3.8 Das Ajtai-Fagin Spiel

Notation:

Für eine Klasse S von σ-Strukturen und eine Teilklasse $C \subseteq S$ sagen wir:

C ist EMSO-definierbar in S,

falls es einen EMSO[σ]-Satz Φ gibt, s.d. f.a. $\mathfrak{A} \in S$ gilt:

$$\mathfrak{A} \in C \iff \mathfrak{A} \models \Phi.$$

Zur Erinnerung:

EMSO[σ] ist die Klasse aller MSO[σ]-Formeln der Form

$$\exists X_1 \cdots \exists X_\ell \; \varphi$$

mit $\ell \geq 0$ und $\varphi \in \mathrm{FO}[\sigma \cup \{X_1, \dots, X_\ell\}]$, wobei $X_1, \dots, X_\ell$ Mengenvariablen sind.

Ziel:

Ein 2-Personen-Spiel, mit dem man für bestimmte Klassen S und C nachweisen kann, dass C nicht EMSO-definierbar in S ist.

~~Für den Spezialfall der existentiellen monadischen Logik zweiter Stufe (EMSO) war der EF-Spiel-Ansatz allerdings sehr erfolgreich.~~

EMSO und das Ajtai-Fagin-Spiel

Definition 3.48 (Das Ajtai-Fagin-Spiel)

Sei σ eine relationale Signatur, sei S eine Klasse von σ-Strukturen und sei $C \subseteq S$. Seien $l, m \geq 1$.

Das <u>(l,m)-Ajtai-Fagin-Spiel für C auf S</u> wird wie folgt gespielt:

<u>Phase</u> 1: Duplicator wählt eine Struktur $\mathfrak{A} \in C$. Danach wählt Spoiler l Mengen

$$X_1^{\mathfrak{A}}, \dots, X_l^{\mathfrak{A}} \subseteq A.$$

<u>Phase 2</u>: Duplicator wählt eine Struktur $\mathfrak{B} \in S \setminus C$ und l Mengen $X_1^{\mathfrak{B}}, \dots, X_l^{\mathfrak{B}} \subseteq B$.

<u>Phase 3</u>: Spoiler und Duplicator spielen das m-Runden EF-Spiel auf $\mathfrak{A}', \mathfrak{B}'$ für $\mathfrak{A}' := (\mathfrak{A}, X_1^{\mathfrak{A}}, \dots, X_l^{\mathfrak{A}})$ und $\mathfrak{B}' := (\mathfrak{B}, X_1^{\mathfrak{B}}, \dots, X_l^{\mathfrak{B}})$.

Satz 3.44 (Ajtai und Fagin, 1988)

Sei σ eine endliche, ~~relationale~~ Signatur, sei S eine Klasse von σ-Strukturen und sei $C \subseteq S$. Dann sind äquivalent:

(a) C ist EMSO-definierbar in S

(b) Es gibt $\ell, m \geq 1$, so dass Spoiler eine Gewinnstrategie im (ℓ, m)-Ajtai-Fagin-Spiel für C auf S hat.

Beweis:

(a) $\Rightarrow$ (b): Sei $\Phi = \exists X_1 \cdots \exists X_\ell\, \varphi$ ein EMSO$[\sigma]$-Satz, der C in S definiert (d.h.: f.a. $\mathfrak{A} \in S$ gilt: $\mathfrak{A} \in C \iff \mathfrak{A} \models \Phi$).

Sei $m := qr(\varphi)$. Spoiler hat folgende Gewinnstrategie im (ℓ, m)-Ajtai-Fagin-Spiel für C auf S:

Phase 1: Sei $\mathfrak{A} \in C$ die von Duplicator gewählte Struktur. Wegen $\mathfrak{A} \models \Phi$, kann Spoiler ℓ Mengen $X_1^{\mathfrak{A}}, \dots, X_\ell^{\mathfrak{A}} \subseteq A$ wählen, so dass für $\mathfrak{A}' := (\mathfrak{A}, X_1^{\mathfrak{A}}, \dots, X_\ell^{\mathfrak{A}})$ gilt: $\mathfrak{A}' \models \varphi$.

Phase 2: Seien $\mathfrak{B} \in S \setminus C$ und $X_1^{\mathfrak{B}}, \dots, X_\ell^{\mathfrak{B}} \subseteq B$ von Duplicator gewählt. Es gilt: $\mathfrak{B} \not\models \Phi$, d.h. für $\mathfrak{B}' := (\mathfrak{B}, X_1^{\mathfrak{B}}, \dots, X_\ell^{\mathfrak{B}})$ gilt: $\mathfrak{B}' \not\models \varphi$.

Phase 3: Wegen $\mathfrak{A}' \models \varphi$, $\mathfrak{B}' \not\models \varphi$ und $qr(\varphi) = m$ hat Spoiler gemäß Satz von Ehrenfeucht Gewinnstrategie im m-Runden EF-Spiel auf $\mathfrak{A}'$, $\mathfrak{B}'$.

(b) $\Rightarrow$ (a): Gemäß Voraussetzung gibt es $\ell, m \geq 1$, so dass Spoiler eine Gewinnstrategie im (ℓ, m)-Ajtai-Fagin-Spiel für C auf S hat. D.h.:

für jedes $\mathfrak{A} \in C$ gibt es Mengen $\overline{X}^{\mathfrak{A}} := X_1^{\mathfrak{A}}, \dots, X_\ell^{\mathfrak{A}} \subseteq A$, so dass

für alle $\mathfrak{B} \in S \setminus C$ und alle $\overline{X}^{\mathfrak{B}} = X_1^{\mathfrak{B}}, \dots, X_\ell^{\mathfrak{B}} \subseteq B$ gilt:

es gibt einen $FO[\sigma \cup \{X_1, \dots, X_\ell\}]$-Satz $\varphi_{\mathfrak{A}; \mathfrak{B}, \overline{X}^{\mathfrak{B}}}$ vom Quantorenrang $\leq m$, s.d.

$(\mathfrak{A}, \overline{X}^{\mathfrak{A}}) \models \varphi_{\mathfrak{A}; \mathfrak{B}, \overline{X}^{\mathfrak{B}}}$ und

$(\mathfrak{B}, \overline{X}^{\mathfrak{B}}) \not\models \varphi_{\mathfrak{A}; \mathfrak{B}, \overline{X}^{\mathfrak{B}}}$

Setze $\varphi_{\mathfrak{A}} := \bigwedge \left\{ \varphi_{\mathfrak{A}; \mathfrak{B}, \overline{X}^{\mathfrak{B}}} : \begin{array}{l} \mathfrak{B} \in S \setminus C, \\ \overline{X}^{\mathfrak{B}} = X_1^{\mathfrak{B}}, \dots, X_\ell^{\mathfrak{B}} \subseteq B \end{array} \right\}$

und $\varphi := \bigvee \{ \varphi_{\mathfrak{A}} : \mathfrak{A} \in C \}$

und $\Phi := \exists X_1 \cdots \exists X_\ell \, \varphi$.

Dann ist Φ ein $\mathrm{EMSO}[\sigma]$-Satz*,

so dass gilt:

1) f.a. $\mathfrak{A} \in C$ gilt: $\mathfrak{A} \models \Phi$, und

2) f.a. $\mathfrak{B} \in S \setminus C$ gilt: $\mathfrak{B} \not\models \Phi$

$*$: Beachte: $\varphi_{\mathfrak{A}}$ und φ sind FO-Formeln, da es nur endlich viele paarweise nicht-äquivalente FO-Formeln vom Quantorenrang $\leq m$ gibt.

$\square$

Das Komplement von Graphzusammenhang

Eingabe: ein ungerichteter Graph G

Frage: Ist G unzusammenhängend?

wird durch die folgende EMSO-Formel definiert:

$$\exists X \Big(\exists y\, X(y) \;\wedge\; \exists z\, \neg X(z) \;\wedge\; \forall x \forall x' \big((X(x) \wedge E(x,x')) \rightarrow X(x') \big) \Big)$$

Unter Verwendung des Ajtai-Fagin-Spiels können wir nachweisen, dass <u>Graph-Zusammenhang</u> <u>nicht</u> EMSO-definierbar ist (in der Klasse aller endlichen ungerichteten Graphen):

<u>Satz 3.45</u> (Fagin, 1975)

Graph-Zusammenhang ist <u>nicht</u> EMSO-definierbar in der Klasse aller endlichen ungerichteten Graphen.

<u>Beweis:</u>

Sei UGraphs die Klasse aller endlichen ungerichteten Graphen und sei Conn die Klasse aller zusammenhängenden endlichen ungerichteten Graphen.

<u>Ziel:</u> Zeige, dass Conn nicht EMSO-definierbar in UGraphs ist.

Gemäß Satz 3.44 genügt es, für alle $l, m \geq 1$ zu zeigen, dass Duplicator eine Gewinnstrategie im (l,m)-Ajtai-Fagin-Spiel für Conn auf UGraphs hat.

Seien also $l, m \geq 1$.

Duplicator spielt das (l,m)-Ajtai-Fagin-Spiel für Conn auf UGraphs gemäß folgender Strategie

<u>Phase 1</u>: Duplicator wählt als $\mathfrak{A} = (A, E^{\mathfrak{A}}) \in$ Conn einen ungerichteten Kreis auf n Knoten, für n hinreichend groß.

"Hinreichend groß" heißt hier, dass n so groß sein soll, dass nach Spoilers Wahl der Mengen $\vec{X}^{\mathfrak{A}} = X_1^{\mathfrak{A}}, \ldots, X_l^{\mathfrak{A}} \subseteq A$ für die resultierende Struktur $\mathfrak{A}' := (\mathfrak{A}, \vec{X}^{\mathfrak{A}})$ gilt:

Es gibt zwei Knoten $v, w \in A$, deren <u>gerichtete</u> 3^m-Nachbarschaften disjunkt und isomorph sind, d.h.:

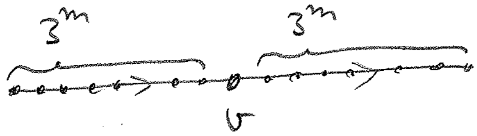
- $\mathrm{Dist}^{\mathfrak{A}'}(v,w) \geq 2 \cdot 3^m + 1$ und
- $\left(N_{3^m}^{\mathfrak{A}'_{\circlearrowright}}(v), v\right) \cong \left(N_{3^m}^{\mathfrak{A}'_{\circlearrowright}}(w), w\right)$, wobei

$\mathfrak{A}'_{\circlearrowright}$ die <u>gerichtete</u> Variante von $\mathfrak{A}'$ bezeichnet, in der die Kanten im Uhrzeigersinn ausgerichtet sind.

Zur genauen Wahl von n schauen wir uns die möglichen 3^m-Nachbarschaften in $\mathfrak{A}'_\emptyset$ an:

Ist $n > 2 \cdot 3^m + 1$, so gilt für jeden Knoten v in $\mathfrak{A}'_\emptyset$:

$N_{3^m}^{\mathfrak{A}'_\emptyset}(v)$ ist ein gerichteter Pfad auf $2 \cdot 3^m + 1$ Knoten, und v ist der Knoten in der Mitte des Pfads. Skizze:



Durch die unären Relationen $\overline{X}^{\mathfrak{A}} = X_1^{\mathfrak{A}}, \dots, X_\ell^{\mathfrak{A}}$ ist außerdem jeder dieser $2 \cdot 3^m + 1$ Knoten mit genau einer von 2^ℓ möglichen "Farben" markiert (nämlich der Teilmenge von $\{1, \dots, \ell\}$, die aus allen j besteht, so dass der Knoten zur Menge $X_j^{\mathfrak{A}}$ gehört).

Somit gibt es höchstens $I := (2^\ell)^{2 \cdot 3^m + 1}$ mögliche 3^m-Nachbarschaften.

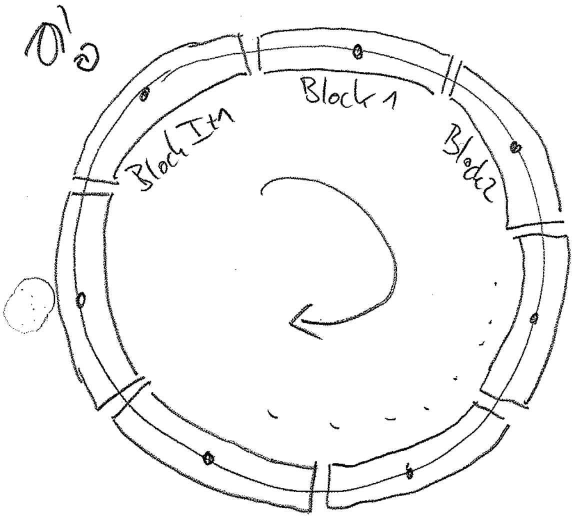
Wir setzen nun

$$n := (I+1) \cdot (2 \cdot 3^m + 1)$$

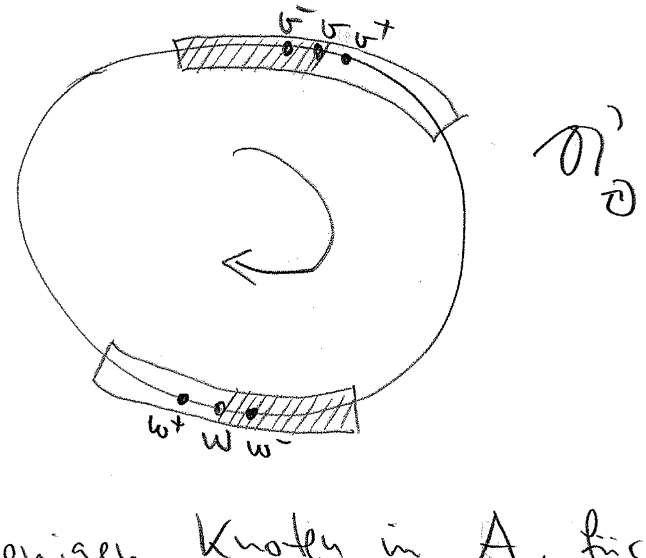
und lassen Duplicator in Phase 1 einen ungerichteten Kreis $\mathfrak{A}$ auf n Knoten wählen.

Seien $\overline{X}^{\mathfrak{A}} := X_1^{\mathfrak{A}}, \dots, X_\ell^{\mathfrak{A}} \subseteq A$ die von Spoiler in Phase 1 gewählten Mengen,
sei $\mathfrak{A}' := (\mathfrak{A}, \overline{X}^{\mathfrak{A}})$ und sei $\mathfrak{A}'_{\circlearrowright}$ die gerichtete Variante von $\mathfrak{A}'$, in der die Kanten im Uhrzeigersinn ausgerichtet sind.

<u>Phase 2</u>: Gemäß unserer Wahl von n wissen wir, dass es zwei Knoten $v, w \in A$ geben muss, so dass gilt:

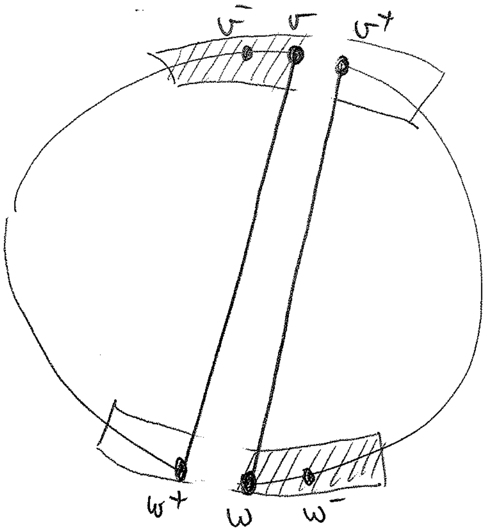


- $\mathrm{Dist}^{\mathfrak{A}'_{\circlearrowright}}(v,w) \geq 2 \cdot 3^m + 1$ und
- $\left(\mathcal{N}_{3^m}^{\mathfrak{A}'_{\circlearrowright}}(v), v\right) \cong \left(\mathcal{N}_{3^m}^{\mathfrak{A}'_{\circlearrowright}}(w), w\right)$



Seien v^-, v^+, w^-, w^+ diejenigen Knoten in A, für die gilt:
$(v^-, v) \in E^{\mathfrak{A}'_{\circlearrowright}}$, $(v, v^+) \in E^{\mathfrak{A}'_{\circlearrowright}}$, $(w^-, w) \in E^{\mathfrak{A}'_{\circlearrowright}}$, $(w, w^+) \in E^{\mathfrak{A}'_{\circlearrowright}}$

In Phase 2 lassen wir Duplicator als $\mathfrak{B} \in \text{UGraphs} \setminus \text{Conn}$ den Graphen $\mathfrak{B} = (B, E^{\mathfrak{B}})$ wie folgt wählen:



- $B := A$
- $E^{\mathfrak{B}}$ entsteht aus $E^{\mathfrak{A}}$, indem man die Kanten zwischen v und v^+ bzw. zwischen w und w^+ löscht und stattdessen neue Kanten zwischen v und w^+ bzw. zwischen w und v^+ einfügt.

Der so konstruierte Graph besteht offensichtlicherweise aus zwei disjunkten Kreisen.

Des Weiteren wählt Duplicator die Mengen $\overline{X}^{\mathfrak{B}} := X_1^{\mathfrak{B}}, \ldots, X_\ell^{\mathfrak{B}} \subseteq B$ identisch zu $\overline{X}^{\mathfrak{A}}$, d.h. $X_i^{\mathfrak{B}} := X_i^{\mathfrak{A}}$ f.a. $i \in \{1, \ldots, \ell\}$.

Man sieht leicht, dass in der zugehörigen Struktur $\mathfrak{B}' := (\mathfrak{B}, \overline{X}^{\mathfrak{B}})$ gilt:

für jeden Knoten $u \in A = B$ ist
$$\left(\mathcal{N}_{3^m}^{\mathfrak{A}'}(u), u\right) \cong \left(\mathcal{N}_{3^m}^{\mathfrak{B}'}(u), u\right)$$

<u>Phase 3:</u> Wir müssen zeigen, dass Duplicator eine Gewinnstrategie im m-Runden EF-Spiel auf $\mathfrak{A}'$ und $\mathfrak{B}'$ hat.

Dies folgt direkt aus dem Satz von Hanf (Satz 3.32): Indem wir die bijektive Abbildung $f: A \to B$ via $f(a) := a$ f.a. $a \in A$ wählen (beachte: hier ist $A = B$), folgt f.a. $a \in A$: $(\mathcal{N}_{3^m}^{\mathfrak{A}'}(a), a) \cong (\mathcal{N}_{3^m}^{\mathfrak{B}'}(f(a)), f(a))$. Somit gilt $\#_\rho(\mathfrak{A}') = \#_\rho(\mathfrak{B}')$ f.a. 3^m-Umgebungstypen ρ, und daher ist Voraussetzung (2) des Satzes von Hanf erfüllt. Die Voraussetzungen (1) und (3) des Satzes von Hanf sind trivialerweise erfüllt.

$\square$ Satz 3.45

<u>Abschließende Bemerkungen:</u>

(a) Man kann praktisch für jede Logik ein geeignetes Spiel entwerfen.

Insbesondere für MSO wird ein solches Spiel in den Übungsaufgaben erarbeitet. Mit dessen Hilfe kann Folgendes gezeigt werden:

<u>Satz 3.46</u> ("MSO = FO auf unären Signaturen")
Sei σ eine Signatur, die aus 1-stelligen Relationssymbolen und Konstantensymbolen besteht.
Für jeden MSO[σ]-Satz gibt es einen äquivalenten FO[σ]-Satz.

<u>Beweis:</u> Übung.

(b) Das Ajtai-Fagin-Spiel lässt sich auf naheliegende Art zu einem Spiel abändern, mit dem man (in Analogie zu Satz 3.44) für geeignete Klassen S und C zeigen kann, dass C nicht ESO-definierbar in S ist.

Auf Grund des Satzes von Fagin ("ESO charakterisiert NP") kann man mit diesem Spiel also nachweisen, dass C nicht in NP liegt.

Dies liefert einen Ansatz, um nachzuweisen, dass $NP \neq coNP$ (und daher auch $P \neq NP$) ist:

Nimm z.B. das NP-vollständige 3-Färbbarkeitsproblem, und sei C das Komplement des 3-Färbbarkeitsproblems (d.h.: C ist die Klasse aller endlichen ungerichteten Graphen, die nicht 3-färbbar sind).

Es gilt:

$NP \neq coNP \iff C \notin NP$

$\iff C$ ist nicht ESO-definierbar in UGraphs

$\iff$ Duplicator hat eine Gewinnstrategie im entsprechenden Spiel für C auf UGraphs

Leider ist dieser Ansatz – genau wie alle anderen Verfahren zum Trennen von NP und coNP – bisher gescheitert (unter Anderem an der enormen Komplexität des Nachweises von Gewinnstrategien).