**Endlichkeitssatz:**

Eine Menge M von Formeln ist erfüllbar genau dann, wenn jede der endlichen Teilmengen von M erfüllbar ist.

Beweis: Es gibt höchsten 22^n verschiedene Formeln in Mn die paarweise zueinander nicht äquivalent sind

**Hornformel:**

Formel in KNF, jedes Disjunktionsglied hat höchsten ein positives Literal.

Umformungen:

(A) => (1 -> A)

(¬A) => (A -> 0)

(¬A¬B  C) => ((A  B) -> C)

(¬A  ¬B) => ((A B -> 0))

**Umformung in KNF und DNF:**

1. Ersetze jede Teilformel der Bauart

¬¬G durch G

¬(G∧H) durch (¬G∨¬H)

¬(G∨H) durch (¬G∧¬H)

2. Distributivgesetz:

(F∨(G∧H)) durch (F∨G)∧(F∨H)

* Formel in KNF

(F∧(G∨H)) durch (F∧G) ∨ (F∧H)

* Formel in DNF



**Markierungsalgorithmus**: Unerfüllbarkeit von Hornformeln

Stoppt spätestens nach n Schritten

**1.** Markiere alle atomaren Formeln A, falls in Form (1->A) vorliegt. Falls keine Formel dieser Bauart: F erfüllbar

**2.** Markiere alle B, falls Teilformeln der Form (A1A2…->B) vorkommen und A1,A2… schon markiert sind. Falls es Formeln der Form (A1A2…->0) und A1,A2 schon markiert sind, gib unerfüllbar aus. Falls keine Formel dieser Form, gib erfüllbar aus.

**3.** Gib erfüllbar aus, falls kein Abbruch bei 2.

-> Kleinste erfüllende Belegung gefunden



**Alternativ: Kanonische Umformung**

**DNF**: Jede Zeile mit Wahrheitswert 1 trägt zu einem Konjunktionsglied bei . Falls A in dieser Zeile 1 ist: A, sonst ¬A einsetzen.

**KNF**: Jede Zeile mit Wahrheitswert 0 trägt zu einem Disjunktionsglied bei . Falls A in dieser Zeile 0 ist: A sonst ¬A einsetzen.

n-lange Formel kann sich zu 2^n aufblähen

Das Erfüllbarkeitsproblem und das Gültigkeitsproblem der Prädikatenlogik ist unentscheidbar. Aus diesem Grund wendet man die Herbrand-Theorie an (da es Formeln gibt, deren Modelle nur unendliche Grundmenge besitzt)

Unerfüllbarkeits-/Gültigkeitsproblem der Prädikatenlogik ist semi-entscheidbar (E(F) mit Endlichkeitssatz)

**Prädikatenlogik**:

u,v,w,x,y,z stehen für Variablen

a,b,c stehen für Konstanten

f,g,h stehen für Funktionssymbole

P,Q,R stehen für Prädikatssymbole

Formel ohne freie Variablen heißt geschlossen/Aussage

Matrix: F\*: Quantoren werden gestrichen

**1. Bereinigte Form**: gebundene Umbenennung von Variablen , so dass keine frei und gebunden vorkommt und dass hinter jedem Quantor verschiedene Variablen stehen. (äquivalent)

(Falls vorhanden, freie Variablen binden / nur für Herbrand, Resolution)

**2. Pränexform**: Vorziehen aller Quantoren (äquivalent)

* Tipp: immer Vorziehen vor „gesamt“ F in einem Schritt!
* (Zuerst Existenzquantoren vorziehen danach Allquantoren, so dass alle vorgezogene Existenzquantoren am Ende ganz links stehen)

**3. Skolemform**  ( ) (erfüllbarkeitsäquivalent)

* Streichen von Existenzq. => Ersetzten immer in **ganz F**
* **Alle** Variablen von Existentquantoren(x) durch Konstanten ersetzten z.b [x/a]
* Stehen vor Existenzq. Variable (x) noch Allq. Variablen(z,w) dann [x/ f(z,w)]

**4. Klauselform** (Matrix F\* in KNF umwandeln/ nur für Resolution)

* Matrix F\*: Einfach Allquantorblock vor F streichen
* F\* in KNF umwandeln

**Nicht äquivalent:**

(∀xF∀xG)≠∀x(FG)

(∃xF∃xG)≠ ∃x(FG)

**Resolution**: Test auf Erfüllbarkeit

Formel muss in KNF vorliegen.

Resolutionshülle: Res\*(F) wird berechnet durch: Res0(F)=F ; Res1(F)=Res0(F) U { {},{}….}; Res3(F)=Res2(F) U Ø = Res\*(F)

F erfüllbar, wenn nicht Element Res\*(F)

F unerfüllbar , wenn Element Res\*(F)

Deduktion: Herleitung der leeren Klausel

G Folgerung von F: Prüfe ob F¬G unerfüllbar, wenn unerfüllbar dann G Folgerung von F, wenn nicht G keine Folgerung von F



**Sätze:**

- Sei F eine Aussage in Skolemform. Dann ist F genau dann erfüllbar, wenn F ein Herbrand-Modell besitzt.

- Jede erfüllbare Formel der Prädikatenlogik besitzt ein abzählbares Modell(also mit abzählbarer Grundmenge)

-Für jede Aussage in Skolemform gilt: F ist erfüllbar genau dann, wenn die Formelmenge E(F) erfüllbar ist. (Endlichkeitssatz)

**Herbrand-Theorie:**

Ausgangspunkt sind geschlossene Formeln

**Herbrand-Struktur:**

A=(UA,IA)

UA= D(F)={a,f(a),g(a,a),…}

IA: fA(a)=f(a)

fA(f(a))=f(F(a))

fA(g(a,a))=f(g(a,a))

Die Wahl von PA ist noch offen

**Prädikatenlogische Resolution:**

1. Es gibt gewissen Substitutionen s1 und s2, die Variablenumbennenungen sind, so dass K1S1 und K2S2 keine gemeinsamen Variablen enthalten

2. Es gibt einen allgemeinsten Unifikator sub, so dass ein Resolvent R gebildet werden kann.

Sei F eine Aussage in Skolemform mit der Matrix F\* in KNF. Dann gilt: F ist genau dann unerfüllbar, wenn e Res\*(F\*) und alle Klauseln entweder eine Grundinstanz oder ein Resolvent ist.

**Herbrand-Expansion: E(F)**

Enstheht indem die Terme in D(F) in jeder möglichen Weise für die Variablen in der Matrix von F substituiert werden

**Rechenhilfen:**

Kleiner Fermat: aP≡ a mod p

aP-1≡ 1 mod p /ggT(a,p)=1

Eulers Phi: aϕ(n)≡ 1 mod n

ggT(k.l) = ggT(-k,l)

**Diskrete Strukturen: Grundbegriffe**

*Halbgruppe*: Menge mit assoziativer Verknüpfung

*Monoid*: Halbgruppe mit neutralem Element

*Gruppe*: Monoid mit beidseitigem Inversen

*Ring*: additive Gruppe mit neutr. Element 0: (R,+,0) und zusätzlicher Operation “\*“,Distributivgesetze

*Körper*: Ring mit kommutativer Multiplikation, bei dem R\{0} eine Gruppe bezüglich der Multiplikation bildet

*Homomorphismus*: Strukturerhaltende Abbildung

**RSA-Verfahren:**

Verschlüsslungsverfahren mit öffentlichem Schlüssel

1. Wähle zwei Primzahlen p,q mit 3<p<q

2. Berechne n=p\*q und ϕ(n) = (p-1)\* (q-1)

3. Wähle e>1 mit ggT(e,ϕ(n))=1

4. Berechne s mit e\*s≡1modϕ(n)

5. Verschlüssel mit y= xe mod n

6. Entschlüssel mit x= ys mod n

**Eulers Phi-Funktion:**

Anzahl der Einheiten in Z/nZ 🡪 ϕ(n) = |(Z/nZ)\*|

Brechnung: ϕ(p)=p-1

ϕ(m\*n)=ϕ(m)\*ϕ(n)

ϕ(pk)=pk-1\*(p-1)

Sonst testen ob durch 2,3,5 teilbar, wenn nur durch eine Zahl testen ob Ergebnis Primzahl, wenn ja obige Formel für 2 Primzahlen, wenn nein dannϕ(n)= n\*(1-1/(2,3,5)). Wenn durch mehrere teilbar ϕ(n)=n\*(1-1/(2,3,5)\*(1-1/(2,3,5))…



**Fibonacci-Zahlen:**

Fn=fn-1+fn-2

Fn≤2n≤F2n

Goldener Schnitt: x1= Φ= (1+√5)/2

X2=Φ^=(1-√5)/2

Fn=[1/√5\*Φn ] auf die nächste ganze Zahl gerundet

Satz: ggT(Fm,Fn)=FggT(m,n)

**Partisionszahlen:**

Eine n-elementige Summe wird in k nichtleere Teilmengen partitioniert.

P(n,K)= Anzahl verschiedener Möglichkeiten, n so in k Summanden zu zerlegen so dass, (n1>n2…>1)

P(n)=∑P(n,k)

**Primzahldichte:**

n/log2n≤π(n)≤((2+e)\*n)/log2n)

Betrand`sches Postulat: Für alle n≥1 existiert eine Primzahl p mit n≤p≤2n

**Graphen 2:**

Planar: möglich Graphen so in die Ebene zu zeichnen, so dass sich Kanten nicht schneiden

Facette: Maximal Fläche in der Ebene, die keine Kanten und Knoten enthält

Eulerformel: n-m+f=2 🡪 nichtleere, zusammenhängende, planare Graphen

**Catalan-Zahlen:**

Cn= Anzahl der Binärbäume mit n Knoten

**Graphen:**

Einfach: ohne Schlingen und Mehrfachkanten

Orientiert: max. eine Kante zwischen zwei Knoten

Komplementär: enthält genau die Kanten die G nicht hat

Vollständig: Enthält alle möglichen Kanten: (n\*(n-1)/2)

∑xev dx= 2\*|E|

Eulerkreis: Kreis wenn jede Kante einmal besucht wird

* Alle Knoten müssen geraden Grad haben

Hamiltonkreis: Kreis wenn jeder Knoten einmal besucht wird