(M)$, und da M ein Support von x ist:

$$(a\ \ b) \cdot x = x$$

und da S ein starker Support von x ist:

$$(a\ \ b) \in \mathsf{Fix}(S),$$

ein Widerspruch zu $a \in S$. □

Mittels der Gruppenoperation konnten wir bisher also schon rekonstruieren, welche Atome in Elementen einer Gruppenoperation vorkommen und ob diese eine fixe Reihenfolge haben.

4.2 Beispiel der λ-Terme

Bisher ist der Support eine Ansammlung an allen Atomen, die irgendwo verschachtelt innerhalb der Struktur vorkommen. Wenn die Strukturen Operationen zur Variablenbindung erlauben, wie z. B. im λ-Kalkül, dann ist es erstrebenswert, wenn diese nicht im Support vorkommen. Die Identitätsfunktion

$$\lambda v.\ v$$

im λ-Kalkül hat keine freien Variablen. Im Folgenden untersuchen wir, wie sich eine Gruppenoperation auf λ-Termen definieren lässt, sodass supp genau die *freien* Variablen bezeichnet, also z. B. $\mathsf{supp}(v) = \{v\}$ aber $\mathsf{supp}(\lambda v.\ v) = \varnothing$.

Definition 4.28. Die Menge der *λ-Terme* (oder *λ-Ausdruck*) ist die kleinste Menge Λ, die unter den folgenden Operationen abgeschlossen ist:

(a) *Variable*: v für $v \in \mathbb{A}$

(b) *Abstraktion*: $\lambda v.\, t$ für $v \in \mathbb{A}$ und $t \in \Lambda$

(c) *Anwendung*: $t\,p$ (oder explizit: $t@p$) für $t, p \in \Lambda$

Die Menge Λ hat eine kanonische Gruppenoperation, die für $v \in \mathbb{A}$ und $t, p \in \Lambda$ rekursiv definiert ist:

$$\pi \cdot v = \pi(v) \qquad \pi \cdot (\lambda v.\, t) = \lambda\, \pi(v).\ \pi \cdot t \qquad \pi \cdot (t@p) = (\pi \cdot t)@(\pi \cdot p) \tag{4.1}$$

Bemerkung 4.29. Λ ist der Träger der initialen F-Algebra für den Funktor

$$FX = \mathbb{A} + \mathbb{A} \times X + X \times X.$$

Definition 4.30. Wir betrachten folgende Funktionen $\Lambda \to \mathcal{P}_\mathsf{f}(\mathbb{A})$:

$$\begin{array}{lll}
\mathsf{vars}\colon \Lambda \to \mathcal{P}_\mathsf{f}(\mathbb{A}) & \mathsf{fv}\colon \Lambda \to \mathcal{P}_\mathsf{f}(\mathbb{A}) & \\
\mathsf{vars}(a) = \{a\} & \mathsf{fv}(a) = \{a\} & \text{für } a \in \mathbb{A} \\
\mathsf{vars}(\lambda v.\, t) = \{v\} \cup \mathsf{vars}(t) & \mathsf{fv}(\lambda v.\, t) = \mathsf{fv}(t) \setminus \{v\} & \text{für } v \in \mathbb{A}, t \in \Lambda \\
\mathsf{vars}(t@p) = \mathsf{vars}(t) \cup \mathsf{vars}(p) & \mathsf{fv}(t@p) = \mathsf{fv}(t) \cup \mathsf{fv}(p) & \text{für } t, p \in \Lambda
\end{array}$$

Lemma 4.31. $(\Lambda, \cdot)$ *ist eine nominale Menge mit* $\mathsf{supp}_\Lambda = \mathsf{vars}$.

Beweis. Nutzt man $\Lambda \cong \mathbb{A}+\mathbb{A}\times\Lambda+\Lambda\times\Lambda$, so ergibt sich aus Lemma 4.17 und Korollar 4.24 genau vars als rekursive Definition von supp:

$$
\begin{aligned}
&\mathsf{supp}\colon \Lambda \to \mathcal{P}_{\mathsf{f}}(\mathbb{A}) && \\
&\mathsf{supp}(a) = \{a\} && \text{für } a \in \mathbb{A} \\
&\mathsf{supp}(\lambda v.\, t) = \{v\} \cup \mathsf{supp}(t) && \text{für } v \in \mathbb{A}, t \in \Lambda \\
&\mathsf{supp}(t@p) = \mathsf{supp}(t) \cup \mathsf{supp}(p) && \text{für } t, p \in \Lambda
\end{aligned}
$$

□

Auf Λ lässt sich α-Äquivalenz explizit als Relation $=_\alpha$ definieren, die durch die folgenden Regeln erzeugt wird:

$$
\frac{}{a =_\alpha a} \qquad \frac{t_1 =_\alpha t_2 \quad p_1 =_\alpha p_2}{t_1@p_1 =_\alpha t_2@p_2} \qquad \frac{a \notin \mathsf{supp}(v_1, t_1, v_2, t_2) \quad (v_1\ a) \cdot t_1 =_\alpha (v_2\ a) \cdot t_2}{\lambda v_1.t_1 =_\alpha \lambda v_2.t_2}
$$

Lemma 4.32. *Die Menge* $=_\alpha \subseteq \Lambda \times \Lambda$ *ist äquivariant.*

Beweis. Per Induktion über die Höhe der Terme. □

Lemma 4.33. $=_\alpha$ *ist eine Äquivalenzrelation auf* Λ.

Beweis. Per Induktion über die Höhe der Terme. Reflexivität und Symmetrie ergeben sich direkt aus der Definition. Für Transitivität: Betrachte $\lambda v_1.t_1 =_\alpha \lambda v_2.t_2 =_\alpha \lambda v_3.t_3$ also gibt es $a \notin \mathsf{supp}(v_1, t_1, v_2, t_2)$ und $a' \notin \mathsf{supp}(v_2, t_2, v_3, t_3)$ mit

$$(v_1\ a) \cdot t_1 =_\alpha (v_2\ a) \cdot t_2 \text{ und } (v_2\ a') \cdot t_2 =_\alpha (v_3\ a') \cdot t_3$$

Sei b frisch für $a, a', v_1, v_2, t_1, t_2$. Da $=_\alpha$ äquivariant ist und da t_1, t_2 und t_3 eine uniforme Höhe haben, die geringer ist als die von $\lambda v_1.t_1$, $\lambda v_2.t_2$ und $\lambda v_3.t_3$, können wir schließen:

$$
\begin{aligned}
(v_1\ b) \cdot t_1 &= (a\ b) \cdot (v_1\ a) \cdot t_1 && \text{(Lemma 4.18)} \\
&=_\alpha (a\ b) \cdot (v_2\ a) \cdot t_2 && (=_\alpha \text{ äquivariant}) \\
&= (a'\ b) \cdot (v_2\ a') \cdot t_2 && \text{(Lemma 4.18)} \\
&=_\alpha (a'\ b) \cdot (v_3\ a') \cdot t_3 && (=_\alpha \text{ äquivariant}) \\
&= (v_3\ b) \cdot t_3 && \text{(Lemma 4.18)}
\end{aligned}
$$

und damit folgt per induktiver Regel $\lambda v_1.t_1 =_\alpha \lambda v_3.t_3$. □

Definition 4.34. Die Menge der λ-Terme modulo α-Äquivalenz wird mit $\Lambda/{=_\alpha}$ bezeichnet und deren Elemente mit $[t]_\alpha \in \Lambda/{=_\alpha}$ (für $t \in \Lambda$).

Ganz allgemein lassen sich nominale Mengen durch äquivariante Äquivalenzrelationen quotientieren:

Definition 4.35. Eine Teilmenge $S \subseteq (X, \cdot)$ (einer Gruppenoperation) heißt *äquivariant* wenn für alle $x \in S$ und $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ auch $\pi \cdot x$ in S enthalten ist.

Wenn eine Relation $R \subseteq X \times X$ äquivariant und obendrein eine Äquivalenzrelation ist, dann erbt der Quotient X/R die Gruppenoperation:

$$\pi \cdot [x]_R := [\pi \cdot x]_R$$

Lemma 4.36. *Die Gruppenoperation auf X/R in Definition 4.35 ist wohldefiniert.*

Beweis. Die Axiome für Gruppenoperationen sind leicht nachzurechnen. Für die Wohldefiniertheit der Definition von $\pi \cdot [x]_R$ sei $[x]_R = [y]_R$, also $(x, y) \in R$. Per Äquivarianz von R folgt $(\pi \cdot x, \pi \cdot y) \in R$ und damit

$$[\pi \cdot x]_R = [\pi \cdot y]_R \qquad \square$$

Lemma 4.37 (Übungsaufgabe)**.** *Für eine äquivariante Äquivalenzrelation $R \subseteq X \times X$ auf einer nominalen Menge $(X, \cdot)$ ist $(X/R, \cdot)$ nominal und hat den Support:*

$$\mathsf{supp}_{X/R}([x]_R) = \bigcap_{y \in [x]_R} \mathsf{supp}_X(y)$$

Da $=_\alpha$ äquivariant ist, erbt $\Lambda/{=_\alpha}$ die Gruppenoperation von Λ:

$$\pi \cdot [t]_\alpha := [\pi \cdot t]_\alpha$$

Da Λ eine nominale Menge ist, ist $\Lambda/{=_\alpha}$ ebenso nominal mit $\mathsf{supp}([t]_\alpha) \subseteq \mathsf{supp}_\Lambda(t)$.

Theorem 4.38. *Alle $[t]_\alpha \in \Lambda/{=_\alpha}$ haben den starken Support $\mathsf{supp}(t) = \mathsf{fv}(t)$.*

Beweis. Wir zeigen per Induktion über t, dass für alle $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ gilt:

$$\pi \in \mathsf{Fix}(\mathsf{fv}(t)) \qquad \Leftrightarrow \qquad \pi \cdot t =_\alpha t$$

- Für $t = a \in \mathbb{A}$ ist $\mathsf{fv}(a) = \{a\}$ und in der Tat:

$$\pi \in \mathsf{Fix}(\{a\}) \qquad \Leftrightarrow \qquad \pi \cdot a = a$$

- Für $t = s@p$ ist $\mathsf{fv}(a) = \mathsf{fv}(s) \cup \mathsf{fv}(p)$ und $\mathsf{Fix}(\mathsf{fv}(s@p)) = \mathsf{Fix}(\mathsf{fv}(s)) \cap \mathsf{Fix}(\mathsf{fv}(p))$, wodurch:

$$\pi \in \mathsf{Fix}(\mathsf{fv}(s@p)) \Leftrightarrow \left\{ \begin{array}{c} \pi \in \mathsf{Fix}(\mathsf{fv}(s)) \\ \& \\ \pi \in \mathsf{Fix}(\mathsf{fv}(p)) \end{array} \right\} \overset{\text{I.H.}}{\Longleftrightarrow} \left\{ \begin{array}{c} \pi \cdot s = s \\ \& \\ \pi \cdot p = p \end{array} \right\} \Leftrightarrow \pi \cdot s@p = s@p$$

- Für $t = \lambda v.s$ ist $\mathsf{fv}(\lambda v.s) = \mathsf{fv}(s) \setminus \{v\}$ mit der Induktionshypothese:

$$\pi \in \mathsf{Fix}(\mathsf{fv}(s)) \qquad \Leftrightarrow \qquad \pi \cdot s =_\alpha s \qquad \forall \pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A}) \qquad \text{(I.H.)}$$

  $(\Rightarrow)$ Wenn $\pi \in \mathsf{Fix}(\mathsf{fv}(s) \setminus \{v\})$, so ist $\pi \cdot \lambda v.s =_\alpha \lambda v.s$ zu zeigen. Hierfür wähle $a \in \mathbb{A}$ frisch für s, $\pi \cdot s$, v, $\pi(v)$ und π (also $\pi(a) = a$). Dann gilt:

$$(v \;\; a) \cdot \pi \cdot (v \;\; a) \in \mathsf{Fix}(\mathsf{fv}(s))$$

Per Induktionshypothese erhalten wir:

$$(v\ \ a) \cdot \pi \cdot (v\ \ a) \cdot s =_\alpha s$$

Damit gilt:[1]

$$(v\ \ a) \cdot s =_\alpha \pi \cdot (v\ \ a) \cdot s = (\pi(v)\ \ \pi(a)) \cdot \pi \cdot s = (\pi(v)\ \ a) \cdot \pi \cdot s$$

Somit ergibt die Regelanwendung (4.1) für $=_\alpha$:

$$\lambda v.s =_\alpha \lambda \pi(v).(\pi \cdot s) = \pi \cdot \lambda v.s$$

($\Leftarrow$) Sei umgekehrt $\pi \cdot \lambda v.s =_\alpha \lambda v.s$, woraus wir $\pi \in \mathsf{Fix}(\mathsf{fv}(s) \setminus \{v\})$ zeigen müssen. Die Annahme der einzigen passenden $=_\alpha$-Regel ergibt ein frisches $a \in \mathbb{A} \setminus \mathsf{supp}(v, \pi(v), s, \pi \cdot s)$ mit

$$(v\ \ a) \cdot s =_\alpha (\pi(v)\ \ a) \cdot \pi \cdot s, \tag{4.2}$$

Da $=_\alpha$ äquivariant ist, können wir die Permutationen nach rechts umschreiben:

$$s =_\alpha \underbrace{(v\ \ a) \cdot (\pi(v)\ \ a) \cdot \pi}_{\pi' :=} \cdot s,$$

und erhalten wir per Induktionshypothese:

$$\pi' \quad \in \quad \mathsf{Fix}(\mathsf{fv}(s)).$$

Für unser Ziel sei $b \in \mathsf{fv}(s) \setminus \{v\}$. Hierfür schließen wir:

Aus	$b \in \mathsf{fv}(s) \setminus \{v\}$	folgt	$v \neq b$.
Aus	$a \notin \mathsf{supp}(s) = \mathsf{fv}(s)$ und $b \in \mathsf{fv}(s)$	folgt	$a \neq b$.
Aus	$a \notin \mathsf{supp}(\pi \cdot s) = \pi \cdot \mathsf{fv}(s)$ und $b \in \mathsf{fv}(s)$	folgt	$a \neq \pi(b)$.

Da $\pi = (\pi(v)\ \ a) \cdot (v\ \ a) \cdot \pi'$, wird b von π wie folgt geschickt:

$$\overbrace{b \xmapsto[\pi' \in \mathsf{Fix}(\mathsf{fv}(s))]{\pi'} b \xmapsto[b \notin \{v,a\}]{(v\ \ a)} b \xmapsto[b \neq a]{(\pi(v)\ \ a)}}^{\pi} \begin{cases} a & \text{falls } b = \pi(v) \\ b & \text{sonst.} \end{cases}$$

Falls $b = \pi(v)$ gelten würde, so wäre $\pi(b) = a$, ein Widerspruch. Damit ist nur $b \neq \pi(v)$ und damit $\pi(b) = b$ möglich. Deshalb gilt $\pi \in \mathsf{Fix}(\mathsf{fv}(s) \setminus \{v\})$, wie gewünscht. □

Bemerkung 4.39 (Alternativ-Beweis von „$\Leftarrow$"). In der Richtung „$\Rightarrow$" zuvor konnten wir a wählen, sodass $\pi(a) = a$. In „$\Leftarrow$" jedoch haben wir keine genauere Information über $\pi(a)$. Als alternative Beweis-Strategie könnte man hier ein weiteres $a' \in \mathbb{A}$ wählen, dass nicht nur für v, $\pi(v)$, s, $\pi \cdot s$ sondern auch noch für π frisch ist und würde aus (4.2) erhalten:

$$\underbrace{(v\ \ a') \cdot s = (a\ \ a')}_{\substack{\text{Lemma 4.18} \\ a, a' \,\#\, s}} \cdot \underbrace{(v\ \ a) \cdot s =_\alpha (a\ \ a')}_{\text{(4.2) und Äquivarianz}} \cdot (\pi(v)\ \ a) \cdot \underbrace{\pi \cdot s = (\pi(v)}_{\substack{\text{Lemma 4.18} \\ a, a' \,\#\, \pi \cdot s}}\ \ a') \cdot \pi \cdot s$$

[1] Für den zweiten Schritt siehe die Nebenrechnung von Blatt 2, A3.

Da $\pi(a') = a'$, können wir umschreiben:

$$s =_\alpha (v\ \ a') \cdot (\pi(v)\ \ \underbrace{a'}_{\pi(a')}) \cdot \pi \cdot s = (v\ \ a') \cdot \pi \cdot (v\ \ a') \cdot s = ((v\ \ a') \star \pi) \cdot s$$

Per Induktionshypothese erhalten wir: $\pi' := (v\ \ a') \star \pi \in \mathsf{Fix}(\mathsf{fv}(s))$. Für die Verifikation von $\pi \in \mathsf{Fix}(\mathsf{fv}(s) \setminus \{v\})$ betrachte $b \in \mathsf{fv}(s) \setminus \{v\}$. Es gilt $b \neq a'$ und $b \neq v$, weshalb b von $\pi = (v\ \ a') \cdot \pi' \cdot (v\ \ a')$ wie folgt geschickt wird.

$$\begin{tikzcd} b \arrow[r, mapsto, "(v\ \ a')", "b \notin \{v, a'\}"'] \arrow[rrr, bend left, "\pi"] & b \arrow[r, mapsto, "\pi'", "\pi' \in \mathsf{Fix}(\mathsf{fv}(s))"'] & b \arrow[r, mapsto, "(v\ \ a')", "b \notin \{v, a'\}"'] & b \end{tikzcd}$$

also gilt $\pi \in \mathsf{Fix}(\mathsf{fv}(s) \setminus \{v\})$, wie gewünscht. □

4.3 Bindungsfunktor

Der Aspekt der Variablen-Bindung lässt sich auch durch einen separaten Funktor beschreiben, den man dann modular einsetzen kann. Dadurch lässt sich Variablen-Bindung nicht nur in anderen syntaktischen Konstrukten verwenden, sondern man trennt auch den induktiven/rekursiven Aspekt von Bindung. Für die konkret betrachtete Äquivalenz $=_\alpha$ mussten wir alle Eigenschaften (Transitivität, Äquivarianz, Support) aufwändig per strukureller Induktion beweisen.

Stattdessen lässt sich dank der nominalen Struktur die Relation α-Äquivalenz auch auf allgemeinen nominalen Mengen definieren.

Definition 4.40. Die Relation $\sim_\alpha \subseteq (\mathbb{A} \times X) \times (\mathbb{A} \times X)$ für eine gegebene nominale Menge $(X, \cdot)$ ist definiert durch:

$$(v_1, x_1) \sim_\alpha (v_2, x_2) \quad :\Longleftrightarrow \quad \text{es gibt } a \in \mathbb{A} \text{ mit } \begin{array}{c} a \notin \mathsf{supp}(v_1, v_2, x_1, x_2) \\ (v_1\ \ a) \cdot x_1 = (v_2\ \ a) \cdot x_2 \end{array}$$

Proposition 4.41 (Übungsaufgabe). *$\sim_\alpha$ ist eine äquivariante Äquivalenzrelation.*

Notation 4.42. Für eine nominale Menge $(X, \cdot)$ schreiben wir $[\mathbb{A}]X$ für den Quotienten $(\mathbb{A} \times X)/ \sim_\alpha$, genannt *Abstraktionsmenge*. Die Äquivalenzklasse von $(a, x) \in \mathbb{A} \times X$ wird mit $\langle a \rangle x$ bezeichnet.

Proposition 4.43. *Für alle $\langle a \rangle x \in [\mathbb{A}]X$ ist $\mathsf{supp}_{[\mathbb{A}]X}(\langle a \rangle x) = \mathsf{supp}_X(x) \setminus \{a\}$.*

Beweis. Nach Lemma 4.37 müssen wir lediglich

$$\mathsf{supp}_{[\mathbb{A}]X}(\langle a \rangle x) = \bigcap_{(b,y) \sim_\alpha (a,x)} \mathsf{supp}(b, y)$$

vereinfachen. Per Reflexivität gilt $\mathsf{supp}(\langle a \rangle x) \subseteq \mathsf{supp}(a, x) = \{a\} \cup \mathsf{supp}(x)$. Für jedes $(b, y) \sim_\alpha (a, x)$ gilt, dass es $c \in \mathbb{A} \setminus \mathsf{supp}(a, b, x, y)$ gibt mit $(a\ \ c) \cdot x = (b\ \ c) \cdot y$, also

$$\mathsf{supp}(b, y) = \{b\} \cup \mathsf{supp}(y) = \{b\} \cup (b\ \ c) \cdot (a\ \ c) \cdot \mathsf{supp}(x) = \{b\} \cup \mathsf{supp}(x) \setminus \{a\}.$$

Also erhalten wir

$$\mathsf{supp}(x) \setminus \{a\} \subseteq \mathsf{supp}(b, y) \qquad \text{für alle } (b, y) \sim_\alpha (a, x). \tag{4.3}$$

Diese untere Schranke $\mathsf{supp}(x) \setminus \{a\}$ ist somit enthalten im Schnitt – der größten unteren Schranke:

$$\mathsf{supp}(x) \setminus \{a\} \subseteq \mathsf{supp}_{[\mathbb{A}]X}(\langle a\rangle x)$$

Für beliebig frisches $b \in \mathbb{A}$, $b \,\#\, (a, x)$, können wir $y := (a\ \ b) \cdot x$ wählen und erhalten für frisches c:

$$(b\ \ c) \cdot y = (b\ \ c) \cdot (a\ \ b) \cdot x \underbrace{=}_{\text{Lemma 4.18}} (a\ \ c) \cdot x \quad \Longrightarrow \quad (b, y) \sim_\alpha (a, x)$$

Aus (4.3) folgt nun $a \notin \mathsf{supp}(b, y)$ und ferner $a \notin \mathsf{supp}(\langle b\rangle y) = \mathsf{supp}(\langle a\rangle x)$, also $\mathsf{supp}(\langle a\rangle x) = \mathsf{supp}(x) \setminus \{a\}$. ☐

Proposition 4.44. $[\mathbb{A}]$ *ist ein Funktor* $\mathsf{Nom} \to \mathsf{Nom}$ *und auf äquivarianten Abbildungen definiert durch*

$$f\colon X \to Y \qquad \mapsto \qquad [\mathbb{A}]f\colon [\mathbb{A}]X \to [\mathbb{A}]Y \quad [\mathbb{A}](f)(\langle a\rangle x) = \langle a\rangle(f(x))$$

Beweis. Es sind folgende Eigenschaften zu prüfen:

1. $[\mathbb{A}]f$ ist wohldefiniert: Wenn $\langle a\rangle x = \langle b\rangle x$, so gibt es ein frisches c mit

   $$(a\ \ c) \cdot x = (b\ \ c) \cdot y$$

   Da $\mathsf{supp}(f(x)) \subseteq \mathsf{supp}(x)$ und $\mathsf{supp}(f(y)) \subseteq \mathsf{supp}(y)$, so ist c auch ausreichend frisch für $a, b, f(x), f(y)$ und außerdem

   $$(a\ \ c) \cdot f(x) = f((a\ \ c) \cdot x) = f((b\ \ c) \cdot y) = (b\ \ c) \cdot f(y)$$

   Also $\langle a\rangle(f(x)) = \langle b\rangle(f(y))$.

2. $[\mathbb{A}]$ erhält Identitäten: Für $f = \mathrm{id}_X$ erhalten wir $[\mathbb{A}](\mathrm{id}_X)(\langle a\rangle x) = \langle a\rangle(\mathrm{id}_X(x)) = \langle a\rangle x$, also $[\mathbb{A}](\mathrm{id}_X) = \mathrm{id}_{[\mathbb{A}]X}$.

3. $[\mathbb{A}]$ erhält Komposition: Für $f\colon X \to Y$ und $g\colon Y \to Z$ gilt

   $$\begin{aligned}[\mathbb{A}](g \cdot f)(\langle a\rangle x) &= \langle a\rangle(g(f(x))) \\ &= [\mathbb{A}](g)(\langle a\rangle(f(x))) = [\mathbb{A}](g)([\mathbb{A}](f)(\langle a\rangle(x)))\end{aligned}$$ ☐

Variablen-Bindung steht in einem engen Zusammenhang mit Frische:

Definition 4.45. Das *frische Produkt* $X * Y$ zweier nominalen Mengen ist

$$X * Y = \{(x, y) \in X \times Y \mid x \,\#\, y\}$$

Proposition 4.46 (Übungsaufgabe)**.** *Für nominale Mengen X und Y gibt es eine bijektive Korrespondenz zwischen äquivarianten Abbildungen der Form*

$$X * \mathbb{A} \to Y \qquad \textit{und} \qquad X \to [\mathbb{A}]Y$$

Diese Korrespondenz ist natürlich in X und Y, genauer sind $[\mathbb{A}]$ und $*$ adjungierte Funktoren:

5 Adjunktionen

Adjunktionen sind eines der wichtigsten Konzepte der Kategorientheorie. Saunders Mac Lane [9, S. vii] prägte den Slogan:

> *„Adjoint functors arise everywhere!"*

5.1 Kategorielle Allgemeinheit

Definition 5.1. Zwei Funktoren $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{C}$ sind *adjungiert* (geschrieben $F \dashv G$), wenn es eine Bijektion

$$\mathcal{D}(FC, D) \cong \mathcal{C}(C, GD)$$

gibt, die natürlich in $C \in \mathcal{C}$ und $D \in \mathcal{D}$ ist. F bzw. G heißen dann links- bzw. rechtsadjungiert.

Notation 5.2. Wir notieren bijektive Korrespondenz zwischen Hom-Mengen ähnlich wie Beweis-Regeln:

$$\frac{FC \to D \text{ in } \mathcal{D}}{C \to GD \text{ in } \mathcal{C}} \quad \text{natürlich in } C \text{ und } D.$$

Sowohl $\mathcal{D}(F(-), -)$ als auch $\mathcal{C}(-, G(-))$ sind Funktoren $\mathcal{C}^{\mathsf{op}} \times \mathcal{C} \to \mathsf{Set}$. Eine Adjunktion zwischen F und G besteht also aus einer Familie von Bijektionen

$$\mathcal{D}(FC, D) \xrightarrow{\phi_{C,D}} \mathcal{C}(C, GD)$$

für jedes $C \in \mathcal{C}$ und $D \in \mathcal{D}$. Die Natürlichkeit in C und D bedeutet, dass für $f\colon C' \to C$ und $g\colon D \to D'$ das Quadrat

$$\begin{tikzcd}
\mathcal{D}(FC, D) \arrow[r, "\phi_{C,D}", "\cong"'] \arrow[d, "\mathcal{D}(Ff,g)"'] & \mathcal{C}(C, GD) \arrow[d, "\mathcal{C}(f,Gg)"] \\
\mathcal{D}(FC', D') \arrow[r, "\phi_{C',D'}", "\cong"'] & \mathcal{C}(C', GD')
\end{tikzcd}$$

in Set kommutiert.

Beispiel 5.3. Für $\mathcal{C} = \mathcal{D} = \mathsf{Set}$ und eine fixe Menge A sind $FX = X \times A$ und $GX = X^A$ adjungiert, denn für alle Mengen X und Y gibt es eine bijektive Korrespondenz

$$\frac{X \times A \to Y}{X \to Y^A}$$

Das bedeutet, dass es für alle Mengen X und Y eine Bijektion

$$\phi_{X,Y}\colon \mathsf{Set}(X \times A, Y) \longrightarrow \mathsf{Set}(X, Y^A)$$

gibt, die natürlich in X und Y ist. Diese Abbildung ϕ ist als *Currying* bekannt und ϕ^{-1} als *Uncurrying*.

Es ist oft leichter, sich folgende konkretere Charakterisierung zu betrachten, die man auch *universelle Eigenschaft* nennt:

Lemma 5.4. *Funktoren F und G sind genau dann adjungiert $F \dashv G$, wenn eine natürliche Transformation $\eta\colon Id_{\mathcal{C}} \to GF$ existiert, sodass für jedes $f\colon X \to GY$ (in $\mathcal{C}$) genau ein $h\colon FX \to Y$ (in $\mathcal{D}$) existiert mit $f = Gh \cdot \eta_X$.*

$$\begin{tikzcd} FX \arrow[r, dashed, "\exists!\, h"] & Y \\ GFX \arrow[r, "Gh"] & GY \\ X \arrow[u, "\eta_X"] \arrow[ur, "f"'] & \end{tikzcd}$$

Hier heißt η die *Einheit* der Adjunktion Wenn G der Vergissfunktor einer algebraischen Theorie ist, dann kann man F als *freie* Konstruktion verstehen.

Beweis. $(\Rightarrow)$: Für $X \in \mathcal{C}$ definieren wir $\eta_X := \phi_{X,FX}(\mathrm{id}_F X)$:

$$\frac{\mathrm{id}_{FX}\colon FX \to FX}{\eta_X\colon X \to GFX}$$

Für die Verifikation, dass η natürlich in X ist rechnen wir für $f\colon X \to Z$:

$$\begin{aligned} GFf \circ \eta_X &= GFf \circ \phi_{X,FX}(\mathrm{id}_{FX}) \\ &= \mathcal{C}(X, GFf)(\phi_{X,FX}(\mathrm{id}_{FX})) \\ &= \phi_{X,FZ}(\mathcal{D}(FX, Ff)(\mathrm{id}_{FX})) && \text{(Natürlichkeit von } \phi) \\ &= \phi_{X,FZ}(Ff \circ \mathrm{id}_{FX}) = \phi_{X,FZ}(\mathrm{id}_{FZ} \circ Ff) && \text{(Neutrales Element id)} \\ &= \phi_{X,FZ}(\mathcal{D}(Ff, FZ)(\mathrm{id}_{FZ})) \\ &= \mathcal{C}(f, GFZ)(\phi_{Z,FZ}(\mathrm{id}_{FZ})) && \text{(Natürlichkeit von } \phi) \\ &= \phi_{Z,FZ}(\mathrm{id}_{FZ}) \circ f = \eta_Z \circ f \end{aligned}$$

Für die universelle Eigenschaft sei nun $f\colon X \to GY$ gegeben. Man muss nun verifizieren, dass $\phi^{-1}_{X,Y}(f)\colon FX \to Y$ das Diagramm

$$\begin{tikzcd} GFX \arrow[r, "G(\phi^{-1}_{X,Y}(f))"] & GY \\ X \arrow[u, "\phi_{X,FX}(\mathrm{id}_{FX})"] \arrow[ur, "f"'] & \end{tikzcd}$$

kommutiert und obendrein der einzige Morphismus $FX \to Y$ mit dieser Eigenschaft ist (siehe Blatt 7).

$(\Leftarrow)$: Sei $\eta\colon \mathrm{Id}_{\mathcal{C}} \to GF$ mit der universellen Eigenschaft gegeben. Nun muss man verifizieren, dass

$$\phi_{X,Y}(h) := Gh \circ \eta_X \qquad \phi_{X,Y}\colon \mathcal{D}(FX, Y) \to \mathcal{C}(X, GY)$$

eine natürliche Transformation ist und dass jedes $\phi_{X,Y}$ bijektiv ist (siehe Blatt 7). $\square$

Beispiel 5.5 (Übungsaufgabe, Blatt 3)**.** Betrachte den Vergissfunktor $U\colon G\text{-}\mathsf{Set} \to \mathsf{Set}$ aus Beispiel 3.7.(a) für eine beliebige Gruppe G. Dann gibt es einen Funktor $F\colon \mathsf{Set} \to G\text{-}\mathsf{Set}$ mit $FX = (G \times X, \cdot)$ der linksadjungiert zu U ist. Die Einheit $\eta_X\colon X \to G \times X$ schickt x auf $\eta(x) = (e, x)$, wobei e das neutrale Element von G ist.

Proposition 5.6 (Übungsaufgabe)**.** *Adjungierte Funktoren sind eindeutig (bis auf natürlichen Isomorphismus): Für Adjunktionen $F \dashv G$ und $F' \dashv G$ gibt es einen natürlichen Isomorphismus $F \cong F'$.*

In der universellen Eigenschaft (Lemma 5.4) wird die Natürlichkeit von η und die Wirkung von F auf Morphismen gar nicht verwendet. Tatsächlich ergibt sich beides bereits auf eindeutige Weise aus der Wirkung von F auf Objekten $\mathbf{obj}\,\mathcal{C} \to \mathbf{obj}\,\mathcal{D}$ und der universellen Eigenschaft:

Lemma 5.7. *Seien ein Funktor $G\colon \mathcal{D} \to \mathcal{C}$, eine Klassenfunktion $F\colon \mathbf{obj}\,\mathcal{C} \to \mathbf{obj}\,\mathcal{D}$ und eine Familie von Morphismen $(\eta_X\colon X \to GFX)_{\mathbf{obj}\,\mathcal{C}}$ mit der Eigenschaft gegeben, dass für jedes $f\colon X \to GY$ (in $\mathcal{C}$) genau ein $h\colon FX \to Y$ (in $\mathcal{D}$) existiert mit $f = Gh \cdot \eta_X$.*

$$\begin{tikzcd} FX \arrow[r, dashed, "\exists!\,h"] & Y \\ GFX \arrow[r, "Gh"] & GY \\ X \arrow[u, "\eta_X"] \arrow[ur, "f"'] & \end{tikzcd}$$

Dann lässt sich F auf eindeutige Weise zu einem Funktor $F\colon \mathcal{C} \to \mathcal{D}$ erweitern, sodass η eine natürliche Transformation ist und $F \dashv G$ eine Adjunktion mit Einheit η.

Ein Morphismus $c\colon X \to Z$ in $\mathcal{C}$ wird dann von F auf den eindeutigen Morphimus

$$Ff := h\colon FX \to FZ \quad \text{mit} \quad \underbrace{\eta_Z \cdot c}_{f} = Gh \cdot \eta_X$$

geschickt:

$$\begin{tikzcd} FX \arrow[r, dashed, "\exists!\,h"] & FZ \\ GFX \arrow[r, "Gh"] & GFZ \\ X \arrow[u, "\eta_X"] \arrow[r, "c"] & Z \arrow[u, "\eta_Z"'] \end{tikzcd} \tag{5.1}$$

Beweis. Wir verifizieren zuerst, dass F die Eigenschaften eines Funktors hat:

1. F erhält Identitäten: Da G Identitäten erhalten ist id_{FX} ein Morphismus, der folgendes Diagramm kommutieren lässt:

$$\begin{tikzcd} GFX \arrow[r, "G\mathrm{id}_{FX}"] & GFX \\ X \arrow[u, "\eta_X"] \arrow[r, "\mathrm{id}_X"] & X \arrow[u, "\eta_X"'] \end{tikzcd}$$

   Aus der Eindeutigkeit der universellen Eigenschaft ergibt sich daher $F\mathrm{id}_X = \mathrm{id}_{FX}$.

2. F erhält Komposition: Betrachte $c_1\colon X \to Y$ und $c_2\colon Y \to Z$. Da G Komposition erhält, kommutiert folgendes Diagramm:

$$\begin{tikzcd} GFX \arrow[r, "GFc_1"] \arrow[rr, bend left, "G(Fc_2 \circ Fc_1)"] & GFY \arrow[r, "GFc_2"] & GFZ \\ X \arrow[u, "\eta_X"] \arrow[r, "c_1"] & Y \arrow[u, "\eta_Y"] \arrow[r, "c_2"] & Z \arrow[u, "\eta_Z"] \end{tikzcd}$$

Aus der Eindeutigkeit der universellen Eigenschaft für $\eta_Z \circ (c_2 \circ c_1) \colon X \to GFZ$ folgt, dass $Fc_2 \circ Fc_1 = F(c_2 \circ c_1)$.

Dass Gleichung 5.1 die einzige Möglichkeit ist, F zu definieren, ergibt sich aus der Eindeutigkeit von linksadjungierten Funktoren (Proposition 5.6). Per Definition von Gleichung 5.1 ist η eine natürliche Transformation $\mathrm{Id}_{\mathcal{C}} \to GF$. □

Definition 5.8. Für jeden Funktor $F \colon \mathcal{C} \to \mathcal{D}$ erhält man einen Funktor $F^{\mathsf{op}} \colon \mathcal{C}^{\mathsf{op}} \to \mathcal{D}^{\mathsf{op}}$ per $F^{\mathsf{op}}X := FX$ und $F^{\mathsf{op}}f := Ff$.

Korollar 5.9. *Wenn $F \dashv G$, so ist $G^{\mathsf{op}} \dashv F^{\mathsf{op}}$.*

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & \mathcal{D} \arrow[l, bend left, "G"] \end{tikzcd} \qquad \Longleftrightarrow \qquad \begin{tikzcd} \mathcal{C}^{\mathsf{op}} \arrow[r, bend left, "F^{\mathsf{op}}"] \arrow[r, phantom, "\top"] & \mathcal{D}^{\mathsf{op}} \arrow[l, bend left, "G^{\mathsf{op}}"] \end{tikzcd}$$

Beweis. $\mathcal{C}^{\mathsf{op}}(G^{\mathsf{op}}D, C) \cong \mathcal{C}(C, GD) \cong \mathcal{D}(FC, D) \cong \mathcal{D}^{\mathsf{op}}(D, F^{\mathsf{op}}C)$ □

Die Einheit $\mathrm{Id}_{\mathcal{C}} \to GF$ von $F \dashv G$ heißt dann *Koeinheit* von $G^{\mathsf{op}} \dashv F^{\mathsf{op}}$. Das ist dann eine natürliche Transformation $G^{\mathsf{op}}F^{\mathsf{op}} \to \mathrm{Id}_{\mathcal{C}}$, also von „Linksadjungiert" ∘ „Rechtsadjungiert" nach Identität. Die Adjunktion $G^{\mathsf{op}} \dashv F^{\mathsf{op}}$ hat selbst auch eine Einheit $\mathrm{Id}_{\mathcal{D}} \to F^{\mathsf{op}}G^{\mathsf{op}}$, die widerum die Koeinheit von $F \dashv G$ ergibt:

$$\epsilon \colon FG \to \mathrm{Id}_{\mathcal{D}}$$

Beispiel 5.10. Für die Exponentiation auf Mengen $(-) \times A \dashv (-)^A$ (Beispiel 5.3) ist die Koeinheit Funktionsevaluation:

$$\epsilon_X \colon X^A \times A \longrightarrow X \qquad \epsilon_X(f, a) = f(a)$$

5.2 Von Gruppenoperationen zu Nominalen Mengen

Definition 5.11. Für eine Gruppenoperation $(X, \cdot)$ in $\mathfrak{S}_{\mathsf{f}}(\mathbb{A})$-Set schreiben wir

$$X_{\mathrm{fs}} := \{x \in X \mid x \text{ hat einen endlichen Support}\}.$$

Proposition 5.12. *Der Inklusionsfunktor $J \colon \mathsf{Nom} \to \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$-$\mathsf{Set}$ hat einen Rechtsadjungierten, der auf Objekten durch $(-)_{\mathrm{fs}}$ gegeben ist.*

$$J \dashv (-)_{\mathrm{fs}}$$

Beweis. Wir kombinieren Korollar 5.9 mit Lemma 5.7 und verifizieren: für jedes $\mathfrak{S}_{\mathsf{f}}(\mathbb{A})$-set X gibt es eine äquivariante Abbildung $\epsilon_X \colon J(X_{\mathrm{fs}}) \to X$, sodass für jede äquivariante Abbildung $f \colon JY \to X$ von einer nominalen Menge Y genau ein $h \colon Y \to X_{\mathrm{fs}}$ mit $f = \epsilon_X \circ Jh$ existiert:

$$\begin{tikzcd} X_{\mathrm{fs}} & Y \arrow[l, dashed, "\exists! h"'] \end{tikzcd}$$

$$\begin{tikzcd} J(X_{\mathrm{fs}}) \arrow[d, "\epsilon_X"'] & JY \arrow[l, "Jh"'] \arrow[dl, "f"] \\ X & \end{tikzcd}$$

Die Koeinheit $\epsilon_X\colon J(X_{\mathrm{fs}}) \to X$ ist die Inklusion $X_{\mathrm{fs}} \subseteq X$. Für $f\colon JY \to X$, also einer äquivarianten Abbildung $f\colon Y \to X$, wobei Y eine nominale Menge ist, setzen wir $h := f$. Denn wenn jedes $y \in Y$ einen endlichen Support $S \subseteq \mathbb{A}$ hat, so ist S auch ein endlicher Support von $f(y) \in X$ (Lemma 4.12). Daher ist das Bild von f eine Teilmenge von X_{fs}. Da die Inklusion $\epsilon_X\colon J(X_{\mathrm{fs}}) \to X$ injektiv ist, muss für die Eindeutigkeit nichts weiter gezeigt werden. □

Definition 5.13. Für $\mathfrak{S}_{\mathsf{f}}(\mathbb{A})$-sets X und Y schreiben wir

$$(X \to_{\mathrm{fs}} Y) := \mathsf{Set}(X,Y)_{\mathrm{fs}} = \{f\colon X \to Y \mid f \text{ hat endlichen Support }\}$$

Per Definition ist $X \to_{\mathrm{fs}} Y$ eine nominale Menge. Wenn es aus dem Kontext klar ist, schreiben wir für nominale Mengen X und Y auch einfach

$$Y^X := (X \to_{\mathrm{fs}} Y).$$

Proposition 5.14. *Für alle nominalen Mengen E ist $(-)^E$ rechtsadjungiert zu $(-) \times E$:*

$$(-) \times E \dashv (-)^E \qquad \text{also:} \qquad \frac{X \times E \to Y \text{ in } \mathsf{Nom}}{X \to Y^E \quad \text{in } \mathsf{Nom}}$$

Wie in Set ist auch hier die Koeinheit Funktionsapplikation:

$$\epsilon_X\colon X^E \times E \to X \qquad \epsilon_X(f,e) = f(e)$$

Beweis. Für $f\colon X{\times}E \to Y$ müssen wir zeigen, dass es genau ein $h\colon X \to Y^E$ mit $\epsilon_Y(h(x),e) = f(x,e)$ für alle $x \in X$, $e \in E$ gibt:

$$\begin{tikzcd}
Y^E \times E \arrow[d, "\epsilon_Y"'] & X \times E \arrow[l, "h\times E"'] \arrow[dl, "f"] \\
Y &
\end{tikzcd}$$

Wir definieren h per Currying:

$$h\colon X \to Y^E \qquad h(x) = (e \mapsto f(x,e))$$

Hierfür müssen wir überprüfen, dass $h(x)$ für alle $x \in X$ endlichen Support hat, also in $Y^E = \mathsf{Set}(E,Y)_{\mathrm{fs}} \subseteq \mathsf{Set}(E,Y)$ liegt und dass h äquivariant ist. Beginnen wir mit Äquivarianz, wobei die Gruppenoperation auf Y^E durch Konjugation $\star$ gegeben ist. Für $\pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$:

$$\begin{aligned}
\pi \star h(x) &= \pi \star (e \mapsto f(x,e)) = (e \mapsto \pi \cdot f(x, \pi^{-1} \cdot e)) \\
&= (e \mapsto f(\pi \cdot x, \pi \cdot \pi^{-1} \cdot e)) = (e \mapsto f(\pi \cdot x, e)) = h(\pi \cdot x)
\end{aligned}$$

Hier haben wir genutzt, dass f äquivariant ist. Der endliche Support von x liefert einen endlichen Support von $h(x)$. Für $\pi \in \mathsf{Fix}(\mathsf{supp}(x))$ verifizieren wir:

$$\pi \star h(x) = h(\pi \cdot x) = h(x)$$

In der ersten Gleichung haben wir bereits bewiesene Äquivarianz von h genutzt. Dass h die einzige (äquivariante) Abbildung $X \to Y^E$ mit $f(x,e) = \epsilon_Y(h(x),e) = h(x)(e)$ ist, folgt nun wie in Set. □

Ähnlich wie den Funktionsraum können wir auch die Potenzmenge einschränken: Die Teilmengen $M \subseteq X$ in $\mathfrak{S}_f(\mathbb{A})$-Mengen entsprechen ja den Abbildungen $X \to 2$ (siehe Blatt 2) und analog entspricht $X \to_{fs} 2$ genau den Teilmengen mit endlichem Support:

Definition 5.15. Für $\mathfrak{S}_f(\mathbb{A})$-sets X schreiben wir $\mathcal{P}_{\mathsf{fs}}(X) := (\mathcal{P}(X))_{\mathsf{fs}}$.

Beispiel 5.16. Eine Teilmenge $M \subseteq \mathbb{A}$ hat endlichen Support gdw. sie endlich oder *koendlich* ist, d.h. falls sie selbst oder ihr Komplement endlich ist.

$$\mathsf{supp}_{\mathcal{P}_{\mathsf{fs}}\mathbb{A}}(M) = \begin{cases} M & \text{falls } M \text{ endlich} \\ \mathbb{A} \setminus M & \text{falls } M \text{ koendlich} \end{cases}$$

5.3 Bindungsfunktor

Der Bindungsfunktor $[\mathbb{A}]$ ist sowohl rechts- als auch linksadjungiert. In den Übungen haben wir bereits den Linksadjungierten untersucht:

Proposition 5.17. $(-) * \mathbb{A} \dashv [\mathbb{A}]$.

Beweis. Wie in den Übungen bereits verifiziert, induziert jede äquivariante Abbildung $f\colon X \to [\mathbb{A}]Y$ eine äquivariante Abbildung $h\colon X * \mathbb{A} \to Y$ (und umgekehrt). Die Einheit

$$\eta_X\colon X \to [\mathbb{A}](\mathbb{A} * X) \qquad \eta_X(x) = \langle a\rangle(a, x) \qquad \text{für frisches } a$$

ist wohldefiniert und erfüllt dann $[\mathbb{A}]h \circ \eta_X = f$. □

Für die Konstruktion des Rechtsadjungierten von $[\mathbb{A}]$ nutzen wir die Abbildungen mit endlichem Support und folgendes Ergebnis:

Lemma 5.18. *Für alle $f\colon X \to_{fs} Y$ und $x \in X$ gilt*

$$\mathsf{supp}_Y(f(x)) \subseteq \mathsf{supp}_{Y^X}(f) \cup \mathsf{supp}_X(x)$$

Beweis. Die Koeinheit $\epsilon_Y\colon Y^X \times X \to Y, (f, x) \mapsto f(x)$ der Adjunktion $(-)\times Y \dashv (-)^Y$ ist äquivariant und der Support auf dem Produkt ist durch die Vereinigung gegeben, und damit:

$$\mathsf{supp}_Y(f(x)) = \mathsf{supp}_Y(\epsilon_Y(f, x)) \subseteq \mathsf{supp}_{Y^X \times X}(f, x) = \mathsf{supp}_{Y^X}(f) \cup \mathsf{supp}_X(x) \qquad \square$$

Lemma 5.19. *Wenn $\langle a\rangle x = \langle b\rangle y$ in $[\mathbb{A}]X$ und $a \neq b$, so ist $a \mathrel{\#} y$ und $b \mathrel{\#} x$.*

Beweis. Mittels $\mathsf{supp}(\langle a\rangle x) = \mathsf{supp}(x) \setminus \{a\}$ gilt:

$$a \notin \mathsf{supp}(\langle a\rangle x) = \mathsf{supp}(\langle b\rangle y) = \mathsf{supp}(y) \setminus \{b\}.$$

Durch $a \neq b$ ist $a \notin \mathsf{supp}(y)$, also $a \mathrel{\#} y$ und symmetrisch $b \mathrel{\#} x$. □

Lemma 5.20. *Wenn $\langle a\rangle x = \langle b\rangle y$ in $[\mathbb{A}]X$, so ist $(a\ b) \cdot x = y$.*

Beweis. Per Definition von $\sim_\alpha$ gibt es ein frisches $c \in \mathbb{A}$ mit

$$(a\ \ c) \cdot x = (b\ \ c) \cdot y \qquad \text{also} \qquad (b\ \ c) \cdot (a\ \ c) \cdot x = y$$

Falls $a = b$, so ist $x = y$ und nichts mehr zu zeigen. Falls $a \neq b$, so liefert Lemma 5.19 dass $b \# x$. Zusammen mit der Frischheit $c \notin \mathsf{supp}(x)$ gilt per Lemma 4.18:

$$(a\ \ b) \cdot x = (b\ \ c) \cdot (a\ \ c) \cdot x = y. \qquad \square$$

Bemerkung 5.21. Aus $(a\ \ b) \cdot x = y$ folgt im Allgemeinen nicht $\langle a \rangle x = \langle b \rangle y$. Für $X := \mathcal{P}_\mathsf{f}(\mathbb{A})$ und $a, b \in \mathbb{A}$ gilt

$$(a\ \ b) \cdot \underbrace{\{a, b\}}_{x} = \underbrace{\{a, b\}}_{y} \qquad \text{aber} \qquad \langle a \rangle \{a, b\} \neq \langle b \rangle \{a, b\}.$$

Proposition 5.22. $[\mathbb{A}] \colon \mathsf{Nom} \to \mathsf{Nom}$ *hat einen Rechtsadjungierten* $R \colon \mathsf{Nom} \to \mathsf{Nom}$, *der auf Objekten gegeben ist durch:*

$$RX = \{g \colon \mathbb{A} \to_{\mathrm{fs}} X \mid \textit{für alle } a \in \mathbb{A} \textit{ ist } a \# g(a)\}$$

Die Koeinheit lautet:

$$\epsilon_X \colon [\mathbb{A}](RX) \to X \qquad \epsilon_X(\langle a \rangle g) = g(a)$$

Beweis. Für die Wohldefiniertheit der Koeinheit ϵ sei $\langle a \rangle g = \langle b \rangle g'$. Nach Lemma 5.20 ist $(a\ \ b) \star g = g'$. Falls $a = b$, so ist $g = g'$ und nichts mehr zu zeigen. Falls $a \neq b$, so ist $b \# g$ und

$$g'(b) = ((a\ \ b) \star g)(b) = (a\ \ b) \cdot g((a\ \ b) \cdot b) = (a\ \ b) \cdot g(a)$$

Wegen $g \in RX$ ist $a \# g(a)$. Aus $b \# g$ folgt mittels Lemma 5.18 auch $b \# g(a)$. Insgesamt ist schließlich $(a\ \ b) \cdot g(a) = g(a)$.

Für die universelle Eigenschaft betrachte $f \colon [\mathbb{A}]X \to Y$, wofür wir nachweisen müssen, dass genau ein $h \colon X \to RY$ existiert mit:

$$\begin{tikzcd}
{[\mathbb{A}](RY)} \arrow[d, "\epsilon_Y"'] & {[\mathbb{A}]X} \arrow[l, "{[\mathbb{A}]h}"'] \arrow[dl, "f"] \\
Y &
\end{tikzcd}$$

Definiere $h \colon X \to RY$ via

$$h(x) = (a \mapsto f(\langle a \rangle x))$$

Zur Wohldefiniertheit: Nachdem h durch Currying von $(x, a) \mapsto f(\langle a \rangle x)$ entsteht, liefert die Adjunktion für $(-) \times \mathbb{A} \dashv (-)^A$ sofort, dass $h(x)$ endlichen Support hat. Da f äquivariant ist, folgt $\mathsf{supp}(f(\langle a \rangle x)) \subseteq \mathsf{supp}(x) \setminus \{a\}$ und weiter $a \# h(x)(a)$, was die Bedingung für $h(x) \in RX$ ist.

Der „lange" Pfad im obigen Dreieck vereinfacht sich wie folgt für alle $g \colon X \to RY$ und $\langle a \rangle x \in [\mathbb{A}]X$:

$$(\epsilon_Y \circ [\mathbb{A}]g)(\langle a \rangle x) = \epsilon_Y(([\mathbb{A}]g)(\langle a \rangle x)) = \epsilon_Y(\langle a \rangle (g(x))) = g(x)(a)$$

Somit gilt für alle $g\colon X \to RY$:

$$\epsilon_Y \circ [\mathbb{A}]g = f \quad\Longleftrightarrow\quad f(\langle a\rangle x) = g(x)(a)$$

Die Richtung $\Leftarrow$ zeigt, dass h das gewünschte Dreieck oben kommutieren lässt, und die Richtung $\Rightarrow$ zeigt, dass h die einzige solche Abbildung ist. $\square$

6 Nominale Datenstrukturen

6.1 Funktor-Algebren

Definition 6.1. Für einen Funktor $F\colon \mathcal{C} \to \mathcal{C}$ besteht eine *F-Algebra* (A, a) aus

(a) einem *Träger* $A \in \mathcal{C}$, und

(b) einer *Struktur* $a\colon FA \to A$

Ein Homomorphismus von F-Algebren $h\colon (A, a) \to (B, b)$ ist eine Abbildung $h\colon A \to B$ mit der Eigenschaft $h \cdot a = b \cdot Fh$.

$$\begin{tikzcd}
FA \arrow[r, "a"] \arrow[d, "Fh"] & A \arrow[d, "h"] \\
FB \arrow[r, "b"] & B
\end{tikzcd}$$

$\mathsf{Alg}(F)$ bezeichnet die Kategorie der F-Algebren mit ihren Homomorphismen.

Es ist nicht schwer, nachzuprüfen, dass die Identitäten in $\mathcal{C}$ genau die Identitäten in $\mathsf{Alg}(F)$ sind und dass die Komposition in $\mathsf{Alg}(F)$ genau die Komposition der Grundkategorie $\mathcal{C}$ ist.

Beispiel 6.2. Jede Gruppe $(G, e, \cdot)$ ergibt eine F-Algebra für den Mengenfunktor $F\colon \mathsf{Set} \to \mathsf{Set}$ mit $FX = \{\bullet\} + X \times X$:

$$a\colon FG \to G \qquad a(\mathsf{in}_1(0)) = e \qquad a(\mathsf{in}_2(g, g')) = g \cdot g'$$

Umgekehrt ist nicht jede F-Algebra (A, a) auch eine Gruppe, da $a\colon FA \to A$ keinerlei Axiomen unterliegt.

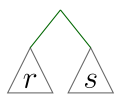
Definition 6.3. Ein Objekt $0 \in \mathcal{C}$ heißt *Initialobjekt*, wenn es für jedes $X \in \mathcal{C}$ genau ein Morphismus $0 \to X$ existiert.

Wenn in einer Kategorie ein Initialobjekt existiert, dann ist es eindeutig bis auf (eindeutigen) Isomorphismus.

Beispiel 6.4. In Set und in Nom ist die leere Menge das (einzige) Initialobjekt.

Die *initiale F-Algebra* ist das Initialobjekt in $\mathsf{Alg}(F)$, sofern eines existiert:

Beispiel 6.5. Für den Mengenfunktor $FX = \{\bullet\} + X \times X$ bilden die Binärbäume den Träger T des Initialobjekts in $\mathsf{Alg}(F)$. Die Struktur $t\colon \{\bullet\} + T \times T \to T$ besteht aus den Konstruktoren: $t(\mathsf{in}_1(\bullet))$ ist ein Baum, der nur aus einem einzigen Blatt besteht, und $t(\mathsf{in}_2(r, s))$ konstruiert aus Binärbäumen r und s einen neuen Baum mit Kindern r und s:

$t(\mathsf{in}_1(\bullet)) = \bullet$ und $t(\mathsf{in}_2(r, s)) =$ 

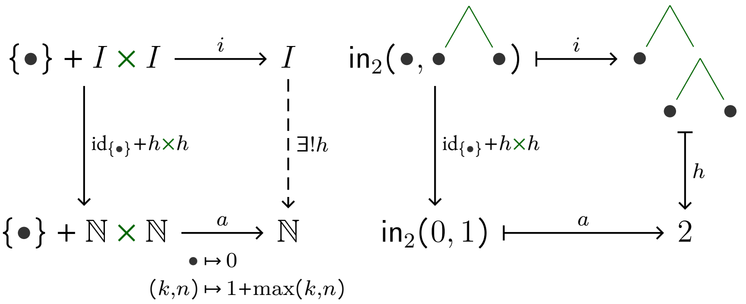


Abbildung 4: Das Homomorphismus-Quadrat für die Höhenberechnung eines Binärbaums

Für jede F-Algebra (A, a) induziert (T, t) einen eindeutigen Homomorphismus $h\colon (T, t) \to (A, a)$. Sei beispielsweise $A = \mathbb{N}$ und a definiert durch

$$a(\mathsf{in}_1(\bullet)) = 0 \qquad a(\mathsf{in}_2(k, n)) = 1 + \max(k, n).$$

Der hierfür induzierte Homomorphismus $h\colon T \to \mathbb{N}$ berechnet die Höhe eines Binärbaums (vgl. Abbildung 4):

$$h(\bullet) = 0 \qquad \text{und} \qquad h\Big(\overset{\wedge}{\triangle_r\ \triangle_s}\Big) = 1 + \max(h(\triangle_r), h(\triangle_s)),$$

Aus ähnlichen Gründen ist Λ der Träger der initialen Algebra für $\mathbb{A} + \mathbb{A} \times (-) + (-) \times (-)$:

Beispiel 6.6. Λ ist Träger der initialen Algebra für

$$F\colon \mathsf{Nom} \to \mathsf{Nom} \qquad FX = \mathbb{A} + \mathbb{A} \times X + X \times X.$$

Die Struktur $\ell_0\colon F\Lambda \to \Lambda$ ist gegeben durch:

$$\ell_0(\mathsf{in}_1(a)) = a \qquad \ell_0(\mathsf{in}_2(a, t)) = \lambda a.\, t \qquad \ell_0(\mathsf{in}_3(r, s)) = r@s$$

6.2 λ-Terme modulo α-Äquivalenz

Theorem 6.7. *$\Lambda/{=_\alpha}$ ist der Träger der initialen Algebra für $G\colon \mathsf{Nom} \to \mathsf{Nom}$, $GX = \mathbb{A} + [\mathbb{A}]X + X \times X$.*

Hierfür nutzen wir die natürlichen Quotienten $q\colon \mathbb{A} \times (-) \to [\mathbb{A}]$ und $\bar{q}\colon F \twoheadrightarrow G$, wobei F der Funktor für λ-Terme ist (Beispiel 6.6).

Beweis. Wir definieren die Struktur: $\ell\colon \mathbb{A} + [\mathbb{A}](\Lambda/{=_\alpha}) + \Lambda/{=_\alpha} \times \Lambda/{=_\alpha}$ via:

$$\ell(\mathsf{in}_1(a)) = [a]_\alpha \qquad \ell(\mathsf{in}_2(\langle a\rangle[t]_\alpha)) = [\lambda a.\, t]_\alpha \qquad \ell(\mathsf{in}_3([r]_\alpha, [s]_\alpha)) = [r@s]_\alpha$$

Wir definieren erst die Wohldefiniertheit von ℓ und danach die universelle Eigenschaft.

Wohldefiniertheit: Die Wohldefiniertheit von $\ell(\mathsf{in}_1(-))$ und $\ell(\mathsf{in}_3(-))$ ist klar. Für die Wohldefiniertheit von $\ell(\mathsf{in}_2(-))$ sei $\langle a\rangle[t]_\alpha = \langle b\rangle[s]_\alpha$. Per Definition von $[\mathbb{A}]$ gibt es ein frisches c mit $(a\ \ c) \cdot [t]_\alpha = (b\ \ c) \cdot [s]_\alpha$, und damit

$$[(a\ \ c) \cdot t]_\alpha = (a\ \ c) \cdot [t]_\alpha = (b\ \ c) \cdot [s]_\alpha = [(b\ \ c) \cdot s]_\alpha$$

und

$$(a\ c) \cdot t =_\alpha (b\ c) \cdot s$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass c frisch ist für t und s (die Definition von $[\mathbb{A}]$ fordert lediglich, dass c frisch für $[t]_\alpha$ und $[s]_\alpha$ ist). Per Regel für die konkrete Relation $=_\alpha$ auf Λ folgt, dass $\lambda a.\, t =_\alpha \lambda b.\, s$ und damit $[\lambda a.\, t]_\alpha = [\lambda b.\, s]_\alpha$, wie gewünscht.

Universelle Eigenschaft: Für eine gegebene G-Algebra $b\colon GB \to B$ definieren wir $f\colon \Lambda \to B$, indem wir die universelle Eigenschaft von (Λ, ℓ_0) auf die F-Algebra $(B, b \circ \bar{q}_B)$ anwenden:

$$\begin{tikzcd}
F\Lambda \arrow[rr, "\ell_0"] \arrow[d, "Ff"'] & & \Lambda \arrow[d, dashed, "\exists! f"] \\
FB \arrow[r, "\bar{q}_B"] & GB \arrow[r, "b"] & B
\end{tikzcd}$$

$$g(a) = g(\mathsf{in}_1(a)) \qquad g(\lambda a.t) = b(\mathsf{in}_2(\langle a \rangle(g(t)))) \qquad g(r@s) = b(\mathsf{in}_3(g(r), g(s)))$$

Wir definieren nun $h\colon \Lambda/{=_\alpha} \to B$ per $h([s]_\alpha) = g(s)$. Für die Wohldefiniertheit überprüfen wir per Induktion, dass für alle $t_1, t_2 \in \Lambda$ mit $t_1 =_\alpha t_2$ auch $f(t_1) = f(t_2)$ gilt:

- Für $a =_\alpha a$ ist nichts für $f(a) = f(a)$ zu zeigen.
- Für $t_1@p_1 =_\alpha t_2@p_2$ gilt $t_1 =_\alpha t_2$ und $p_1 =_\alpha p_2$. Per Induktionshypothese gilt also $f(t_1) = f(t_2)$ und $f(p_1) = f(p_2)$. Da f ein Algebrahomomorphismus ist, gilt ebenso $f(t_1@p_1) = f(t_2@p_2)$.
- Für $\lambda v_1.t_1 =_\alpha \lambda v_2.t_2$ existiert ein frisches c mit $(v_1\ c) \cdot t_1 =_\alpha (v_2\ c) \cdot t_2$ (Definition der expliziten α-Äquivalenz auf Λ). Per Induktionshypothese und Äquivarianz von f folgt

  $$(v_1\ c) \cdot f(t_1) = f((v_1\ c) \cdot t_1) = f((v_2\ c) \cdot t_2) = (v_2\ c) \cdot f(t_2)$$

  Per Äquivarianz von f ist c auch frisch für $f(t_1)$ und $f(t_2)$ und per Definition der abstrakten α-Äquivalenz auf $\mathbb{A} \times (-)$ folgt:

  $$\langle v_1 \rangle (f(t_1)) = \langle v_2 \rangle (f(t_2))$$

  und damit:

  $$\begin{aligned} f(\lambda v_1.t_1) &= f(l_0(\mathsf{in}_2(v_1, t_1))) = b(\bar{q}_B(Ff(\mathsf{in}_2(v_1, t_1)))) = b(\mathsf{in}_2(q_B(v_1, f(t_1)))) \\ &= b(\mathsf{in}_2(\langle v_1 \rangle (f(t_1)))) = b(\mathsf{in}_2(\langle v_2 \rangle (f(t_2)))) = \cdots = f(\lambda v_2.t_2) \end{aligned}$$

Somit ist $h\colon \Lambda/{=_\alpha} \to B$ wohldefiniert und erfüllt $h \circ [-]_\alpha = f$. Für die benötigte Homomorphieeigenschaft genügt es, folgendes Diagramm zu betrachten:

$$\begin{tikzcd}
F\Lambda \arrow[rr, "\ell_0"] \arrow[d, two heads, "\bar{q}_\Lambda"'] \arrow[dd, bend right=60, "Ff"'] \arrow[drr, phantom, "\text{Def. } \ell"] & & \Lambda \arrow[d, two heads, "{[-]_\alpha}"] \arrow[dd, bend left=60, "f"] \\
G\Lambda \arrow[r, two heads, "{G[-]_\alpha}"] \arrow[dr, "Gf"'] \arrow[d, phantom, "\text{Nat. } \bar{q}"] & G(\Lambda/{=_\alpha}) \arrow[r, "\ell"] \arrow[d, "Gh"] \arrow[dr, phantom, "?"] & \Lambda/{=_\alpha} \arrow[d, "h"] \\
FB \arrow[r, "\bar{q}_B"'] & GB \arrow[r, "b"'] & B
\end{tikzcd}$$

$$\begin{aligned} FX &= \mathbb{A} + \mathbb{A} \times X + X \times X \\ GX &= \mathbb{A} + [\mathbb{A}]X + X \times X \end{aligned}$$

Das obere Quadrat kommutiert genau, weil ℓ wohldefiniert ist (vgl. Definition von ℓ oben). Das äußere Quadrat kommutiert per Definition von f. Da die Abbildung $G[-]_\alpha \circ \bar{q}_\Lambda$ ein Epimorphismus in Nom ist, kommutiert auch das untere gewünschte Quadrat, also ist h ein Homomorphismus von G-Algebren.

Die Eindeutigkeit von h folgt aus der Eindeutigkeit von f, wieder mittels des Epimorphismus $[-]_\alpha \colon \Lambda \twoheadrightarrow \Lambda/{=_\alpha}$. □

Das Überraschende an diesem Resultat ist, dass es also egal ist, ob man α-Äquivalenz für komplette Terme definiert (wie zu Beginn von Abschnitt 4.2) oder ob man α-Äquivalenz ebenenweise betrachtet.

Beispiel 6.8. $(x\ \ y) \cdot [(\lambda x.x)\,x]_\alpha = [(x\ \ y) \cdot ((\lambda y.y)\,y)]_\alpha$.

Beispiel 6.9. Wir können capture-avoiding Substitution als äquivariante Abbildung

$$\frac{\mathsf{subst}\colon \quad \Lambda/{=_\alpha} \times \mathbb{A} \times \Lambda/{=_\alpha} \longrightarrow \Lambda/{=_\alpha}}{\overline{\mathsf{subst}}\colon \quad \Lambda/{=_\alpha} \longrightarrow \mathbb{A} \times \Lambda/{=_\alpha} \to_{\mathsf{fs}} \Lambda/{=_\alpha}}$$

rekursiv definieren, indem wir eine passende Algebra-Struktur

$$r\colon \mathbb{A} + [\mathbb{A}]R + R \times R \longrightarrow R \quad \text{auf} \quad R := (\Lambda/{=_\alpha}^{\mathbb{A}\times\Lambda/=_\alpha})_{\mathsf{fs}}$$

definieren:

$$\begin{aligned} r(\mathsf{in}_1 \underbrace{a}_{\in\, \mathbb{A}}) &= \overbrace{(b,t) \mapsto \begin{cases} t & \text{falls } a = b \\ a & \text{falls } a \neq b \end{cases}}^{\mathbb{A}\times\Lambda/=_\alpha \longrightarrow_{\mathsf{fs}} \Lambda/=_\alpha} \\ r(\mathsf{in}_3(\underbrace{f @ p}_{\in\, R \times R})) &= (b,t) \mapsto \ell(\mathsf{in}_3(f(b,t) @ p(b,t))) \\ r(\mathsf{in}_2(\underbrace{\langle a \rangle s}_{\in\, [\mathbb{A}]R})) &= (b,t) \mapsto \ell(\mathsf{in}_2(\langle a \rangle (s(b,t)))) \end{aligned}$$

Im Fall der Variablenbindung müssen wir nicht explizit nach $a = b$ unterscheiden. Wegen des Bindungsfunktors und weil das Frische Produkt $(-) * \mathbb{A}$ dessen Linksadjungierter ist, wurde der Repräsentant $\langle a \rangle s$ schon automatisch so gewählt, dass $a \neq b$.

7 Automatentheorie

In der üblichen Theorie deterministischer endlicher Automaten spiegelt sich der Aspekt der Endlichkeit nicht nur in der Zustandsmenge, sondern auch im Eingebealphabet Σ wider. Der Grund dafür ist, dass für unendliche Eingabealphabete selbst einfach strukturierte Sprachen wie die folgende nicht von endlichen Automaten erkannt werden können:

Beispiel 7.1 (Übungsaufgabe)**.** Für ein unendliches Eingabealphabet Σ gibt es keinen *endlichen* deterministischen Automaten, der folgende Sprache akzeptiert:

$$L := \{awa \mid a \in \Sigma, w \in \Sigma^*\}$$

Wäre Σ endlich, so gibt es einen deterministischen Automaten mit $1+2\cdot|\Sigma|$ Zuständen: Für das erste Eingabesymbol a merkt sich der Automat das Zeichen a im Zustand und wechselt anschließend zwischen einem finalen und nichtfinalen Zustand, je nach dem, ob das letzte Eingabezeichen a war oder nicht, siehe Abbildung 5. Mittels nominaler Mengen, können wir diesen Akt des Merkens explizit machen und auch unendliche Eingabealphabete unterstützen.

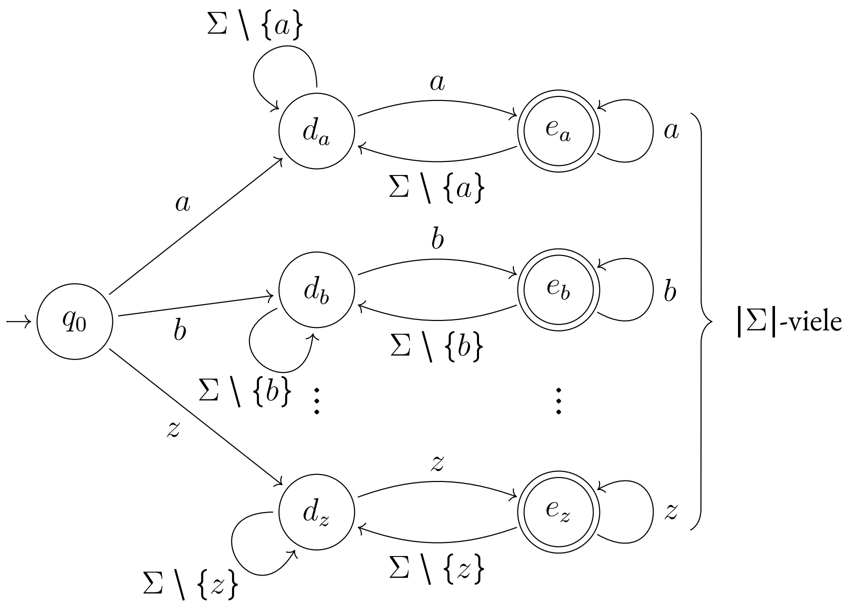


Abbildung 5: Ein Automat für $L = \{awa \mid a \in \Sigma, w \in \Sigma^*\}$

Definition 7.2. Für eine nominale Menge Σ, genannt *(Eingabe)alphabet* besteht ein nichtdeterministischer nominaler Automat aus folgenden Daten:

(a) Einer nominalen *Zustandsmenge* Q

(b) Einer äquivarianten *Übergangsrelation* $\delta \subseteq Q \times \Sigma \times Q$.

(c) Äquivarianten Teilmengen $I \subseteq Q$ und $F \subseteq Q$ von *Initial-* und *Finalzuständen*.

Ein nominaler Automat heißt

- orbit-endlich (*NOFA*), wenn Q orbit-endlich ist,

- deterministisch, wenn δ der Graph einer Funktion $Q \times \Sigma \to Q$ und I einelementig ist.
- *DOFA*, wenn er deterministisch und orbit-endlich ist.
- endlich, wenn Q endlich ist.

Lemma 7.3. *Wenn ein nominaler Automat deterministisch ist, dann ist $\delta \colon Q \times \Sigma \to Q$ eine äquivariante Abbildung.*

Beweis. Einfaches Durchrechnen. □

Beispiel 7.4. Die endlichen nominalen Automaten sind genau die üblichen (deterministischen bzw. nichtdeterministischen) endlichen Automaten.

7.1 Sprachsemantik

Definition 7.5. Ein *Lauf* (engl.: run) eines Worts $a_1 \cdots a_k = w \in \Sigma^*$ (der Länge k) ist eine Sequenz von $k + 1$ Zuständen $q_0, \ldots, q_k \in Q$ mit $(q_i, a_{i+1}, q_{i+1}) \in \delta$ für alle $i < k$. Ein Lauf $q_0, \ldots, q_k$ ist *akzeptierend*, wenn $q_k \in F$.

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \longrightarrow \cdots \longrightarrow q_{k-1} \xrightarrow{a_k} q_k$$

Die *Sprache* $L(q) \subseteq \Sigma^*$ eines Zustands $q \in Q$ eines nominalen Automaten ist durch

$$L(q) = \{w \in \Sigma^* \mid w \text{ hat einen akzeptierenden Lauf } q_0, q_1, \ldots \text{ mit } q_0 = q\}$$

definiert. Alternativ kann man $L(q)$ rekursiv definieren:

$$L(q) := \{\epsilon \mid q \in F\} \cup \{aw \in \Sigma^* \mid a \in \Sigma, q' \in Q, (q, a, q') \in \delta, w \in L(q')\}$$

Die Sprache *des Automaten* ist dann die Sprache seiner Initialzustände:

$$L := \bigcup_{q \in I} L(q)$$

Beispiel 7.6. Für jede nominale Menge Σ wird die Sprache

$$L := \{awa \mid a \in \Sigma, w \in \Sigma^*\}$$

von einem Automat mit der nominalen Zustandsmenge $Q := 1 + 2 \times \Sigma$ akzeptiert:

- $I := \mathsf{in}_1(\bullet)$
- $F := \{(1, a) \mid a \in \Sigma\}$
- $$\begin{aligned} \delta := {} & \{(\bullet, a, (0, a)) \in Q \times \Sigma \times Q \mid a \in \Sigma\} \\ \cup {} & \{((k, a), a, (1, a)) \in Q \times \Sigma \times Q \mid k \in 2, a \in \Sigma\} \\ \cup {} & \{((k, a), b, (0, a)) \in Q \times \Sigma \times Q \mid k \in 2, a, b \in \Sigma, a \neq b\} \end{aligned}$$

Die Übergange sind wie im endlichen Fall in Abbildung 5 zu verstehen. Tatsächlich ist δ der Graph einer Funktion:

$$\delta(\bullet, a) = (1, a) \qquad \delta((k,a), b) = \begin{cases} (1,a) & \text{falls } a = b \\ (0,a) & \text{falls } a \neq b \end{cases}$$

Für speziellere Eingabealphabete Σ erhalten wir:

- Wenn Σ orbit-endlich ist, so ist auch Q orbit-endlich.
- Wenn Σ sogar endlich ist, so dann auch Q.

Beispiel 7.7 (Übungsaufgabe)**.** Die Sprache $L = \{wavau \mid w, v, u \in \Sigma^*, a \in \Sigma\}$ (mindestens ein Zeichen kommt mindestens zweimal vor) wird von einem NOFA erkannt.

Theorem 7.8 (Übungsaufgabe)**.** *Die Semantik eines nominalen Automaten $L\colon Q \to \mathcal{P}_{\mathsf{fs}}(\Sigma^*)$ ist äquivariant.*

7.2 Abschlusseigenschaften

Proposition 7.9. *Die Sprache*

$$L^{\sharp *} := \{a_1 \cdots a_k \mid k \in \mathbb{N}, a_i \in \mathbb{A} \textit{ paarweise verschieden}\}$$

wird von keinem orbit-endlichen Automaten erkannt.

Beweis. Sei Q die Zustandsmenge eines orbit-endlichen Automaten, der $L^{\sharp *}$ akzeptiert. Auf Grund der Orbit-Endlichkeit von Q existiert das Maximum:

$$n := 1 + \max_{q \in Q} |\mathsf{supp}(q)|$$

Wähle $k := 2 \cdot n$ *verschiedene* Atome $a_1, \ldots, a_{2 \cdot n} \in \mathbb{A}$, womit wir ein Wort

$$a_1 \cdots a_{2 \cdot n} \;\in\; L^{\sharp *}$$

in der Sprache erhalten. Für dieses Wort muss mindestens ein akzeptierender Lauf des Automaten existieren:

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{\cdots} q_{n-1} \xrightarrow{a_n} q_n \xrightarrow{a_{n+1}} q_{n+1} \xrightarrow{\cdots} q_{2n-1} \xrightarrow{a_{2 \cdot n}} \boxed{q_{2 \cdot n}}$$

Per Definition von n ist $|\mathsf{supp}(q_n)| < n$, also gilt:

$$|\{a_1, \ldots, a_n\}| > |\mathsf{supp}(q_n)| \qquad \text{und} \qquad |\{a_{n+1}, \ldots, a_{2 \cdot n}\}| > |\mathsf{supp}(q_n)|$$

Sei $a_i \in \{a_1, \ldots, a_n\} \setminus \mathsf{supp}(q_n)$, $a_j \in \{a_{n+1}, \ldots, a_{2n}\} \setminus \mathsf{supp}(q_n)$ und setze $\pi := (a_i \;\; a_j)$. Per Support von q_n erhalten wir

$$\pi \cdot q_n = q_n.$$

Das nutzen wir, um die erste Hälfte des obigen Laufs mittels π umzubenennen und den Rest unverändert zu lassen: Aus der Äquivarianz von δ erhalten wir den Lauf

$$\begin{tikzcd}
q_0 \arrow[r, "a_1"] & q_1 \arrow[r, "\cdots"] & q_{n-1} \arrow[r, "a_n"] & q_n \arrow[r, "a_{n+1}"] \arrow[d, equal] & q_{n+1} \arrow[r, "\cdots"] & q_{2n-1} \arrow[r, "a_{2\cdot n}"] & q_{2\cdot n} \\
\pi\cdot q_0 \arrow[r, "\pi \cdot a_1"] & \pi\cdot q_1 \arrow[r, "\cdots"] & \pi\cdot q_{n-1} \arrow[r, "\pi \cdot a_n"] & \pi\cdot q_n & & &
\end{tikzcd}$$

Per Äquivarianz von I erhalten wir $\pi \cdot q_0 \in I$. Also akzeptiert der NOFA das Wort

$$(\pi \cdot a_1) \cdots (\pi \cdot a_n)\ a_{n+1} \cdots a_{2\cdot n}.$$

Das ist aber ein Widerspruch, weil dieses Wort das Atom $a_j = \pi(a_i)$ zweimal enthält und daher nicht in $L^{\sharp *}$ enthalten ist. □

Korollar 7.10. *Die Klasse der Sprachen, die von NOFAs erkannt wird, ist nicht abgeschlossen unter Komplement.*

Beweis. Die Sprache aus Beispiel 7.7 wird von einem NOFA erkannt, deren Komplement jedoch nicht (Proposition 7.9). □

Lemma 7.11. *Die Klasse der Sprachen, die von DOFAs erkannt wird, ist abgeschlossen unter Komplement.*

Daraus ergibt sich, dass die Determinisierung von NOFAs im allgemeinen fehlschlägt; es gibt also NOFAs deren Sprache von keinem DOFA erkannt wird:

Korollar 7.12. *Nicht alle NOFAs lassen sich determinisieren.*

Beweis. Betrachte den NOFA zur Sprache $L = \{wavau \mid w, v, u \in \Sigma^*, a \in \Sigma\}$ aus Beispiel 7.7. Gäbe es einen DOFA, der L erkennt, so gäbe es nach Lemma 7.11 auch einen DOFA, der dessen Komplement $L^{\sharp *} = \Sigma^* \setminus L$ erkennt. Es gibt jedoch nicht einmal einen NOFA für $\Sigma^* \setminus L$ (Proposition 7.9). □

8 Prägarben: Nominale Mengen im Kontext

Um Terme mit eingebetteten Variablen aus $\mathbb{A}$ als mathematische Struktur zu modellieren, gibt es (mindestens) zwei grundsätzliche Herangehensweisen:

1. Variante 1: Für einen gegebenen Term t kann ich per Struktur abfragen, welche Variablen $\mathsf{supp}(t) \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ darin (frei) vorkommen. Wie wir gesehen haben, muss $\mathsf{supp}(t)$ gewisse Axiome erfüllen, um mit der Intuition von Variablen verträglich zu sein.

2. Variante 2: Für eine gegebene (endliche) Menge von Variablen $S \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ kann ich per Struktur abfragen, welche Terme man unter Verwendung (ausschließlich) dieser Variablen S bauen könnte. Die Menge S ist also ein *Kontext*, in dem ein Term existiert.

Welche Axiome sollte man bei Termen in Kontexten einfordern? Hier einige Vorschläge:

- *Monotonie*: Wenn $S \subseteq S'$ und $S, S' \in \mathcal{P}_\mathsf{f}(\mathbb{A})$, dann sollte jeder Term t, der sich mittels der Variablen aus S bauen lässt, auch mit den mehr zur Verfügung stehenden Variablen S' bauen lassen.
- *Opake Namen*: Die Terme t, die ich aus $S \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ bauen kann, sollte nicht von der konkreten Wahl der Namen abhängig sein: aus $\{a, b\}$ sollten bis auf Umbenennung die selben Terme wie aus $\{v, w\}$ bildbar sein.
- *Schnitterhaltung*: Wenn ich einen Term t sowohl mittels der Variablen $S \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ als auch mittels $S' \in \mathcal{P}_\mathsf{f}(\mathbb{A})$, dann sollten im Term nur solche Variablen vorkommen, die sowohl in S als auch in S' enthalten sind. Und damit sollte es auch möglich sein, den Term t aus $S \cap S'$ zu bauen.

Die ersten zwei Axiome treffen Aussagen zu injektiven Abbildungen zwischen Kontexten:

Definition 8.1. Die Kategorie $\mathbb{I}$ der *Kontexte* enthält folgende Daten:

- Objekte: $\mathbf{obj}\,\mathbb{I} := \mathcal{P}_\mathsf{f}(\mathbb{A})$. Wir nennen eine endliche Teilmenge $\Gamma \in \mathcal{P}_\mathsf{f}(\mathbb{A})$ *Kontext*.
- Morphismen: $\mathbb{I}(\Gamma, \Delta) := \{\varrho\colon \Gamma \to \Delta \mid \varrho \text{ injektiv }\}$.
- Identitäten und Komposition sind wie in Set.

Die Kategorie der kontextabhängigen Strukturen ist dann die Funktorkategorie:

$$[\mathbb{I}, \mathsf{Set}]$$

Dies ist eine Kategorie, da $\mathbb{I}$ klein ist. Ein Objekt $X \in \mathbf{obj}[\mathbb{I}, \mathsf{Set}]$ nennt man *Prägarbe* (engl.: Presheaf). Wir verstehen ein solches X als Zuordnungsvorschrift, die jedem Kontext $\Gamma \in \mathbb{I}$ eine Menge von Termen $X(\Gamma) \in \mathsf{Set}$ zuordnet, die intuitiv im Kontext Γ existieren. Für jede (injektive) Umbenennung $\varrho\colon \Gamma \rightarrowtail \Delta$ erhalten wir eine Abbildung $X(\varrho)\colon X(\Gamma) \to X(\Delta)$, die Terme im Kontext Γ auf Terme im Kontext Δ abbildet.

8.1 Adjunktion zu Nominalen Mengen

Im Folgenden werden wir die Kategorie der nominalen Mengen Nom per Adjunktion zur Funktorkategorie $[\mathbb{I}, \mathsf{Set}]$ in Beziehung setzen und zeigen, dass Nom genau den schnitterhaltenden Funktoren in $[\mathbb{I}, \mathsf{Set}]$ entspricht.

Notation 8.2. Für eine Abbildung $f\colon X \to Y$ und $Z \subseteq X$ bezeichnet $f|_Z\colon Z \to f[Z]$, $z \mapsto f(z)$ die *Restriktion* von f auf den Definitionsbereich Z.

Definition 8.3. Setze $K\colon \mathsf{Nom} \to [\mathbb{I}, \mathsf{Set}]$ per:

$$\begin{aligned}(KX)(\Gamma) &:= \{x \in X \mid \mathsf{supp}(x) \subseteq \Gamma\}\\ &= \{x \in X \mid \Gamma \text{ ist ein Support von } x\}\end{aligned}$$

Für $\varrho\colon \Gamma \rightarrowtail \Delta$ setze $KX(\varrho)\colon KX(\Gamma) \to KX(\Delta)$ per:

$$KX(\varrho)(x) = \pi \cdot x \qquad \text{für beliebiges } \pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A}) \text{ mit } \pi|_\Gamma = \varrho \tag{8.1}$$

Für jede äquivariante Abbildung $f\colon X \to Y$ und $\Gamma \in \mathbb{I}$ setze

$$(Kf)_\Gamma\colon KX(\Gamma) \to KY(\Gamma) \qquad (Kf)_\Gamma(x) = f(x) \tag{8.2}$$

Bemerkung 8.4. Die Bedingung $\pi|_\Gamma = \varrho$ bezieht sich lediglich darauf, dass der Graph der Funktionen identisch ist, also $\forall a \in \Gamma\colon \pi(a) = \varrho(a)$.

Proposition 8.5. *K ist ein wohldefinierter Funktor* $\mathsf{Nom} \to [\mathbb{I}, \mathsf{Set}]$.

Beweis. Für jede nominale Menge $X \in \mathsf{Nom}$ verifizieren wir zunächst, dass KX ein Funktor $\mathbb{I} \to \mathsf{Set}$ ist:

- Für die Definition auf Objekten ist nichts zu zeigen.
- Wohldefiniertheit von $KX(\varrho)(x)$: per Lemma 4.18 ist $\pi \cdot x$ unabhängig von der Wahl von π. Per A4 auf Blatt 5 gibt es mindestens ein solches $\pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$.
- $KX(\varrho)(x) \in KX(\Delta)$: da supp äquivariant ist, folgt aus $\mathsf{supp}(x) \subseteq \Gamma$ auch

  $$\mathsf{supp}(\pi \cdot x) = \pi \cdot \mathsf{supp}(x) \subseteq \pi \cdot \Gamma = \pi[\Gamma] = \varrho[\Gamma] \subseteq \Delta$$

  und damit ist $\pi \cdot x$ ein Element von $KX(\Delta)$.
- KX erhält Identitäten: für $\varrho = \mathrm{id}_\Gamma$ kann $\pi = \mathrm{id}_{\mathbb{A}}$ gewählt werden:

  $$KX(\mathrm{id}_\Gamma)(x) = \mathrm{id}_{\mathbb{A}} \cdot x = x \qquad \text{also} \qquad KX(\mathrm{id}_\Gamma) = \mathrm{id}_{KX(\Gamma)}$$

- KX erhält Komposition: für $\varrho\colon \Gamma \rightarrowtail \Delta$ und $\varrho'\colon \Delta \rightarrowtail \Delta'$ mit entsprechenden $\pi, \pi' \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$ erfüllt auch $(\pi' \cdot \pi)$ die gewünschte Eigenschaft für $(\varrho' \circ \varrho)\colon \Gamma \rightarrowtail \Delta'$ aus (8.1):

  $$KX(\varrho')(KX(\varrho)(x)) = \pi' \cdot (\pi \cdot x) = (\pi' \cdot \pi) \cdot x = KX(\varrho' \circ \varrho)(x)$$

Es bleibt noch zu prüfen, dass wir für jede äquivariante Abbildung $f\colon X \to Y$ eine natürliche Transformation $Kf\colon KX \to KY$ (zwischen den Funktoren $KX, KY\colon \mathbb{I} \to \mathsf{Set}$) erhalten. Zunächst ist für jedes $\Gamma \in \mathbb{I}$ und $x \in KX(\Gamma)$ in der Tat auch $(Kf)_\Gamma(x)$ in $KY(\Gamma)$, da $\mathsf{supp}(f(x)) \subseteq \mathsf{supp}(x) \subseteq \Gamma$ (Korollar 4.13). Für $\varrho\colon \Gamma \rightarrowtail \Delta$ lautet das zu prüfende Natürlichkeitsquadrat:

$$\begin{tikzcd} \Gamma \arrow[d, tail, "\varrho"'] & KX(\Gamma) \arrow[r, "(Kf)_\Gamma"] \arrow[d, "KY(\varrho)"'] & KY(\Gamma) \arrow[d, "KY(\varrho)"] \\ \Delta & KX(\Delta) \arrow[r, "(Kf)_\Delta"] & KY(\Delta) \end{tikzcd}$$

Für $x \in KX(\Gamma)$ und zu ϱ passendes $\pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A})$ gilt:

$$\begin{aligned}
KY(\varrho)((Kf)_\Gamma(x)) &= KY(\varrho)(f(x)) = \pi \cdot f(x) && (\pi|_\Gamma = \varrho) \\
&= f(\pi \cdot x) && (f \text{ äquivariant}) \\
&= (Kf)_\Delta(\pi \cdot x) \\
&= (Kf)_\Delta(KY(\varrho)(x)) && (\pi|_\Gamma = \varrho)
\end{aligned}$$

Aus der Definition von Kf ist sofort klar, dass K Identitäten und Komposition erhält. □

Definition 8.6. Aus einer Prägarbe $F\colon \mathbb{I} \to \mathsf{Set}$ konstruieren wir die nominale Menge

$$JF := \{(\Gamma, x) \mid \Gamma \in \mathcal{P}_{\mathsf{f}}(\mathbb{A}), x \in F\Gamma\}/\sim$$

wobei die Relation $\sim$ definiert ist durch:

$$(\Gamma, x) \sim (\Delta, y) \quad :\Longleftrightarrow \quad \exists \Upsilon \supseteq \Gamma \cup \Delta\colon\ F(\Gamma \hookrightarrow \Upsilon)(x) = F(\Delta \hookrightarrow \Upsilon)(y)$$

Intuitiv identifiziert $\sim$ zwei Terme aus unterschiedlichen Kontexten, wenn sie in irgendeinem größeren Kontext den gleichen Term bezeichnen. Hier bezeichnet $\Delta \hookrightarrow \Upsilon$ die Injektion einer Teilmenge Δ in eine Obermenge Υ.

Lemma 8.7. *$\sim$ ist eine Äquivalenzrelation.*

Beweis. Reflexivität und Symmetrie sind klar. Betrachte für die Transitivität die Paare

$$(\Gamma, x) \sim (\Delta, y) \quad \text{und} \quad (\Delta, y) \sim (\Theta, z)$$

mit den Zeugen Υ_1 und Υ_2. In $\mathbb{I}$ kommutiert folgendes Diagramm, da es nur aus Teilmengeninklusionen besteht:

$$\begin{tikzcd}
& & \Upsilon_1 \cup \Upsilon_2 & & \\
& \Upsilon_1 \arrow[ur, hook] & & \Upsilon_2 \arrow[ul, hook'] & \\
\Gamma \arrow[ur, hook] \arrow[uurr, hook, bend left] & & \Delta \arrow[ul, hook'] \arrow[ur, hook] & & \Theta \arrow[ul, hook'] \arrow[uull, hook', bend right]
\end{tikzcd}$$

Folglich ist $\Upsilon_1 \cup \Upsilon_2$ die obere Schranke, die $(\Gamma, x) \sim (\Theta, z)$ bezeugt:

$$\begin{aligned}
F(\Gamma \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(x) &= F(\Upsilon_1 \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(F(\Gamma \hookrightarrow \Upsilon_1)(x)) \\
&= F(\Upsilon_1 \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(F(\Delta \hookrightarrow \Upsilon_1)(y)) \\
&= F(\Upsilon_2 \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(F(\Delta \hookrightarrow \Upsilon_2)(y)) \\
&= F(\Upsilon_2 \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(F(\Theta \hookrightarrow \Upsilon_2)(z)) \\
&= F(\Theta \hookrightarrow \Upsilon_1 \cup \Upsilon_2)(z)
\end{aligned}$$

□

Wir schreiben $[\Gamma, x]_\sim$ für die Äquivalenzklasse von (Γ, x) in JF.

Lemma 8.8. *Für alle $F\colon \mathbb{I} \to \mathsf{Set}$ ist JF eine nominale Menge mittels der Gruppenwirkung*

$$\pi \cdot [\Gamma, x]_\sim = \big[\pi[\Gamma], F(\pi|_\Gamma)(x)\big]_\sim \qquad \text{für } \pi \in \mathfrak{S}_{\mathsf{f}}(\mathbb{A}) \text{ und } [\Gamma, x]_\sim \in JF.$$

Beweis. 1. Die Gruppenwirkung ist wohldefiniert: Sei $(\Gamma, x) \sim (\Delta, y)$ durch $\Upsilon \supseteq \Gamma \cup \Delta$ mit $F(\Gamma \hookrightarrow \Upsilon)(x) = F(\Delta \hookrightarrow \Upsilon)(y)$ bezeugt. In $\mathbb{I}$ kommutiert das linke Diagramm:

$$\begin{tikzcd}
\Gamma \arrow[r, hook] \arrow[d, "\pi|_\Gamma"'] & \Upsilon \arrow[d, "\pi|_\Upsilon"] & \Delta \arrow[l, hook'] \arrow[d, "\pi|_\Delta"] \\
\pi[\Gamma] \arrow[r, hook] & \pi[\Upsilon] & \pi[\Delta] \arrow[l, hook']
\end{tikzcd}
\quad \overset{F}{\longmapsto} \quad
\begin{tikzcd}
x \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] & & y \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] \\
F\Gamma \arrow[r, hook] \arrow[d, "F(\pi|_\Gamma)"'] & F\Upsilon \arrow[d, "F(\pi|_\Upsilon)"] & F\Delta \arrow[l, hook'] \arrow[d, "F(\pi|_\Delta)"] \\
F(\pi[\Gamma]) \arrow[r, hook] & F(\pi[\Upsilon]) & F(\pi[\Delta]) \arrow[l, hook']
\end{tikzcd}$$

Der Funktor F schickt das Diagramm auf das rechte, das bezeugt, dass

$$(\pi[\Gamma], F(\pi|_\Gamma)(x)) \sim (\pi[\Delta], F(\pi|_\Delta)(y)).$$

2. Die Axiome der Gruppenwirkung folgen direkt aus der Funktorialität von F.
3. Die Menge $\Gamma \subseteq \mathbb{A}$ ist ein endlicher Support von $[\Gamma, x]_\sim$, denn für alle $\pi \in \mathsf{Fix}(\Gamma)$ gilt $\pi|_\Gamma = \mathrm{id}_\Gamma$ und damit:

$$\pi \cdot [\Gamma, x]_\sim = [\pi[\Gamma], F(\pi|_\Gamma)(x)]_\sim = [\Gamma, F(\mathrm{id}_\Gamma)(x)]_\sim = [\Gamma, x]_\sim \qquad \square$$

Die Adjunktion $J \dashv K$ zwischen $[\mathbb{I}, \mathsf{Set}]$ und Nom werden wir mittels Lemma 5.7 beweisen, wofür wir eine Familie von Morphismen

$$\eta_F\colon \quad F \to KJF \qquad \text{in } [\mathbb{I}, \mathsf{Set}] \text{ für jedes } F\colon \mathbb{I} \to \mathsf{Set}$$

angeben, die dann die Einheit der Adjunktion bilden. Zwar wird sich die Natürlichkeit von η in F automatisch aus dem zu nutzenden Lemma 5.7 ergeben, jedoch müssen wir zuerst verifizieren, dass jedes η_F auch ein Morphismus in der Funktorkategorie $[\mathbb{I}, \mathsf{Set}]$ ist:

Lemma 8.9. *Für jede Prägarbe $F\colon \mathbb{I} \to \mathsf{Set}$ gibt es*

$$\eta_F \in [\mathbb{I}, \mathsf{Set}](F, KJF) \quad \textit{definiert durch} \quad (\eta_F)_\Gamma\colon \begin{array}{ccc} F(\Gamma) & \to & K(JF)(\Gamma) \\ x & \mapsto & [\Gamma, x]_\sim \end{array} \qquad \text{für } \Gamma \in \mathbb{I}.$$

Beweis. $(\eta_F)_\Gamma(x)$ ist wohldefiniert, weil Γ ein Support von $[\Gamma, x]_\sim \in JF$ ist und damit ist $[\Gamma, x]_\sim \in K(JF)(\Gamma)$. Für die Natürlichkeit von $(\eta_F)_\Gamma$ in Γ sei $\varrho\colon \Gamma \rightarrowtail \Delta$ in $\mathbb{I}$ und ein beliebiges $\pi \in \mathfrak{S}_\mathsf{f}(\mathbb{A})$ mit $\pi|_\Gamma = \varrho$:

$$\begin{tikzcd}
 & x \arrow[rrr, mapsto] \arrow[ddd, mapsto] \arrow[dr, phantom, "\in"] & & & {[\Gamma, x]_\sim} \arrow[dd, mapsto, "\text{da } \pi|_\Gamma = \varrho"] \arrow[dl, phantom, "\ni"] \\
\Gamma \arrow[d, tail, "\varrho"'] & & F\Gamma \arrow[r, "(\eta_F)_\Gamma"] \arrow[d, "F\varrho"'] & K(JF)(\Gamma) \arrow[d, "K(JF)(\varrho)"] & \\
\Delta & & F\Delta \arrow[r, "(\eta_F)_\Delta"] & K(JF)(\Delta) & \pi \cdot [\Gamma, x]_\sim \arrow[d, phantom, "\parallel\ (\text{Def.} \cdot \text{auf } JF)"] \\
 & F\varrho(x) \arrow[rr, mapsto] \arrow[ur, phantom, "\in"] & & {[\Delta, F\varrho(x)]_\sim} \arrow[r, phantom, "\overset{?}{=}"] & {[\pi[\Gamma], F(\pi|_\Gamma)(x)]_\sim}
\end{tikzcd}$$

Die noch zu zeigende Gleichheit der Äquivalenzklassen $(\Delta, F\varrho(x)) \sim (\pi[\Gamma], F(\pi|_\Gamma)(x))$ wird durch die obere Schranke $\Upsilon := \Delta$ bezeugt, da $\pi[\Gamma] = \varrho[\Gamma] \subseteq \Delta$:

$$\begin{aligned} F(\Delta \hookrightarrow \Delta)(F\varrho(x)) = F\varrho(x) &= F((\pi[\Gamma] \hookrightarrow \Delta) \circ \pi|_\Gamma)(x) \\ &= F(\pi[\Gamma] \hookrightarrow \Delta)(F(\pi|_\Gamma)(x)) \end{aligned}$$

Somit ist η_F in der Tat eine natürliche Transformation, also liegt η_F in $[\mathbb{I}, \mathsf{Set}]$. $\square$

Theorem 8.10. *J lässt sich zu einem Funktor $[\mathbb{I}, \mathsf{Set}] \to \mathsf{Nom}$ erweitern, der linksadjungiert zu K ist.*

$$\begin{tikzcd}
{[\mathbb{I}, \mathsf{Set}]} \arrow[rr, bend left, "J"] \arrow[rr, phantom, "\perp"] && \mathsf{Nom} \arrow[ll, bend left, "K"]
\end{tikzcd}$$

Beweis. Nachdem wir bereits eine Familie von Morphismen $\eta_F \in [\mathbb{I}, \mathsf{Set}](F, KJF)$ angegeben haben (Lemma 8.9), müssen wir für die Adjunktion $J \dashv K$ noch deren universelle Eigenschaft prüfen (Proposition 5.6). Sei also eine natürliche Transformation $\alpha\colon F \to KX$ für $F\colon \mathbb{I} \to \mathsf{Set}$ und eine nominale Menge X gegeben. Wir müssen nun eine eindeutige äquivariante Abbildung $h\colon JF \to X$ finden, für die folgendes Diagramm kommutiert:

$$\begin{tikzcd}
JF \arrow[r, dashed, "\exists! h"] & X \\
K(JF) \arrow[r, "Kh"] & KX \\
F \arrow[u, "\eta_F"] \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

Für die Eindeutigkeit betrachte beliebiges $h\colon JF \to X$ mit $\alpha = Kh \circ \eta_F$ und $[\Gamma, x]_\sim \in JF$:

$$\begin{aligned}
\alpha_\Gamma(x) = (Kh \circ \eta_F)_\Gamma(x) = (Kh)_\Gamma\big((\eta_F)_\Gamma(x)\big) &\overset{\text{Def. } \eta_F}{=} (Kh)_\Gamma\big([\Gamma, x]_\sim\big) \\
&\overset{(8.2)}{=} h([\Gamma, x]_\sim)
\end{aligned}$$

Folglich ist h durch das kommutierende Dreieck $Kh \circ \eta_F = \alpha$ eindeutig bestimmt. Für die Existenz müssen wir also nur noch prüfen, dass $[\Gamma, x]_\sim \mapsto \alpha_\Gamma(x)$ wohldefiniert und äquivariant ist:

1. Wohldefiniertheit: Sei $(\Gamma, x) \sim (\Delta, y)$ bezeugt durch $\Upsilon \supseteq \Gamma \cup \Delta$:

$$\begin{aligned}
\alpha_\Gamma(x) &= \mathrm{id}_{\mathbb{A}} \cdot \alpha_\Gamma(x) \\
&= KX(\Gamma \hookrightarrow \Upsilon)(\alpha_\Gamma(x)) && (\text{Def. } KX(\varrho), (8.1), \mathrm{id}_{\mathbb{A}}|_\Gamma = (\Gamma \hookrightarrow \Upsilon)) \\
&= \alpha_\Upsilon(F(\Gamma \hookrightarrow \Upsilon)(x)) && (\text{Natürlichkeit, siehe unten}) \\
&= \alpha_\Upsilon(F(\Delta \hookrightarrow \Upsilon)(y)) && \big((\Gamma, x) \sim (\Delta, y)\big) \\
&= KX(\Delta \hookrightarrow \Upsilon)(\alpha_\Delta(y)) && (\text{Natürlichkeit, siehe unten}) \\
&= \mathrm{id}_{\mathbb{A}} \cdot \alpha_\Delta(y) = \alpha_\Delta(y)
\end{aligned}$$

Hier haben wir folgende Natürlichkeitsquadrate genutzt:

$$\begin{tikzcd}
x \in & F\Gamma \arrow[r, "F(\Gamma \hookrightarrow \Upsilon)"] \arrow[d, "\alpha_\Gamma"'] & F\Upsilon \arrow[d, "\alpha_\Upsilon"] & F\Delta \arrow[l, "F(\Delta \hookrightarrow \Upsilon)"'] \arrow[d, "\alpha_\Delta"] & \ni y \\
& KX(\Gamma) \arrow[r, "KX(\Gamma \hookrightarrow \Upsilon)"] & KX(\Upsilon) & KX(\Delta) \arrow[l, "KX(\Delta \hookrightarrow \Upsilon)"'] &
\end{tikzcd}$$

2. Äquivarianz von $h([\Gamma, x]_\sim) := \alpha_\Gamma(x)$: Für $\pi \in \mathfrak{S}_\mathrm{f}(\mathbb{A})$ gilt:

$$
\begin{aligned}
\pi \cdot h([\Gamma, x]_\sim) &= \pi \cdot \alpha_\Gamma(x) \\
&= KX(\pi|_\Gamma)(\alpha_\Gamma(x)) && \text{(Def. } KX(\pi|_\Gamma)\text{, (8.1))} \\
&= \alpha_{\pi[\Gamma]}(F(\pi|_\Gamma)(x)) && \text{(Natürlichkeit von } \alpha\text{)} \\
&= h([\pi[\Gamma], F(\pi|_\Gamma)(x)]_\sim) && \text{(Def. } h\text{)} \\
&= h(\pi \cdot [\Gamma, x]_\sim) && \text{(Def. } \cdot \text{ für } JF\text{)}
\end{aligned}
$$

Damit ist $h([\Gamma, x]_\sim) := \alpha_\Gamma(x)$ die gewünschte eindeutige äquivariante Abbildung. □

8.2 Schnitterhaltung

Die nominalen Mengen sind genau die schnitterhaltenden Prägarben:

Definition 8.11. Eine Prägarbe $F\colon \mathbb{I} \to \mathsf{Set}$ *erhält Schnitte*, wenn für alle $(\Gamma, x) \sim (\Delta, y)$ ein $z \in F(\Gamma \cap \Delta)$ existiert mit

$$F(\Gamma \cap \Delta \hookrightarrow \Gamma)(z) = x \qquad \text{und} \qquad F(\Gamma \cap \Delta \hookrightarrow \Delta)(z) = y.$$

Insbesondere gilt $(\Gamma \cap \Delta, z) \sim (\Gamma, x)$.

$$
\begin{tikzcd}[column sep=small]
x & \in & F\Gamma & & F\Delta & \ni & y \\
& & & F(\Gamma \cap \Delta) \arrow[ul, bend left, "F(\Gamma\cap\Delta\hookrightarrow\Gamma)"] \arrow[ur, bend right, "F(\Gamma\cap\Delta\hookrightarrow\Delta)"'] & & & \\
& & & \rotatebox[origin=c]{90}{$\in$} & & & \\
& & & \exists z \arrow[uuulll, bend left, mapsto] \arrow[uuurrr, bend right, mapsto] & & &
\end{tikzcd}
$$

Bemerkung 8.12. Für schnitterhaltende Prägarben ist $z \in F(\Gamma \cap \Delta)$ eindeutig bestimmt. Gäbe es nämlich ein weiteres solches $z' \in F(\Gamma \cap \Delta)$ mit $F(\Gamma \cap \Delta \hookrightarrow \Delta)(z') = y$, so wäre insbesondere $(\Gamma \cap \Delta, z) \sim (\Gamma \cap \Delta, z')$. Per Schnitterhaltung gäbe es also ein $z'' \in F((\Gamma \cap \Delta) \cap (\Gamma \cap \Delta)) = F(\Gamma \cap \Delta)$ mit $z' = F\mathrm{id}_{\Gamma\cap\Delta}(z'') = z$.

Lemma 8.13. *Für jede nominale Menge X erhält $KX\colon \mathbb{I} \to \mathsf{Set}$ Schnitte.*

Beweis. Für gegebene $x \in KX(\Gamma)$ und $y \in KX(\Delta)$ sei $(\Gamma, x) \sim (\Delta, y)$ durch $\Upsilon \supseteq \Gamma \cup \Delta$ bezeugt:

$$KX(\Gamma \hookrightarrow \Upsilon)(x) = KX(\Delta \hookrightarrow \Upsilon)(y)$$

Per Definition von KX ist $x = y$ und $x \in X$ hat sowohl Γ als auch Δ als Support. Per Lemma 4.9 hat x auch Support $\Gamma \cap \Delta$ und damit ist $z := x$ das gesuchte Element in $KX(\Gamma \cap \Delta)$. □

Umgekehrt ist jede schnitterhaltende Prägarbe isomorph zu KX für eine passende nominale Menge X:

Lemma 8.14. *Für jede schnitterhaltende Prägarbe $F\colon \mathbb{I} \to \mathsf{Set}$ ist η_F ein Isomorphismus.*

Damit ist F also isomorph zu KX für die nominale Menge $X := JF$.

Beweis. Wir zeigen, dass η_F komponentenweise injektiv und surjektiv ist:

- Für jeden Kontext $\Gamma \in \mathbb{I}$ ist $(\eta_F)_\Gamma \colon F(\Gamma) \to K(JF)(\Gamma)$ injektiv:

  Betrachte $x, y \in F(\Gamma)$ mit

  $$[\Gamma, x]_\sim = (\eta_F)_\Gamma(x) = (\eta_F)_\Gamma(y) = [\Gamma, y]_\sim$$

  Also ist $(\Gamma, x) \sim (\Gamma, y)$ und es gibt per Schnitterhaltung ein $z \in \Gamma \cap \Gamma = \Gamma$ mit

  $$x = F(\Gamma \cap \Gamma \hookrightarrow \Gamma)(z) = y$$

- Für jeden Kontext $\Gamma \in \mathbb{I}$ ist $(\eta_F)_\Gamma \colon F(\Gamma) \to K(JF)(\Gamma)$ surjektiv:

  Betrachte $[\Delta, y]_\sim \in K(JF)(\Gamma)$. Per Definition von K ist Γ ein Support von $[\Delta, y]_\sim$. Wähle eine beliebige Injektion $\varrho \colon (\Delta \setminus \Gamma) \rightarrowtail \mathbb{A} \setminus (\Delta \cup \Gamma)$ und definiere[2]

  $$\pi \in \mathfrak{S}_\mathrm{f}(\mathbb{A}) \qquad \text{mit} \qquad \pi(a) = \begin{cases} \varrho(a) & \text{Wenn } a \in \Delta \setminus \Gamma \\ \varrho^{-1}(a) & \text{Wenn } a \in \mathrm{Im}(\varrho) \\ a & \text{sonst.} \end{cases}$$

  Folglich ist $\pi \in \mathsf{Fix}(\Gamma)$ und damit:

  $$[\Delta, y]_\sim = \pi \cdot [\Delta, y]_\sim = \big[\pi[\Delta], F(\pi|_\Delta)(y)\big]_\sim$$

  Da F Schnitte erhält, gibt es ein $z \in \Delta \cap \pi[\Delta]$ mit $(\Delta \cap \pi[\Delta], z) \sim (\Delta, y)$ (siehe Bemerkung in Definition 8.11). Der Schnitt $\Delta \cap \pi[\Delta]$ vereinfacht sich wie folgt:

  $$\begin{aligned} \Delta \cap \pi[\Delta] &= \Delta \cap \pi[(\Delta \cap \Gamma) \cup (\Delta \setminus \Gamma)] = \Delta \cap (\pi[\Delta \cap \Gamma] \cup \pi[\Delta \setminus \Gamma]) \\ &= (\Delta \cap \pi[\Delta \cap \Gamma]) \cup (\Delta \cap \pi[\Delta \setminus \Gamma]) && \text{(Distributivität)} \\ &= (\Delta \cap (\Delta \cap \Gamma)) \cup \varnothing = \Delta \cap \Gamma && \text{(Def. } \pi\text{)} \end{aligned}$$

  Für $x := F(\Delta \cap \Gamma \hookrightarrow \Gamma)(z)$ erhalten wir also

  $$(\Gamma, x) \sim (\Delta \cap \Gamma, z) = (\Delta \cap \pi[\Delta], z) \sim (\Delta, y)$$

  und damit $(\eta_F)_\Gamma(x) = [\Gamma, x]_\sim = [\Delta, y]_\sim$ wie gewünscht. ☐

Korollar 8.15. *Für jede schnitterhaltende Prägarbe* $F \colon \mathbb{I} \to \mathsf{Set}$ *und* $(\Gamma, x) \sim (\Delta, y)$ *ist* $z \in F(\Gamma \cap \Delta)$ *aus Definition 8.11 eindeutig bestimmt.*

Die beiden Lemmata zuvor ergeben in Kombination:

Theorem 8.16. *Die nominalen Mengen entsprechen genau die schnitterhaltenden Prägarben.*

[2] Man beachte die Ähnlichkeit zum Beweis von Lemma 4.9.

9 Ausblick

Zum Abschluss blicken wir noch auf ein paar weitere nominale Konzepte:

Definition 9.1. Der *Frischequantor* (engl.: freshness quantifier) $\text{И}a.\varphi$ beschreibt, dass eine Aussage *für ausreichend frisches* $a \in \mathbb{A}$ gilt:

$$\text{И}a.\varphi \qquad :\Longleftrightarrow \qquad \text{Die Menge } \mathbb{A} \setminus \{a \in \mathbb{A} \mid \varphi\} \text{ ist endlich}$$

Dieser Quantor verhält sich gleichzeitig wie Existenzquantor und wie ein Allquantor. Man muss nicht zwischen „für ein frisches a“ und „für alle frischen a“ unterscheiden, sondern kann einfach eine Aussage „für frisches a“ treffen:

Proposition 9.2. *Für eine nominale Menge X und eine äquivariante Relation $R \subseteq \mathbb{A} \times X$ und $x \in X$ sind die folgenden Aussagen äquivalent:*

(a) $\text{И}a.\,(a, x) \in R$

(b) es existiert ein $a \in \mathbb{A}$ mit $a \mathrel{\#} x$ und $(a, x) \in R$

(c) für alle $a \in \mathbb{A}$ mit $a \mathrel{\#} x$ gilt $(a, x) \in R$

Beweis. Hier ist $\varphi := (a, x) \in R$ und $\text{И}a.(a, x) \in R$ bedeutet somit, dass

$$\mathbb{A} \setminus \{a \in \mathbb{A} \mid (a, x) \in R\}$$

endlich ist.

(a)⇒(b) Wenn $\mathbb{A} \setminus \{a \in \mathbb{A} \mid (a, x) \in R\}$ endlich ist, dann ist $\{a \in \mathbb{A} \mid (a, x) \in R\}$ unendlich. Da $\mathsf{supp}(x)$ endlich ist, kann die Menge

$$\{a \in \mathbb{A} \mid \varphi\} \setminus \mathsf{supp}(x)$$

nicht leer sein. Das bezeugende $a \in \mathbb{A}$ mit $a \notin \mathsf{supp}(x)$ und $(a, x) \in R$ ist genau das Gesuchte.

(b)⇒(c) Sei $a \in \mathbb{A}$ mit $a \mathrel{\#} x$ und $(a, x) \in R$. Für die Verifikation der allquantifizierten Aussage sei $b \in \mathbb{A}$ frisch für x. Nachdem a und b frisch für x sind, erhalten wir $(a\ \ b) \in \mathsf{Fix}(x)$ und damit $(a\ \ b) \cdot x = x$. Da R äquivariant ist, folgt aus $(a, x) \in R$:

$$R \ni (a\ \ b) \cdot (a, x) = ((a\ \ b) \cdot a, (a\ \ b) \cdot x) = (b, x).$$

(c)⇒(a) Aus die allquantifizierte Aussage ist äquivalent zur Teilmengenbeziehung:

$$\mathbb{A} \setminus \mathsf{supp}(x) \quad \subseteq \qquad \{a \in \mathbb{A} \mid (a, x) \in R\}$$

Also folgt:

$$\mathsf{supp}(x) \quad \supseteq \quad \mathbb{A} \setminus \{a \in \mathbb{A} \mid (a, x) \in R\}$$

Aus der Endlichkeit von $\mathsf{supp}(x)$ folgt Endlichkeit der Menge auf der rechten Seite, also $\text{И}a.\ (a, x) \in R$. $\square$

Beispiel 9.3. Für die abstrakte α-Äquivalenz auf $\mathbb{A} \times X$ (Definition 4.40), die dem Abstraktionsfunktor zugrunde liegt, betrachtet man Proposition 9.2 für die nominale Menge $X' := (\mathbb{A} \times X) \times (\mathbb{A} \times X)$ und die Relation:

$$R := \{(a, (v_1, x_1), (v_2, x_2)) \in \mathbb{A} \times X' \mid (v_1\ a) \cdot x_1 = (v_2\ a) \cdot x_2\}$$

Die Relation ist äquivariant, da die Bedingung $(v_1\ a) \cdot x_1 = (v_2\ a) \cdot x_2$ invariant unter bijektiver Umbenennung ist. Dann ist α-Äquivalenz definiert durch:

$$(v_1, x_1) \sim_\alpha (v_2, x_2) \quad :\Longleftrightarrow \quad \text{И}a.\ (v_1\ a) \cdot x_1 = (v_2\ a) \cdot x_2$$

Zusammenfassend haben Nominalen Menge schöne logische und kategorielle Eigenschaften und dienen als mathematisches Vehikel zur Modellierung von Variablenbindung und von Automaten für unendliche Eingabealphabete. Verwandt zur Automatentheorie und initialen Algebren lassen sich auch potentiell unendliche Datenstrukturen mit Bindung mittels Koalgebren beschreiben [8]. Wie bei den regulären Sprachen in klassischen Mengen induzieren auch die orbit-endlichen Koalgebren eines Funktors einen Fixpunkt mit einer entsprechenden universellen Eigenschaft [10, 11].

Literatur

[1] Jiří Adámek, Horst Herrlich, and George E. Strecker. Abstract and concrete categories. the joy of cats, 2004.

[2] Steve Awodey. *Category Theory*. Oxford Logic Guides. OUP Oxford, 2010. URL: `http://books.google.de/books?id=-MCJ6x2lC7oC`.

[3] Mikolaj Bojanczyk, Bartek Klin, and Slawomir Lasota. Automata theory in nominal sets. *Log. Methods Comput. Sci.*, 10, 2014. URL: `http://dx.doi.org/10.2168/LMCS-10(3:4)2014`, `doi:10.2168/LMCS-10(3:4)2014`.

[4] N.G de Bruijn. Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. *Indagationes Mathematicae (Proceedings)*, 75(5):381–392, 1972. `doi:10.1016/1385-7258(72)90034-0`.

[5] Murdoch Gabbay and Andrew M. Pitts. A new approach to abstract syntax involving binders. In Giuseppe Longo, editor, *Proceedings of the Fourteenth Annual IEEE Symp. on Logic in Computer Science, LICS 1999*, pages 214–224. IEEE Computer Society Press, July 1999.

[6] Murdoch James Gabbay and Martin Hofmann. Nominal renaming sets. In Iliano Cervesato, Helmut Veith, and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, 15th International Conference, LPAR 2008, Doha, Qatar, November 22-27, 2008. Proceedings*, volume 5330 of *Lecture Notes in Computer Science*, pages 158–173. Springer, 2008. `doi:10.1007/978-3-540-89439-1\_11`.

[7] Thomas Jech. *Set Theory*. Springer Berlin Heidelberg, 2003. URL: `http://dx.doi.org/10.1007/3-540-44761-X`, `doi:10.1007/3-540-44761-x`.

[8] Alexander Kurz, Daniela Petrisan, Paula Severi, and Fer-Jan de Vries. Nominal coalgebraic data types with applications to lambda calculus. *Logical Methods in Computer Science*, 9(4), 2013.

[9] Saunders Mac Lane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics. Springer New York, 1998. URL: `http://books.google.de/books?id=eBvhyc4z8HQC`.

[10] Stefan Milius, Lutz Schröder, and Thorsten Wißmann. Regular behaviours with names. *Applied Categorical Structures*, 24(5):663–701, 08 2016. `doi:10.1007/s10485-016-9457-8`.

[11] Stefan Milius and Thorsten Wißmann. Finitary corecursion for the infinitary lambda calculus. In Lawrence S. Moss and Paweł Sobociński, editors, *Proc. 6th Conference on Algebra and Coalgebra in Computer Science (CALCO 2015)*, volume 35 of *Leibniz International Proceedings in Informatics*, pages 336–351. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2015. URL: `http://coalg.org/calco15/papers/p21-Wi%C3%9Fmann.pdf`, `doi:10.4230/LIPIcs.CALCO.2015.336`.

[12] Joshua Moerman and Jurriaan Rot. Separation and Renaming in Nominal Sets. In Maribel Fernández and Anca Muscholl, editors, *CSL 2020*, volume 152 of *LIPIcs*, pages 31:1–31:17, Dagstuhl, Germany, 2020. LIPIcs. `doi:10.4230/LIPIcs.CSL.2020.31`.

[13] Andrew M. Pitts. *Nominal Sets: Names and Symmetry in Computer Science*, volume 57 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2013. doi:10.1017/CBO9781139084673.

[14] Lutz Schröder, Dexter Kozen, Stefan Milius, and Thorsten Wißmann. Nominal automata with name binding. In Javier Esparza and Andrzej Murawski, editors, *Proc. 20th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2017)*, volume 10203 of *LNCS*, pages 124–142. Springer, 04 2017. doi:10.1007/978-3-662-54458-7_8.

[15] Thorsten Wißmann. Supported sets – A new foundation for nominal sets and automata. In *Computer Science Logic (CSL'23)*, LIPIcs, pages 38:1–38:19, 02 2023. doi:10.4230/LIPIcs.CSL.2023.38.

[16] Thorsten Wißmann. Algebra des Programmierens (Vorlesungsmitschrift), 2017. URL: https://www8.cs.fau.de/wp-content/uploads/media/ss17/algprog/algprog.pdf.

Symbolverzeichnis

Verwendete Symbole in der Reihenfolge ihrer Definition:

Index