Universität Koblenz-Landau,
Abteilung Koblenz

FB 4 – Informatik

Seminar

Entscheidungsverfahren für logische Theorien

Endliche Modelle

Tobias Hebel

Koblenz, am 18.02.2005

Inhaltsverzeichnis

1 Einleitung

Viele Probleme in Bezug auf prädikatenlogische Formeln der ersten Ordnung sind im Allgemeinen algorithmisch unentscheidbar. Insbesondere gilt dies für die Frage, ob eine gegebene Formel ein Modell besitzt (Entscheidbarkeitsproblem) oder ob jede zu einer Formel passende Struktur ein Modell dieser Formel ist (Gültigkeitsproblem).
In vielen Fällen ist diese Allgemeinheit jedoch nicht notwendig. Durch die Aufteilung prädikatenlogischer Formeln in Klassen mit bestimmten Eigenschaften können wir die oben gemachte Aussage einschränken und Formelklassen oder genauer Präfixvokabularklassen finden, die entscheidbar sind.

2 Grundlagen

Zur Darstellung und Unterscheidung der verschiedenen Formelklassen werden wir die folgende Notation verwenden, die Formeln in Pränexform beschreibt
Zeichenketten aus dem Alphabet $\{\forall, \exists\}$ nennen wir Präfix. Eine Stelligkeitessequenz ist eine Funktion p, $\mathbb{N} \rightarrow \mathbb{N}_0 \cup \{\omega\}$, wobei ω die erste unendliche Zahl ist.

2.1 Präfixvokabularklassen

Für beliebige Präfixmengen Π und beliebige Stelligkeitessequenzen p und f ist [Π, p, f] (bzw. $[\Pi, p, f]_=$) die Menge aller prädikatenlogischen Pränexformeln erster Ordnung φ ohne Gleichheit (bzw. mit Gleichheit) folgendermaßen definiert:

- das Präfix von φ gehört zu Π,
- die Anzahl der n-stelligen Prädikatssymbole in φ ist ≤ p(n),
- die Anzahl der n-stelligen Funktionssymbole in φ ist ≤ f(n),
- φ enthält keine nullstelligen Prädikatssymbole mit Ausnahme der logischen Konstanten TRUE und FALSE, keine nullstelligen Funktionssymbole und keine freien Variablen.

Die letzte Einschränkung nehmen wir nur vor, um die Übersichtlichkeit zu erhöhen, da nullstellige Prädikatensymbole die Entscheidbarkeit nicht beeinflussen. Ähnlich verhält es sich mit nullstelligen Funktionssymbolen, also Konstanten, da man diese in freie Variablen umbenennen kann, was ebenfalls zu keinen neuen Klassen führt.

Wir nennen eine Präfixmenge geschlossen, wenn sie alle Teilzeichenketten Ihrer Präfixe enthält. Eine Präfixmenge Π heißt Standard, wenn sie entweder die Menge aller möglichen Präfixe ist oder durch eine Zeichenkette $w \in \{\forall, \exists, \forall^*, \exists^*\}$ dargestellt werden kann. Im ersten Fall schreiben wir statt Π nur *all.*

Eine Stelligkeitssequenz p heißt Standard, wenn sie die folgende Bedingung erfüllt: $p(n)=\omega \rightarrow p(n) + p(n+1) + p(n+2) + \ldots = \infty$. Hierbei ist darauf zu achten, dass keine Äquivalenz vorliegt, sondern nur eine Implikation, was in den späteren Kapiteln zu Missverständnissen führen kann. ω bedeutet in diesem Fall auch nicht „unendlich“, sondern eher „beliebig viele“, schließlich gibt es keine unendlich langen Formeln.

Die Standardstelligkeitssequenz, die ω jedem n zuordnet, wird als *all* notiert. Jede andere Stelligkeitssequenz endet mit einer Kette aus Nullen, $0=p(m)=p(m+1)=\ldots$ In diesem Falle wird die Sequenz folgendermaßen notiert: $(p(1), p(2), \ldots, p(m-1))$.

Eine Präfixvokabularklasse [Π, p, f] (bzw. $[\Pi, p, f]_=$) heißt Standard, wenn Π, p und f Standard genannt werden dürfen.

2.2 essentiell endliche Klassen

Wir nennen Präfixvokabularklassen [Π, s] oder $[\Pi, s]_=$ essentiell endlich, bei denen Π und $s=(s_1, s_2,\ldots)$ im folgenden Sinne endliche sind:

- $\Pi \in \{\forall, \exists\}^*$, das heißt, Π enthält kein Vorkommen von $\forall^*$ oder $\exists^*$ und definiert deshalb eine endliche Menge von Präfixen.
- $s_i \neq \omega$ für alle i und $s_i=0$ für alle bis auf endlich viele i. s definiert also nur eine endliche Menge von Prädikatssymbolen, wenn man von Umbenennungen absieht.

Essentiell endliche Klassen sind aus trivialen Gründen entscheidbar. Sie können sehr einfach in eine äquivalente Formel reduziert werden, deren quantorenfreier Teil in minimaler KNF ist. Wenn wir also eine essentiell endliche Formel in eine solche Form überführen, und das Entscheidungsproblem somit auf endlich viele Instanzen reduzieren und die Wahrheitswerte in einer Tabelle nachschlagen, sind wir in der Lage, das Problem zu lösen und nur logarithmischen Workspace zu verbrauchen.

Im Folgenden werden wir unsere Aufmerksamkeit deshalb auf Standartklassen [Π, s, t] (bzw. $[\Pi, s, t]_=$) richten, die mindestens eine der folgenden Bedingungen erfüllen:

- Π enthält ein Vorkommen von $\forall^*$ oder $\exists^*$;
- $t \neq 0$;
- s ist nicht endlich.

Damit ergeben sich 7 maximale entscheidbare Klassen:

2.3 Maximale entscheidbare Klassen

Für jede der folgenden Klassen sind das Erfüllbarkeitsproblem und das endliche Erfüllbarkeitsproblem entscheidbar:

(1) $[\exists^*\forall^*, all]_=$

(2) $[\exists^*\forall^2\exists^*, all]$

(3) $[all, (\omega), (\omega)]$

(4) $[\exists^*\forall\exists^*, all, all]$

(5) $[\exists^*, all, all]_=$

(6) $[all, (\omega), (1)]_=$

(7) $[\exists^*\forall\exists^*, all, (1)]_=$

Für die Klasse (3) werden wir das im Kapitel 3 exemplarisch mit der „endliches Modell“ – Eigenschaft beweisen.

2.4 Die „endliches Modell“ - Eigenschaft

Eine Klasse $X \subseteq FO$[1] besitzt die „endliches Modell“ - Eigenschaft, wenn SAT(X)=FIN-SAT(X), das heißt, wenn jede erfüllbare Formel in X ein endliches Modell hat. Ein Modell ist endlich, wenn es ein endliches Universum besitzt.

Obwohl die „endliches Modell“ - Eigenschaft einer Klasse X impliziert, dass SAT(X) entscheidbar ist, gibt sie oft keinen Hinweis auf dessen Komplexität. In den meisten Fällen erfordert der Nachweis der „endliches Modell“ – Eigenschaft eine obere Grenze s(n).

2.5 Die „kleines Modell“ - Eigenschaft

Wenn jede erfüllbare Formel $\psi \in X$ ein Modell der Kardinalität $k \leq s(|\psi|)$ besitzt, sagen wir, dass ψ die „kleines Modell“ – Eigenschaft besitzt. Damit haben wir eine nichtdeterministische obere Grenze für die Komplexität von SAT(X) festgelegt, wie im Folgenden gezeigt.

2.6 Eine Abschätzung der Komplexität

Die Frage, ob eine gegebene prädikatenlogische Formel erster Ordnung der Länge n mit k universellen Quantoren ein Modell der Länge m besitzt, kann nichtdeterministisch in der Zeit $p(m^k n)$ entschieden werden, für ein Polynom p.

Beweis: Zur Erinnerung, jede Formel $\psi \in FO$ ist über dem gleichen Universum erfüllbar wie ihre Skolemnormalform und kann leicht in diese überführt werden[2].
Wir können also annehmen, dass die gegebene Formel die Form $\forall x_1 \ldots \forall x_k \varphi$ hat, wobei φ quantorenfrei ist.
Um zu überprüfen, ob diese Formel ein Modell $\mathcal{A}$ mit einem Universum $A=\{a_0,\ldots a_{m-1}\}$ hat, geht der Entscheidungsalgorithmus alle k-Tupel $a_1, \ldots, a_k \in A^k$ durch und rät hinreichende Informationen über $\mathcal{A}$, um zu testen, ob $\mathcal{A} \models \varphi[a_1, \ldots, a_k]$, ob also $\mathcal{A}$ mit der Belegung $a_1, \ldots, a_k$ aus dem Universum A ein Modell von φ ist.

[1] First Order (Logic) = Prädikatenlogik erster Ordnung
[2] siehe z.B.: Schöning, 2000, Seite 63

Da der Wahrheitswert von $\varphi[a_1, \ldots, a_k]$ von höchstens n Termen und atomaren Formeln abhängt, müssen für die Bestätigung, dass $\mathcal{A} \models \forall x_1 \ldots \forall x_k \varphi$ höchstens $m^k n$ Funktions- und Wahrheitswerte geraten werden. Dieser Wert ergibt sich, weil es im Universum der Größe m genau m^k k-Tupel von Individuen gibt und für jeden k-Tupel n Funktions- und Wahrheitswerte geraten werden müssen.

Während der Berechnung generiert und unterhält der Entscheidungsalgorithmus eine konsistente Liste von Funktions- und Wahrheitswerten atomarer Formeln. Immer, wenn ein Funktionswert $f(b_1,\ldots,b_r)$ oder ein Wahrheitswert $P(b_1,\ldots,b_s)$ benötigt wird, überprüft er, ob der Wert schon in der Liste ist. Wenn nicht, wird er geraten und der Liste hinzugefügt.

Elemente dieser Struktur können mit O(log m) Bits dargestellt werden, also benötigt jeder Eintrag der Liste nicht mehr als n log m Bits. Daraus folgt, dass die Liste mit $O(n^2 m^k \log m)$ Schritten erzeugt werden kann – man erinnere sich, dass es höchstens $m^k n$ Einträge von einer Länge von höchstens n log m gibt.

Die Zeit, die der Algorithmus zur Entscheidungsfindung braucht, ist ein kleines Polynom vom Grad der Länge der Liste, also ein Polynom in $m^k n$.

□

3 Anwendung der „endliches Modell“ – Eigenschaft

Interessanterweise wurden, bevor Church und Turing die Unentscheidbarkeit der Prädikatenlogik bewiesen, positive Lösungen des Entscheidungsproblems für einzelne Unterklassen gefunden. Die Bekanntesten Vertreter dieser Klassen sind die folgenden:

3.1 Klassische Entscheidbare Klassen

Die Folgenden Klassen werden die Klassischen Entscheidbaren Klassen genannt, da für sie schon sehr früh positive Lösungen des Entscheidungsproblems vorlagen.

[all, (ω)]	Löwenheim – 1915
[$\exists^*\forall^*$, all]	Bernays, Schönfinkel – 1928
[$\exists^*\forall\exists^*$, all]	Ackermann – 1928
[$\exists^*\forall^2\exists^*$, all]	Gödel – 1932, Kalmar – 1933, Schütte – 1934

Wir werden die „endliche Modell“ – Eigenschaft exemplarisch an der ersten Klasse nachweisen und diese erweitern, so dass sie zu einer der maximal entscheidbaren Klassen wird.

3.2 Monadische Formeln

Die Klassen [all, (ω)] und [all, (ω)]$_=$ heißen Löwenheimklasse und Löwenheimklasse mit Gleichheit. Die Formeln in diesen Klassen heißen relationale monadisch Formeln. Sie enthalten nur einwertige Prädikatssymbole und keine Funktionssymbole.
Wenn wir die Löwenheimklasse mit einwertigen Funktionssymbolen erweitern, erhalten wir die volle monadische Klasse [*all*, (ω), (ω)], die eine der maximalen entscheidbaren Klassen ist. Ihre Elemente heißen monadische Formeln.

Im Weiteren werden wir beweisen, dass die Löwenheimklasse mit Gleichheit und die volle monadische Klasse die „endliche Modell“ – Eigenschaft besitzen. Dazu werden wir Abschätzungen der Größe minimaler Modelle monadischer Formeln angeben und so die „kleines Modell“ – Eigenschaft der Klassen beweisen.

3.3 „kleines Modell" – Eigenschaft für die Löwenheimklasse mit Gleichheit

Sei ψ eine relationale monadische Formel, eventuell mit Gleichheit, vom Quantorenrang q mit m Prädikaten. Wenn ψ erfüllbar ist, dann hat es ein Modell der Kardinalität von höchstens $q2^m$.

Beweis: Sei $\mathcal{A}$= (A, P_1,…, P_m) $\models$ ψ. Nun konstruieren wir zu jedem $a \in A$ eine „Farbe" $c(a)=c_1 \ldots c_m \in \{0,1\}^*$ (also eine Kette von Nullen und Einsen, die so viele Stellen hat, wie die Formel Prädikate). Hierbei wird $c_i=1$, gdw. $\mathcal{A} \models P_i a$. Sei $A_c \subseteq A$ die Menge aller a mit der Farbe c. Damit sind alle Elemente des Universums, die zum gleichen Ergebnis führen, in jeweils einer Menge enthalten.
Jetzt wählen wir für jedes $c \in \{0,1\}^m$ eine Menge $B_c \subseteq A_c$ so, dass $B_c=A_c$ wenn $|A_c| \leq q$ und $|B_c| = q$, wenn $|A_c| > q$. Sei nun $\mathcal{B}$ die so erhaltene Unterstruktur von $\mathcal{A}$ mit dem Universum B := $\bigcup_{c\in\{0,1\}^m} B_c$. Wir haben A also ohne Darstellungsmöglichkeiten zu verlieren gekürzt, so dass $|B| \leq q2^m$.
Keine Formel mit q Variablen (und mehr darf sie nicht haben, da wir nur q Quantoren zulassen und keine freien Variablen) kann zwischen $\mathcal{A}$ und $\mathcal{B}$ unterscheiden. Aus $\mathcal{A} \models \psi$ und ψ hat den Quahntorenrang q folgt: $\mathcal{B} \models \psi$.

□

⇒ **Das Erfüllbarkeitsproblem für relationale monadische Formeln ist entscheidbar.**

Für die Löwenheimklasse ohne Gleichheit ergibt sich sogar die niedrigere Grenze von 2^m Elementen, da hier ein Element von jeder Farbe ausreichend ist.

Für die volle monadische Klasse erhalten wir eine etwas höhere obere Grenze für die Größe der Strukturen, die überprüft werden.

3.4 Komplexitätsabschätzung für die volle monadische Klasse

Jede erfüllbare (voll) monadische Formel ψ der Länge n hat ein Modell der Kardinalität $2^{O(n)}$.

Beweis: Wir werden zeigen, dass jede monadische Formel ψ der Länge n in eine Formel φ∈[all, (ω), (0)] überführt werden kann, so dass ψ und φ über dem gleichen Universum erfüllbar sind.
Sei also ψ eine monadische Formel, die das Atom Pft enthält, wobei P ein monadisches Prädikat, f ein Funktionssymbol und t ein Term ist. Und sei Q ein neues Prädikat, das noch nicht in ψ vorkommt. Dann ist ψ über dem gleichen Universum erfüllbar wie:

$$\psi\,[Pft\,/\,Qt] \wedge \forall x\,(Pfx \leftrightarrow Qx)$$

Dabei erhalten wir ψ[Pft / Qt) aus ψ, indem wir jedes Vorkommen des Atoms Pft in ψ durch Qt (bei jeweils beliebigem t) ersetzen. Wiederholtes Durchführen dieses Verfahrens erzeugt eine Formel:

$$\psi' := \alpha \wedge \forall x\beta$$

Dabei enthält α keine Funktionssymbole und β ist eine Konjuktion von Äquivalenzen der Form Pfx ↔ Qx.
Seien $f_1,\ldots, f_m$ die Funktionssymbole in β. Man beachte, dass ∀xβ die Skolemform von $\forall x \exists y_1 \ldots \exists y_m \beta\,[f_i\,(x)\,/\,y_i]$ und dass diese Formel weiterhin relational ist.
Aus dem Skolemnormalformtheorem folgt, dass

$$\varphi := \alpha \wedge \forall x \exists y_1 \ldots \exists y_m \beta\,[f_i\,(x)\,/\,y_i]$$

Ist erfüllbar über dem gleichen Universum wie ψ' und somit auch ψ. Offensichtilich enthält φ höchstens n Prädikate. Der Beweis, dass das Modell eine Kardinalität von höchstens $2^{O(n)}$ hat, folgt aus 3.3.

□

⇒ Monadische Formeln haben die „endliches Modell" – Eigenschaft

⇒ SAT([*all*, (ω), (ω)]) ist entscheidbar.

4 Quellen

The Classical Decision Problem / Egon Boerger; Erich Grädel; yuri Gurevich
- Berlin; Heidelberg; New York; Barcelona; Budapest; Hong Kong; London; Milan; Paris; Santa clara; Singapore; Tokyo : Springer 1997

Logik für Informatiker / von Uwe Schöning – 5. Auflage,
- Heidelberg; Berlin: Spektrum Akad. Verl., 2000
(Spektrum Hochschultaschenbuch)