5 Das Isomorphieproblem

Eine *Äquivalenzstruktur* ist eine Struktur $\mathcal{A} = (U, R)$, wobei R eine Äquivalenzrelation ist.

Für $n \geq 1$ sei $f_\mathcal{A}(n)$ die Anzahl der Äquivalenzklassen der Größe n in $\mathcal{A}$. Sei weiter $f_\mathcal{A}(0) \in \mathbb{N} \cup \{\infty\}$ die Anzahl der unendlichen Äquivalenzklassen von $\mathcal{A}$. Dann ist $f_\mathcal{A} \colon \mathbb{N} \to \mathbb{N} \cup \{\infty\}$ eine Funktion. Für zwei *abzählbare* Äquivalenzstrukturen $\mathcal{A}$ und $\mathcal{B}$ gilt

$$\mathcal{A} \cong \mathcal{B} \iff \forall n \in \mathbb{N} \colon f_\mathcal{A}(n) = f_\mathcal{B}(n)\,.$$

Lemma 5.1. *Das folgende Problem ist entscheidbar:*
Eingabe: automatischen Präsentation einer Äquivalenzstruktur $\mathcal{A}$
$n \in \mathbb{N}$
$k \in \mathbb{N} \cup \{\infty\}$

Frage: Gilt $f_\mathcal{A}(n) = k$*?*

Beweis:
Wir berechnen aus n und k einen Satz φ aus $\mathrm{FO}[\exists^{\infty}, \text{ꓤ}]$ mit $\mathcal{A} \models \varphi_{n,k} \iff f_{\mathcal{A}}(n) = k$. Da die Gültigkeit dieses Satzes in einer automatischen Struktur entscheidbar ist, folgt das Ergebnis.

Zunächst gilt für jede Äquivalenzstruktur $\mathcal{A} = (U, R)$ und jedes $a \in U$:

- für $n \geq 1$: $\big|[a]\big| \geq n$ gdw. $\mathcal{A} \models \exists x_1, \ldots, x_n \colon \bigwedge\limits_{1 \leq i \leq n} R(a, x_i) \wedge \bigwedge\limits_{1 \leq i < j \leq n} x_i \neq x_j$
- $\big|[a]\big| = \infty$ gdw. $\mathcal{A} \models \exists^{\infty} x \colon R(a, x)$

Damit erhalten wir:

- für $k, n \in \mathbb{N}$: $f_{\mathcal{A}}(n) \geq k$ gdw. $\mathcal{A} \models \exists a_1, \ldots, a_k \colon \bigwedge\limits_{1 \leq i \leq k} \big|[a_i]\big| = n \wedge \bigwedge\limits_{1 \leq i < j \leq k} \neg R(a_i, a_j)$.

  Nach obiger Überlegung kann „$\big|[a_i]\big| = n$“ durch eine Formel aus FO ausgedrückt werden. Damit kann „$f_{\mathcal{A}}(n) \geq k$“ durch eine FO-Formel ausgedrückt werden und dadurch auch „$f_{\mathcal{A}}(n) = k$“.

- für $n \geq 1$: $f_{\mathcal{A}}(n) = \infty$ gdw. $\mathcal{A} \models \exists^{\infty} a \colon \big|[a]\big| = n$.
- $f_{\mathcal{A}}(0) = \infty$ gdw. $\reflectbox{R} xy \colon \Big(\big|[x]\big| = \infty \wedge \big|[y]\big| = \infty \wedge \neg R(x, y)\Big)$

$\square$

Proposition 5.2. *Das Nicht-Isomorphieproblem für automatische Äquivalenzstrukturen ist semi-entscheidbar.*

Beweis:
Seien $\mathcal{A}$ und $\mathcal{B}$ automatische Äquivalenzstrukturen. Dann gilt

$$\begin{aligned} \mathcal{A} \ncong \mathcal{B} &\iff \exists n \in \mathbb{N} \colon f_{\mathcal{A}}(n) \neq f_{\mathcal{B}}(n) \\ &\iff \exists n \in \mathbb{N}\, \exists k \in \mathbb{N} \cup \{\infty\} \colon \big(f_{\mathcal{A}}(n) = k \wedge f_{\mathcal{B}}(n) \neq k\big)\,. \end{aligned}$$

Es gilt also $\mathcal{A} \ncong \mathcal{B}$, wenn es n und k gibt mit $f_{\mathcal{A}}(n) = k$ und $f_{\mathcal{B}}(n) \neq k$. Die Eigenschaft „$f_{\mathcal{A}}(n) = k$ und $f_{\mathcal{B}}(n) \neq k$“ ist nach vorherigem Lemma entscheidbar ist. Ein Semi-Entscheidungsalgorithmus probiert nacheinander alle Paare n und k durch und testet diese Eigenschaft. $\square$

Wir zeigen jetzt, daß das Isomorphieproblem für automatische Äquivalenzstrukturen unentscheidbar ist. Wir reduzieren Hilberts 10. Problem, d.h. die Frage, ob zwei multivariate Polynome aus $\mathbb{N}[x_1, \ldots, x_k]$ einen Schnittpunkt haben, hierauf.

Für $\overline{n} \in \mathbb{N}^k$ sei $a^{\overline{n}} = ba^{n_1}ba^{n_2}b \cdots a^{n_k}b \in \{a, b\}^*$. Setze $L = \{a^{\overline{n}} \mid \overline{n} \in \mathbb{N}^k\}$.

Lemma 5.3. *Aus $p \in \mathbb{N}[x_1, \ldots, x_k]$ kann ein NFA M_p mit $L(M_p) \subseteq L$ berechnet werden, so daß für alle $\overline{n} \in \mathbb{N}^k$ gilt: M_p hat genau $p(\overline{n})$ viele akzeptierende Läufe auf $a^{\overline{n}}$.*

Beweis:
Induktion über den Aufbau des Polynoms p:

- $p = 0$: M_p DFA mit $L(M_p) = \emptyset$.
- $p = 1$: M_p DFA mit $L(M_p) = L$.
- $p = n_i$ (für $i = 3$ und $k = 4$):

$a \quad a \quad a \quad a \quad a$

$b \quad b \quad b \quad a \quad b$

$0 \quad 1 \quad 2 \quad\quad\quad 4$

- $p = q + r$: disjunkte Vereinigung der NFAs M_q und M_r
- $p = q \cdot r$: Kreuzproduktkonstruktion von M_q und M_r $\square$

Proposition 5.4. *Aus $p \in \mathbb{N}[x_1, \ldots, x_k]$ kann eine automatische Darstellung einer Äquivalenzstruktur $\mathcal{A}_p$ berechnet werden mit*

- *$f_{\mathcal{A}}(n) \in \{0, \infty\}$ für alle $n \in \mathbb{N}$ (d.h. zu jeder Äquivalenzklasse gibt es unendlich viele derselben Größe)*
- *$f_{\mathcal{A}}(0) = 0$ (d.h. $\mathcal{A}$ hat nur endliche Äquivalenzklassen)*
- *$f_{\mathcal{A}}(m) = \infty$ gdw. es gibt $\overline{n} \in \mathbb{N}^k$ mit $p(\overline{n}) = m$.*

Beweis:
Konstruiere zunächst NFA M_p nach Lemma 5.3.

Sei L_0 die Menge der akzeptierenden Läufe von M_p (d.h. $L_0 \subseteq Q\big(\{a,b\}\,Q\big)^*$).

Setze $R_0 = \big\{(u,v) \in L_0^2 \;\big|\; u \text{ und } v \text{ sind Läufe auf demselben Wort}\big\}$

Dann ist $\mathcal{A}_0 = (L_0, R_0)$ automatische Äquivalenzstruktur und es gilt $\big|[a^{\overline{n}}]\big| = p(\overline{n})$ für alle $\overline{n} \in \mathbb{N}^k$. Wir haben also

- $f_{\mathcal{A}_0}(0) = 0$ (d.h. $\mathcal{A}_0$ hat nur endliche Äquivalenzklassen)
- $f_{\mathcal{A}_0}(m) > 0$ gdw. es gibt $\overline{n} \in \mathbb{N}^k$ mit $\big|[a^{\overline{n}}]\big| = m$ gdw. es gibt $\overline{n} \in \mathbb{N}^k$ mit $p(\overline{n}) = m$.

Wir setzen nun $L = L_0c^*$ und $R = \big\{(uc^m, vc^m) \;\big|\; (u,v) \in R_0, m \in \mathbb{N}\big\}$. Dann ist $\mathcal{A}_p = (L, R)$ die gesuchte Äquivalenzstruktur. $\square$

Sei $c \in \mathbb{N}[x, y]$ das Polynom $c(x, y) = (x + y)(x + y + 1) + 2y$, d.h. $c\colon \mathbb{N}^2 \to \mathbb{N}$ ist eine injektive Funktion.

Sei weiter $p_<(x, y) = c(x, x + y + 1)$ und $p_> = c(x + y + 1, y)$.

Wir betrachten die Äquivalenzstruktur $\mathcal{T} = \mathcal{A}_{p_>} \uplus \mathcal{A}_{p_<}$. Sie „kodiert“ die Menge $\{(n_1, n_2) \in \mathbb{N}^2 \mid n_1 \neq n_2\}$:

- $f_\mathcal{T}(0) = 0$
- $f_\mathcal{T}(m) = \infty$
  gdw. $f_\mathcal{T}(m) > 0$
  gdw. es gibt $n_1, n_2 \in \mathbb{N}$ mit $m = p_>(n_1, n_2)$ oder $m = p_<(n_1, n_2)$
  gdw. es gibt $n_1 \neq n_2$ mit $m = c(n_1, n_2)$

Satz 5.5. *Die Klasse der automatischen Präsentationen P mit $\mathcal{A}(P) \cong \mathcal{T}$ ist unentscheidbar.*

Beweis:
Seien $p, q \in \mathbb{N}[x_1, \dots, x_k]$ Polynome. Betrachte die automatische Struktur

$$\mathcal{A}_{p,q} = \mathcal{T} \uplus \mathcal{A}_{c(p,q)} \,.$$

Da in $\mathcal{T}$ und in $\mathcal{A}_{c(p,q)}$ zu jeder Äquivalenzklasse unendlich viele gleichgroße existieren, erhalten wir $f_{\mathcal{A}_{p,q}}(m) = \max\big(f_{\mathcal{T}}(m), f_{\mathcal{A}_{c(p,q)}}(m)\big)$ für alle $m \in \mathbb{N}$.

Wir zeigen:

$$\mathcal{A}_{p,q} \ncong \mathcal{T} \iff \exists \overline{n} \in \mathbb{N}^k \colon p(\overline{n}) = q(\overline{n})$$

„$\Leftarrow$“ Sei also $\overline{n} \in \mathbb{N}^k$ mit $p(\overline{n}) = q(\overline{n})$. Setze $m = c\big(p(\overline{n}), q(\overline{n})\big)$.

$\implies f_{\mathcal{A}_{c(p,q)}}(m) = \infty$ und $f_{\mathcal{T}}(m) = 0$

$\implies f_{\mathcal{A}_{p,q}}(m) = \max\big(f_{\mathcal{T}}(m), f_{\mathcal{A}_{c(p,q)}}(m)\big) = \infty \neq f_{\mathcal{T}}(m)$

$\implies \mathcal{A}_{p,q} \ncong \mathcal{T}$

„$\Rightarrow$“ Gelte umgekehrt $\mathcal{A}_{p,q} \ncong \mathcal{T}$.

Wegen $f_{\mathcal{T}}(0) = 0 = f_{\mathcal{A}_{p,q}}(0)$ gibt es also $m \geq 1$ mit $f_{\mathcal{A}_{p,q}}(m) \neq f_{\mathcal{T}}(m)$

$\Longrightarrow f_{\mathcal{A}_{c(p,q)}}(m) \geq f_{\mathcal{A}_{p,q}}(m) = \infty$ und $f_{\mathcal{T}}(m) = 0$

Wegen $f_{\mathcal{A}_{c(p,q)}}(m) = \infty$ gibt es $\overline{n} \in \mathbb{N}^k$ mit $m = c\big(p(\overline{n}), q(\overline{n})\big)$.

$\Longrightarrow f_{\mathcal{T}}\Big(c\big(p(\overline{n}), q(\overline{n})\big)\Big) = f_{\mathcal{T}}(m) = 0$

$\Longrightarrow p(\overline{n}) = q(\overline{n})$

Also ist die Abbildung $(p, q) \mapsto \mathcal{A}_{p,q}$ eine Reduktion der Menge der schnittfreien Paare von Polynomen auf die Menge der automatischen Präsentation von $\mathcal{T}$. $\square$

Wir haben also gezeigt, daß das Isomorphieproblem für automatische Äquivalenzstrukturen unentscheidbar, aber semi-entscheidbar ist. Es ist sogar vollständig für die Klasse der semi-entscheidbaren Probleme (jedes semi-entscheidbare Problem kann hierauf reduziert werden).

Für automatische lineare Ordnungen und für automatische Bäume ist dieses Problem nicht einmal semi-entscheidbar, sondern „Σ_1^1-vollständig“.

Bemerkung. Proposition 5.2 wurde gezeigt in S. Rubin: „Automata presenting structures: A survey of the finite string case“, *Bull. Symbolic Logic*, 14:169–209, 2008.

Satz 5.5 steht in D. Kuske, J. Liu und M. Lohrey: „The isomorphism problem on classes of automatic structures with transitive relations“, *Transactions of the AMS*, 365:5103-5151, 2013. Dort stehen auch die Ergebnisse zu automatischen linearen Ordnungen und Bäumen.