Untere Beweisschranken durch effiziente Interpolation

von Fabian Achammer

Diese Seminararbeit ist im Rahmen des Seminars *Beweiskomplexität* unter Anleitung von Professor Stefan Hetzl and der TU Wien im Sommersemester 2022 entstanden. Ziel ist es, die Beweismethode der monotonen effizienten Interpolation vorzustellen und damit zu zeigen, dass der Resolutionskalkül und der schnittfreie Sequentialkalkül nicht polynomial beschränkt sind. Die Arbeit basiert auf den entsprechenden Kapiteln in *Proof Complexity* von Jan Krajíček [Kra19].

Inhaltsverzeichnis

1 Monotone effiziente Interpolation

Unser Ziel ist es, eine super-polynomiale untere Schranke für Beweissysteme zu finden. Dazu genügt es, für ein Beweissystem P, eine Folge von unerfüllbaren Klauselmengen $(C_n)_{n\in\mathbb{N}}$ (Anzahl und Größe der Klauseln wachsen höchstens polynomial in n), sowie ein super-polynomiales $u : \mathbb{N} \to \mathbb{N}$ zu finden, sodass asymptoisch für $n \to \infty$ gilt: Jede P-Widerlegung π von C_n erfüllt $u(n) \leq |\pi|$.

Wir betrachten zunächst Klauselmengen

$$A(\overline{p}, \overline{q}) = \big\{A_1(\overline{p}, \overline{q}), \ldots, A_m(\overline{p}, \overline{q})\big\}$$
$$B(\overline{p}, \overline{r}) = \big\{B_1(\overline{p}, \overline{r}), \ldots, B_l(\overline{p}, \overline{r})\big\}$$

sodass die Tupeln von Variablen $\overline{p}$, $\overline{q}$, $\overline{r}$ paarweise disjunkt sind und $A \cup B$ unerfüllbar ist. Zudem fordern wir, dass die Anzahl der Variablen und Klauseln polynomial durch einen Parameter n beschränkt sind. Für eine Klausel C schreiben wir $\bigvee C$ für die Disjunktion ihrer Literale. Für eine Klauselmenge S schreiben wir $\bigwedge \bigvee S$ für die Formel

$$\bigwedge_{C\in S} \bigvee C.$$

Meistens werden wir statt $\bigvee C$ bzw. $\bigwedge \bigvee S$ auch einfach C bzw. S schreiben, wenn aus dem Kontext klar ist, dass statt der Klausel bzw. Klauselmenge die entsprechende Formel gemeint ist.

Die Beweistechnik der effizienten Interpolation besteht darin, dass wir jeder P-Widerlegung π der Klauselmenge $A \cup B$ einen Schaltkreis $I(\overline{p})$ zuordnen, der die Implikation

$$A(\overline{p}, \overline{q}) \to \neg B(\overline{p}, \overline{r})$$

interpoliert, sowie $\big|I(\overline{p})\big| \leq |\pi|^{O(1)}$ erfüllt.

Damit haben wir das Problem, untere Schranken für Beweise zu finden, darauf reduziert, untere Schranken für gewisse interpolierende Schaltkreise zu finden, und zu zeigen, dass ein Beweissystem effiziente Interpolation erlaubt. Für allgemeine Schaltkreise sind derzeit nur schwache untere Schranken bekannt, deshalb betrachten wir in dieser Arbeit nur *monotone* effiziente Interpolation, das heißt wir fordern zusätzlich, dass I ein monotoner Schaltkreis ist und dass die Atome aus $\overline{p}$ in den A_i nur positiv oder in den B_j nur negativ auftreten. In diesem Fall gibt es eine günstige untere Schranke, auf die wir später verweisen werden. Wir fassen dieses Setting in zwei Definitionen zusammen:

Definition 1. *Seien $\overline{p}$, $\overline{q}$, $\overline{r}$ disjunkte Tupel von Variablen und seien $A(\overline{p}, \overline{q})$ und $B(\overline{p}, \overline{r})$ Klauselmengen. Wir sagen, dass das* Tupel (A, B) das Setup für monotone effiziente Interpolation erfüllt*, wenn gilt:*

1. *$A \cup B$ ist unerfüllbar und*
2. *jedes der Atome aus $\overline{p}$ kommt nur positiv in A vor oder jedes der Atome aus $\overline{p}$ kommt nur negativ in B_n vor.*

Seien $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ und $(w_n)_{n\in\mathbb{N}}$ Folgen natürlicher Zahlen und seien

$$\overline{p_n} = (p_1, \ldots, p_{u_n}), \quad \overline{q_n} = (q_1, \ldots, q_{v_n}), \quad \overline{r} = (r_1, \ldots, r_{w_n})$$

Folgen von Tupeln von Variablen, sodass für jedes $n \in \mathbb{N}$ die Tupel $\overline{p_n}$, $\overline{q_n}$, $\overline{r_n}$ paarweise disjunkt sind. Seien weiter

$$A_n = \big\{A_1(\overline{p_n}, \overline{q_n}), \ldots, A_{m_n}(\overline{p_n}, \overline{q_n})\big\}$$
$$B_n = \big\{B_1(\overline{p_n}, \overline{r_n}), \ldots, B_{l_n}(\overline{p_n}, \overline{r_n})\big\}$$

Folgen von Klauselmengen. Sei weiter $C_n = (A_n, B_n)$. Wir sagen, dass die Folge $(C_n)_{n\in\mathbb{N}}$ das Setup für monotone effiziente Interpolation erfüllt*, wenn gilt:*

1. *Für jedes $n \in \mathbb{N}$ erfüllt C_n das Setup für monotone effiziente Interpolation und*
2. *die Anzahl der Klauseln und Variablen in $A_n \cup B_n$ is polynomial beschränkt:*
$$u_n, v_n, w_n, m_n, l_n = n^{O(1)}.$$

Definition 2. *Sei P ein Beweissystem. Wir sagen, P* erlaubt monotone effiziente Interpolation*, wenn es eine Funktion $f : \{0,1\}^* \to \{0,1\}^*$ gibt, für die gilt:*

1. *Für jede P-Widerlegung π von Klauselmengen $A(\overline{p}, \overline{q}) \cup B(\overline{p}, \overline{r})$, sodass (A, B) das Setup für monotone effiziente Interpolation erfüllt, gilt:*
   (a) *$f(\pi)$ ist ein monotoner Schaltkreis $I(\overline{p})$.*
   (b) *$I(\overline{p})$ interpoliert die Implikation*
   $$A(\overline{p}, \overline{q}) \to \neg B(\overline{p}, \overline{r}),$$
   das heißt
   $$A(\overline{p}, \overline{q}) \to I(\overline{p}) \quad \textit{und} \quad I(\overline{p}) \to \neg B(\overline{p}, \overline{r}).$$
   (Wir nennen so einen Schaltkreis einen interpolierenden Schaltkreis für (A, B)*)*
2. *f ist polynomial beschränkt: $\big|f(\pi)\big| = |\pi|^{O(1)}$.*

Aus Definition 2 folgt direkt

Lemma 3. *Es gelte:*

1. $((A_n, B_n))_{n\in\mathbb{N}}$ *sei eine Folge, die das Setup für monotone effiziente Interpolation erfüllt.*
2. *Jeder monotone interpolierende Schaltkreis für* (A_n, B_n) *habe mindestens Größe* $s(n)$.
3. P *sei ein Beweissystem, das monotone effiziente Interpolation erlaubt.*

Dann gilt für jede P*-Widerlegung* π *der Klauselmenge* $A_n \cup B_n$*:*

$$|\pi| = s(n)^{\Omega(1)}.$$

2 Untere Schranke für monotone Schaltkreise

Wir beschäftigen uns nun damit, wie wir eine Folge konstruieren können, die das Setup für monotone effiziente Interpolation erfüllt. Seien $\overline{p}, \overline{q}$ disjunkte Tupel von Variablen und sei n die Anzahl der Variablen in $\overline{p}$. Dann setzen wir für eine Klauselmenge $C(\overline{p}, \overline{q})$

$$\mathrm{Sat}_n(C) := \left\{\overline{a} \in \{0,1\}^n \;\middle|\; C(\overline{a}, \overline{q}) \in \mathrm{SAT}\right\}.$$

Wir beobachten, dass jeder interpolierende Schaltkreis $I(\overline{p})$, wie in Definition 2 die Mengen $\mathrm{Sat}_n(A)$ und $\mathrm{Sat}_n(B)$ trennt:

Definition 4. *Sei* $n \in \mathbb{N}$ *und* $\overline{p} = (p_1, \ldots, p_n)$ *ein Tupel von verschiedenen Variablen. Ein Schaltkreis* $I(\overline{p})$ trennt die Mengen $U, V \subseteq \{0,1\}^n$*, falls für*

$$W(I) := \left\{\overline{a} \in \{0,1\}^n \;\middle|\; I(\overline{a}) = 1\right\}$$

gilt: $U \subseteq W(I)$ *und* $W(I) \cap V = \emptyset$.

Die Mengen $\mathrm{Sat}_n(A)$ und $\mathrm{Sat}_n(B)$ geben uns eine Möglichkeit eine Folge (A_n, B_n) zu konstruieren, die das Setup für monotone effiziente Interpolation erfüllt. Um die Polaritätseigenschaften der gemeinsamen Variablen in A_n und B_n anhand der Sat_n-Mengen festzustellen, brauchen wir zunächst ein paar Begriffe.

Definition 5. *Sei* $n \in \mathbb{N}$*. Für* $\overline{a}, \overline{b} \in \{0,1\}^n$ *definieren wir die Produktordnung*

$$\overline{a} \preceq \overline{b} : \iff \forall i \leq n \; a_i \leq b_i,$$

sowie $\overline{a} \succeq \overline{b} : \iff \overline{b} \preceq \overline{a}$.

Definition 6. *Sei $n \in \mathbb{N}$. Eine Menge $L \subseteq \{0,1\}^n$ heißt* nach oben (unten) abgeschlossen in $\{0,1\}^n$*, wenn für $\overline{a} \in L$ und $\overline{b} \in \{0,1\}^n$ mit $\overline{a} \preceq \overline{b}$ ($\overline{a} \succeq \overline{b}$) gilt: $\overline{b} \in L$. Eine Menge $L \subseteq \{0,1\}^*$ heißt* nach oben (unten) abgeschlossen*, wenn $L \cap \{0,1\}^n$ für alle $n \in \mathbb{N}$ nach oben (unten) abgeschlossen in $\{0,1\}^n$ ist.*

Mithilfe geeigneter NP-Mengen können wir Folgen konstruieren, die das Setup für monotone effiziente Interpolation erfüllen:

Lemma 7. *Seien U und V disjunkte* NP*-Mengen, sodass U nach oben abgeschlossen ist oder V nach unten abgeschlossen ist. Dann existiert eine Folge $((A_n, B_n))_{n\in\mathbb{N}}$, die das Setup für monotone effiziente Interpolation erfüllt, sodass gilt:*

1. *$U \cap \{0,1\}^n = Sat_n(A_n)$,*
2. *$V \cap \{0,1\}^n = Sat_n(B_n)$ und*
3. *für jeden monotonen Schaltkreis I gilt: I ist interpolierender Schaltkreis für (A_n, B_n) genau dann wenn I die Mengen $Sat_n(A_n)$ und $Sat_n(B_n)$ trennt.*

Beweis. Wir setzen

$$U_n := U \cap \{0,1\}^n\,, \qquad V_n := V \cap \{0,1\}^n\,.$$

Wegen der NP-Vollständigkeit von SAT existieren dann Klauselmengen $A'_n(\overline{p_n}, \overline{q_n})$ und $B'_n(\overline{p_n}, \overline{r_n})$ mit $U_n = \mathrm{Sat}_n(A'_n)$ und $V_n = \mathrm{Sat}_n(B'_n)$, sodass die Anzahl der Klauseln und Variablen in A'_n und B'_n polynomial durch n beschränkt sind.

Falls U nach oben abgeschlossen ist, setzen wir $B_n := B'_n$ und betrachten die Klauselmenge $A_n(\overline{p_n}, \overline{q_n})$, die aus A'_n dadurch entsteht, dass jedes negative Vorkommen der Atome aus $\overline{p_n}$ entfernt wird. Dann kommen die Atome aus $\overline{p_n}$ in A_n nur positiv vor. Wir zeigen, dass für jedes $\overline{a} \in \{0,1\}^n$ gilt: $A_n(\overline{a}, \overline{q_n})$ ist genau dann erfüllbar, wenn $A'_n(\overline{a}, \overline{q_n})$ erfüllbar ist.

Sei $A_n(\overline{a}, \overline{q_n})$ erfüllbar. Dann gibt es eine Belegung der $\overline{q_n}$, sodass jede Klausel aus $A_n(\overline{a}, \overline{q_n})$ erfüllt ist. Da jede der Klauseln aus $A'_n(\overline{a}, \overline{q_n})$ eine Obermenge einer der Klauseln in $A_n(\overline{a}, \overline{q_n})$ ist, ist auch $A'_n(\overline{a}, \overline{q_n})$ erfüllbar.

Sei $A'_n(\overline{a}, \overline{q_n})$ erfüllbar. Da U_n nach oben abgeschlossen in $\{0,1\}^n$ ist und $\overline{a} \preceq (1,\ldots,1)$, ist $A'_n((1,\ldots,1), \overline{q_n})$ erfüllbar und A_n ist nach Konstruktion erfüllbar, wenn $A'_n((1,\ldots,1), \overline{q_n})$ erfüllbar ist.

Falls stattdessen V nach unten abgeschlossen ist, setzen wir $A_n := A'_n$ und wir können analog eine Klauselmenge $B_n(\overline{p_n}, \overline{r_n})$ konstruieren, indem wir die positiven Vorkommen der Atome aus $\overline{p_n}$ in B'_n entfernen, sodass für jedes $\overline{a} \in \{0,1\}^n$ gilt: $B_n(\overline{a}, \overline{r_n})$ ist genau dann erfüllbar, wenn $B'_n(\overline{a}, \overline{r_n})$ erfüllbar ist.

Damit folgt $U_n = \mathrm{Sat}_n(A_n)$ und $V_n = \mathrm{Sat}_n(B_n)$. Da U und V disjunkt sind, sind auch U_n und V_n disjunkt, womit $A_n \cup B_n$ unerfüllbar ist. Somit ist $C_n = (A_n, B_n)$ eine Folge, die das Setup für monotone effiziente Interpolation erfüllt.

Sei nun $I(\overline{p_n})$ ein monotoner Schaltkreis. Da

$$A_n(\overline{p}, \overline{q}) \to I(\overline{p}) \quad \text{und} \quad I(\overline{p}) \to \neg B(\overline{p}, \overline{r}),$$

genau dann erfüllt ist, wenn $U_n \subseteq W(I)$, sowie $W(I) \cap V_n = \emptyset$ gilt (wenn also $W(I)$ die Mengen U_n und V_n trennt), folgt die Behauptung. □

Damit haben wir das Problem, eine geeignete Folge zu finden, die das Setup für monotone effiziente Interpolation erfüllt, darauf reduziert, geeignete NP-Mengen zu finden, die nur durch hinreichend große monotone Schaltkreise getrennt werden können. Wir werden dieses Problem lösen, indem wir die NP-Mengen $\mathrm{Color}_{n,k}$ und $\mathrm{Clique}_{n,\ell}$ betrachten:

Definition 8. *Sei $k \in \mathbb{N}$. Ein ungerichteter Graph (V, E) heißt* k-färbbar*, wenn es eine Funktion $f : V \to \{1, \ldots, k\}$ gibt, sodass für jede Kante $(u, v) \in E$ gilt: $f(u) = f(v) \implies u = v$. Wir nennen f eine* k-Färbung von (V, E). *Für $n, k \in \mathbb{N}$ ist $\mathrm{Color}_{n,k}$ die Menge aller k-färbbaren ungerichteten Graphen mit n Knoten. Weiter setzen wir $\mathrm{Color}_k := \cup_{n\in\mathbb{N}}\mathrm{Color}_{n,k}$.*

Definition 9. *Sei (V, E) ein ungerichteter Graph. Eine Teilmenge $C \subseteq V$ heißt* Clique von (V, E)*, falls für alle $u \neq v \in C$ gilt: $(u, v) \in E$. Für $n, \ell \in \mathbb{N}$ ist $\mathrm{Clique}_{n,\ell}$ die Menge aller ungerichteten Graphen mit n Knoten, die eine Clique C mit $|C| \geq \ell$ besitzen. Weiter setzen wir $\mathrm{Clique}_\ell := \cup_{n\in\mathbb{N}}\mathrm{Clique}_{n,\ell}$.*

Wir können endliche ungerichtete Graphen durch Binärstrings kodieren: Sei $(\{1, \ldots, n\}, E)$ ein endlicher ungerichteter Graph. Für $1 \leq k < m \leq n$ setzen wir

$$w_{k,m} := \begin{cases} 1 & \text{falls } (k, m) \in E \\ 0 & \text{sonst.} \end{cases}$$

Damit können wir den Graphen durch den String

$$w_{1,2}w_{1,3} \ldots w_{1,n} \ldots w_{n-2,n}w_{n-1,n}$$

der Länge $\binom{n}{2}$ darstellen. Auf diese Weise können wir die Mengen Color_k und Clique_ℓ als Teilmengen von $\{0, 1\}^*$ betrachten. Weiter fassen wir einige Eigenschaften von Color_k und Clique_ℓ zusammen in

Proposition 10. *Es gilt:*

1. *Color_k und Clique_ℓ sind* NP*-Mengen.*
2. *Für $k < \ell$ sind Color_k und Clique_ℓ disjunkt.*
3. *Color_k ist nach unten abgeschlossen.*
4. *Clique_ℓ ist nach oben abgeschlossen.*

Beweis. Zunächst kann in polynomialer Zeit entschieden werden, ob ein $x \in \{0,1\}^*$ einen Graph der Länge n darstellt, indem die Länge von x betrachtet wird.

Color_k ist eine NP-Menge, da für einen gegebenen Graphen G der Größe n und eine Funktion $f : \{1,\dots,n\} \to \{1,\dots,k\}$ in höchstens $\binom{n}{2}$ Schritten entschieden werden kann, ob f eine k-Färbung für G ist, indem die definierende Bedingung für alle Kanten überprüft wird.

Clique_ℓ ist eine NP-Menge, da für einen gegebenen Graphen (V,E) und eine Teilmenge $C \subseteq V$ in höchstens $\binom{n}{2}$ Schritten entschieden werden kann, ob C eine Clique ist, indem die definierende Bedingung für alle Knoten in C überprüft wird.

Color_k und Clique_ℓ sind disjunkt: Sei $k < \ell$ und sei $f : \{1,\dots,n\} \to \{1,\dots,k\}$ eine k-Färbung von $(V,E) \in \text{Color}_k$. Angenommen $C \subseteq V$ sei eine Clique mit $|C| \geq \ell > k$. Da je zwei Knoten $u, v \in C$ miteinander verbunden sind, folgt aber $f(u) \neq f(v)$ und somit $\left|f(C)\right| \geq \ell$ im Widerspruch dazu, dass f eine k-Färbung von (V,E) ist.

Color_k ist nach unten abgeschlossen: Sei $m \in \mathbb{N}$. Falls $m \neq \binom{n}{2}$ für alle $n \in \mathbb{N}$, dann ist $\text{Color}_k \cap \{0,1\}^m = \emptyset$ trivialerweise nach unten abgeschlossen in $\{0,1\}^m$. Falls $m = \binom{n}{2}$ für ein $n \in \mathbb{N}$, dann ist $\text{Color}_k \cap \{0,1\}^m = \text{Color}_{n,k}$ nach unten abgeschlossen in $\{0,1\}^m$, da jede k-Färbung eines Graphen auch jeden Teilgraphen färbt.

Clique_ℓ ist nach oben abgeschlossen: Wir betrachten nur den Fall $m = \binom{n}{2}$, der andere Fall verläuft analog wie bei Color_k. Dann gilt $\text{Clique}_\ell \cap \{0,1\}^m = \text{Clique}_{m,\ell}$ ist nach oben abgeschlossen, da jede Clique mit der Größe mindestens ℓ erhalten bleibt, wenn Kanten in einem Graph hinzugefügt werden. □

Wir zitieren hier eine untere Schranke für monotone Schaltkreise, die Color_k und Clique_ℓ trennen:

Satz 11 (Razborov, Alon, Boppana)**.** *Sei $n \in \mathbb{N}$, $3 \leq k < \ell$ und es gelte*

$$\sqrt{k}\ell \leq \frac{n}{8\log(n)}.$$

Dann hat jeder monotone Schaltkreis, der $\text{Color}_{n,k}$ und $\text{Clique}_{n,\ell}$ trennt, mindestens Größe $\Omega\left(2^{\sqrt{k}}\right)$.

Damit können wir eine untere Schranke für Beweissysteme zeigen, die monotone effiziente Interpolation erlauben:

Satz 12. *Sei P ein Beweissystem, das monotone effiziente Interpolation erlaubt. Dann existiert eine Folge $((A_n, B_n))_{n\in\mathbb{N}}$, die das Setup für monotone effiziente Interpolation erfüllt, sodass für jede P-Widerlegung π von $A_n \cup B_n$ gilt:*

$$|\pi| = \Omega\left(2^{\sqrt[6]{n}}\right).$$

Insbesondere sind Beweissysteme, die monotone effiziente Interpolation erlauben, nicht polynomial beschränkt.

Beweis. Wir setzen $k_n := \lfloor n^{1/3} \rfloor$, $\ell_n := \lceil n^{2/3} \rceil$. Dann sind die Mengen Color_{k_n} und Clique_{ℓ_n} nach Proposition 10 für alle $n \geq 1$ disjunkt und Color_{k_n} ist nach unten abgeschlossen. Nach Lemma 7 existiert für alle $n \geq 1$ eine Folge $((A_m^{(n)}, B_m^{(n)}))_{m\in\mathbb{N}}$, die das Setup für monotone effiziente Interpolation erfüllt, sodass für $A_n := A^{(n)}_{\binom{n}{2}}$ und $B_n := B^{(n)}_{\binom{n}{2}}$, gilt:

$$\text{Color}_{n,k_n} = \text{Sat}_{\binom{n}{2}}(A_n) \quad \text{und} \quad \text{Clique}_{n,\ell_n} = \text{Sat}_{\binom{n}{2}}(B_n).$$

Weiters ist auch (A_n, B_n) eine Folge, die das Setup für monotone effiziente Interpolation erfüllt.

Sei nun I ein monotoner interpolierender Schaltkreis für (A_n, B_n). Nach Lemma 7, trennt I die Mengen Color_{n,k_n} und Clique_{n,ℓ_n} und mit Satz 11 folgt für n hinreichend groß $|I| = \Omega\left(2^{\sqrt[6]{n}}\right)$. Damit folgt insgesamt mit Lemma 3: $|\pi| = \Omega\left(2^{\sqrt[6]{n}}\right)$. □

3 Untere Schranke für den Resolutionskalkül

Der Resolutionskalkül R ist ein Beweisystem, das auf Klauselmengen operiert. Die einzige Schlussregel ist die Resolutionsregel für Klauselmengen A, B und ein Atom p:

$$\frac{A \cup \{p\} \quad B \cup \{\neg p\}}{A \cup B}$$

Der Resolutionskalkül ist ein Widerlegungssystem: Um zu zeigen, dass eine Formel φ eine Tautologie ist, reicht es zu zeigen, dass aus $\text{CNF}(\neg\varphi)$ die leere Klausel hergeleitet werden kann, das heißt, dass $\neg\varphi$ nicht erfüllbar sein kann. Wir werden nur Widerlegungen von Klauselmengen betrachten:

Definition 13. *Eine R-Widerlegung π einer Klauselmenge C ist eine endliche Folge von Klauseln $(C_1, \ldots, C_n)$, sodass für $1 \leq i \leq n$ gilt:*

1. *$C_i \in C$ oder*
2. *es gibt $1 \leq j, k < i$ sodass C_i durch Resolution aus C_j und C_k hervorgeht.*

Weiter soll gelten $C_n = \emptyset$.

Satz 14. *R erlaubt monotone effiziente Interpolation.*

Beweis. Seien $A(\overline{p}, \overline{q})$ und $B(\overline{p}, \overline{r})$ Klauselmengen, sodass (A, B) das Setup für monotone effiziente Interpolation erfüllt. Wir betrachten zunächst den Fall, dass die Variablen aus $\overline{p}$ nur positiv in A auftreten. Sei weiter $\pi = (C_1, \ldots, C_k)$ eine R-Widerlegung von $A \cup B$.

Für Klauseln C schreiben wir C^p, C^q und C^r für jene Teilmengen von C, die aus den Literalen bestehen, die nur Atome aus $\overline{p}$, $\overline{q}$ bzw. $\overline{r}$ enthalten. Weiter setzen wir $C^{p,r} := C^p \cup C^r$. Wir konstruieren induktiv einen Schaltkreis, indem wir für alle $1 \leq i \leq k$ Variablen y_i betrachten und sie so zuweisen, dass der Schaltkreis mit Ausgabe y_i die Implikation

$$A \wedge \neg C_i^q \to C_i^{p,r} \vee \neg B \tag{$*$}$$

interpoliert.

Wir betrachten $C_i^p = \{L_1, \ldots, L_m\}$. Falls $C_i \in A$, definieren wir für $0 \leq j < m$ induktiv $y_{i,0} := \bot$ und $y_{i,j+1} := y_{i,j} \vee L_j$. Weiter setzen wir $y_i := y_{i,m}$. Damit berechnet y_i die Disjunktion $\bigvee C_i^p$, die ($*$) interpoliert. Falls $C_i \in B$, setzen wir $y_i := \top$.

Falls C_i durch Resolution einer Variable x aus $\overline{p}$ oder $\overline{r}$ aus C_j und C_l hervorgeht, das heißt

$$C_i = C_j \setminus \{x\} \cup C_l \setminus \{\neg x\},$$

setzen wir $y_i := y_j \wedge y_l$. Dann interpoliert der Schaltkreis mit Ausgabe y_i die Implikation ($*$): Zunächst gilt $C_i^q = C_j^q \cup C_l^q$ und

$$C_i^{p,r} = (C_j^{p,r} \setminus \{x\}) \cup (C_l^{p,r} \setminus \{\neg x\}).$$

Seien nun I_j und I_l Interpolanten für ($*$) in Bezug auf C_j bzw. C_l. Dann gilt

$$A \wedge \neg \underbrace{(C_j^q \cup C_l^q)}_{=C_i^q} \to I_j \wedge I_l$$

und

$$I_j \wedge I_l \to \left(C_j^{p,r} \wedge C_l^{p,r}\right) \vee \neg B.$$

Weiter ist

$$C_j^{p,r} \wedge C_l^{p,r}$$

äquivalent zu

$$\Big((C_j^{p,r} \setminus \{x\}) \vee x\Big) \wedge \big((C_l^{p,r} \setminus \{\neg x\}) \vee \neg x\big)$$

bzw.

$$\begin{aligned}&\Big((C_j^{p,r} \setminus \{x\}) \wedge (C_l^{p,r} \setminus \{\neg x\})\Big)\\ &\vee(\neg x \wedge (C_j^{p,r} \setminus \{x\}))\\ &\vee(x \wedge (C_l^{p,r} \setminus \{\neg x\}))\\ &\vee (x \wedge \neg x)\,.\end{aligned}$$

Aus jedem dieser Disjunkte folgt $\bigvee C_i^{p,r}$, womit gezeigt ist, dass $I_j \wedge I_l$ die gewünschte Interpolationseigenschaft hat.

Falls C_i durch Resolution einer Variable aus $\overline{q}$ aus C_j und C_k hervorgeht, setzen wir $y_i := y_j \vee y_k$ und können auf ähnliche Weise wie zuvor zeigen, dass die gewünschte Interpolationseigenschaft erfüllt ist.

Schließlich ist der Schaltkreis mit Ausgabe y_k der gesuchte Schaltkreis für die monotone effiziente Interpolation, da $C_k = \emptyset$ und damit die Implikation $(*)$ äquivalent zur gewünschten Implikation $A \to \neg B$ ist. Der Schaltkreis ist monoton, da alle p in A nur positiv auftreten. Sei n die Anzahl der Variablen in $\overline{p}$. Dann ist die Anzahl der Instruktionen des Schaltkreises durch kn beschränkt. Damit erlaubt R monotone effiziente Interpolation.

Falls die Variablen aus $\overline{p}$ nur negativ in B auftreten, verläuft der Beweis analog. Der induktiv konstruierte Schaltkreis interpoliert in diesem Fall mit $C^{p,q} := C^p \cup C^q$ die Implikation

$$A \wedge \neg C_i^{p,q} \to C_i^r \vee \neg B.$$

□

Unter Anwendung von Satz 12 folgt

Korollar 15. *R ist nicht polynomial beschränkt.*

4 Untere Schranke für den schnittfreien Sequentialkalkül

Der schnittfreie Sequentialkalkül LK^- operiert auf *Sequenten*, das sind Paare von endlichen Folgen von Formeln Γ, Δ geschrieben als

$$\Gamma \longrightarrow \Delta.$$

Γ heißt *Antezedent* und Δ heißt *Sukzedent*. Ein Sequent ist wahr unter einer Wahrheitsbelegung, wenn eine Formel in Γ unter der Wahrheitsbelegung falsch ist, oder wenn eine Formel in Δ unter der Wahrheitsbelegung wahr ist.

Um zu zeigen, dass LK^- monotone effiziente Interpolation erlaubt, ist es praktisch, dass wir uns auf Formeln in konjunktiver Normalform bzw. Klauselmengen beschränken. Dann können wir Negationsregeln durch zusätzliche initiale Sequente ersetzen. Damit betrachten wir die folgenden Schlussregeln:

Definition 16. *Die Schlussregeln des schnittfreien Sequentialkalküls LK^- sind:*

- *Initiale Sequenten:*

$$p \longrightarrow p, \quad \bot \longrightarrow, \quad \longrightarrow \top,$$
$$p, \neg p \longrightarrow, \quad \longrightarrow p, \neg p, \quad \neg p \longrightarrow \neg p, \quad \neg\top \longrightarrow, \quad \longrightarrow \neg\bot,$$

  wobei p ein Atom ist.

- *Strukturregeln:*
  - *Abschwächungsregeln:*

$$\frac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \text{ und } \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}.$$

  - *Austauschregeln:*

$$\frac{\Gamma_1, A, B, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, B, A, \Gamma_2 \longrightarrow \Delta} \text{ und } \frac{\Gamma \longrightarrow \Delta_1, A, B, \Delta_2}{\Gamma \longrightarrow \Delta_1, B, A, \Delta_2}.$$

  - *Kontraktionsregeln:*

$$\frac{\Gamma_1, A, A, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, A, \Gamma_2 \longrightarrow \Delta} \text{ und } \frac{\Gamma \longrightarrow \Delta_1, A, A, \Delta_2}{\Gamma \longrightarrow \Delta_1, A, \Delta_2}.$$

- *logische Regeln:*
  - *Konjunktionsregeln:*

$$\frac{A, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta} \text{ bzw. } \frac{A, \Gamma \longrightarrow \Delta}{B \wedge A, \Gamma \longrightarrow \Delta}$$
$$\text{und } \frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}.$$

  - *Disjunktionsregeln:*

$$\frac{A, \Gamma \longrightarrow \Delta \qquad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta} \text{ und}$$
$$\frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \vee B} \text{ bzw. } \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, B \vee A}.$$

Analog zu R-Widerlegungen definieren wir Widerlegungen in LK^-:

Definition 17. *Eine* LK^--Herleitung *ist eine endliche Folge von Sequenten* $(S_1, \dots, S_n)$*, sodass für alle* $1 \leq i \leq n$ *gilt:*

1. S_i *ist ein initialer Sequent oder*
2. *es gibt ein* $j < i$*, sodass* S_i *durch Anwendung einer einstelligen Schlussregel aus Definition 16 auf* S_j *entsteht oder*
3. *es gibt ein* $j, k < i$*, sodass* S_i *durch Anwendung einer zweistelligen Schlussregel aus Definition 16 auf* S_j *und* S_k *entsteht.*

Seien $A = \{A_1, \dots, A_k\}$ *und* $B = \{B_1, \dots, B_\ell\}$ *Klauselmengen. Eine* LK^-*-Herleitung, die in*

$$\bigvee A_1, \dots, \bigvee A_k \longrightarrow \bigwedge \neg B_1, \dots, \bigwedge \neg B_\ell$$

endet, nennen wir LK^--Widerlegung von $A \cup B$.

Satz 18. LK^- *erlaubt monotone effiziente Interpolation.*

Beweis. Seien $A(\overline{p}, \overline{q})$ und $B(\overline{p}, \overline{r})$ Klauselmengen, sodass (A, B) das Setup für monotone effiziente Interpolation erfüllt. Sei weiter π eine LK^--Widerlegung von $A \cup B$.

Wir können ohne Beschränkung der Allgemeinheit annehmen, dass jeder Antezedent in π keine Variablen aus $\overline{r}$ und jeder Sukzedent keine Variablen aus $\overline{q}$ enthält, da es keine Schlussregel gibt, sodass Variablen, die ausschließlich im Antezedenten auftreten, nach Anwendung der Schlussregel im Sukzedenten auftreten (und umgekehrt). Da der letzte Sequent in π die Eigenschaft hat, dass die Variablen aus $\overline{q}$ und $\overline{r}$ getrennt sind, reicht es, nur jene Sequenten in π zu betrachten, die diese Trennungseigenschaft haben. Zudem können wir voraussetzen, dass kein Sequent der Form $\neg p \longrightarrow \neg p$ in π auftritt, da die Variablen aus $\overline{p}$ entweder nur positiv in A bzw. nur negativ in B (und damit nur positiv im Sukzedenten) auftreten.

Wir definieren nun induktiv einen Schaltkreis indem wir zunächst jedem Sequent $S = \Gamma(\overline{p}, \overline{q}) \longrightarrow \Delta(\overline{p}, \overline{r})$ in π eine Variable y_S zuordnen. Außerdem wollen wir die Zuweisung an y_S so wählen, dass der Schaltkreis mit Ausgabe y_S die Implikation $\bigwedge \Gamma \to \bigvee \Delta$ interpoliert. Für die initialen Sequenten setzen wir die Variable y_S folgendermaßen:

Sequent S	y_S
$p \longrightarrow p$	p
$\bot \longrightarrow$	$\bot$
$p, \neg p \longrightarrow$	$\bot$
$\neg\top \longrightarrow$	$\bot$
$\longrightarrow \top$	$\top$
$\longrightarrow p, \neg p$	$\top$
$\longrightarrow \neg\bot$	$\top$

Falls S durch eine einstellige Schlussregel aus dem Sequenten T entsteht, setzen wir $y_S := y_T$. Für jede der einstelligen Schlussregeln überträgt sich die Interpolationseigenschaft von T auf S mit der gleichen Interpolante.

Falls S durch die zweistellige Konjunktionsregel aus den Sequenten U und V entsteht, machen wir die Zuweisung $y_S := y_U \wedge y_V$ und falls S durch die zweistellige Disjunktionsregel aus den Sequenten U und V entsteht, setzen wir $y_S := y_U \vee y_V$. Auch in diesen Fällen überträgt sich die Interpolationseigenschaft.

Sei Z der letzte Sequent in π. Dann interpoliert der Schaltkreis mit Ausgabe y_Z die geforderte Implikation. Dass der Schaltkreis monoton ist, folgt daraus, dass kein Sequent der Form $\neg p \longrightarrow \neg p$ auftritt. Weiter zeigt die Konstruktion, dass die Anzahl der Instruktionen im Schaltkreis durch die Anzahl der Beweisschritte beschränkt ist. Damit erlaubt LK^- monotone effiziente Interpolation □

Mit Satz 12 folgt schließlich

Korollar 19. *LK^- ist nicht polynomial nach unten beschränkt.*

Literatur

[Kra19] Jan Krajíček. *Proof Complexity*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, United Kingdom, 2019.