LUP

- REZOLUCE V LOGICE 1. ŘÁDU
- AUTOMATICKÉ DOKAZOVAČE
- PRINCIPY METOD STROJOVÉHO DOKAZOVÁNÍ V BOOLEOVSKÝCH DOMÉNÁCH A V PREDIKÁTOVÉ LOGICE
- HLEDÁNÍ MODELŮ V OBECNÝCH DOMÉNÁCH

- FORMAL LOGIC
  - STUDIES INFERENCES
  - GIVEN STATEMENT φ AND COLLECTION OF STATEMENTS Γ
    - DOES φ FOLLOW LOGICALLY FROM Γ
  - WE WANT OUR SYNTAX AND SEMANTHICS TO BE ADEQUATE
    - CORRECTNESS
      - ONLY VALID FORMULAS ARE DERIVABLE
    - COMPLETENESS
      - ALL VALID FORMULAS ARE DERIVABLE
  - LIMITS OF FORMAL METHODS
    - INCOMPLETENESS
      - IMPOSSIBLE TO DESCRIBE BASIC ARITHMETIC OF NATURAL NUMBERS BY A SET OF AXIOMS THA ARE ALGORITHMICALLY RECOGNIZABLE
    - UNDECIDABILITY
      - THERE IS NO DECISION PROCEDURE FOR VALIDITY IN FIRST-ORDER LOGIC

- PROPOSITIONAL LOGIC
  - ELEMENTARY PROPOSITIONS CALLED ATOMIC FORMULAE (ATOMS)
    - WE ASSIGN TRUTH VALUES TO THEM
  - WE COMBINE THEM USING BOOLEAN CONNECTIVES
  - SET OF PROPOSITIONAL FORMULAE IS THE SMALLEST SET SATISFYING
    - EVERY PROPOSITIONAL VARIABLE IS A FORMULA
    - IF φ IS FORMULA, THEN $(\neg\varphi)$ IS FORMULA
    - IF φ AND ψ ARE FORMULAE, THEN $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ AND $(\varphi \rightarrow \psi)$ ARE FORMULAE
  - SEMANTICS
    - VALUATION V IS ASSIGNMENT OF TRUTH VALUES TO PROPOSITIONAL VARIABLES
    - IF $V(\varphi) = 1$ THAN WE ALSO WRITE $V \models \varphi$
      - "FORMULA φ IS SATISFIED BY VALUATION V"
  - SEMANTIC CONSEQUENCE
    - FORMULA φ IS A CONSEQUENCE OF ψ IF ψ IS SATISFIED BY EVERY VALUATION V THAT SATISFIES ψ
    - $\psi \models \varphi$
    - REFLEXIVE AND TRANSITIVE
    - THANKS TO THIS WE CAN REPLACE SUBFORMULA BY EQUIVALENT FORMULA
    - $\varphi \models \varphi \vee \psi$
    - $\varphi \wedge \psi \models \varphi$
    - $\varphi \models \psi \rightarrow \varphi$
    - $\neg\varphi \models \varphi \rightarrow \psi$

- FORMULA φ FOLLOWS FROM A SET OF FORMULAE Γ, IF φ IS SATISFIED BY EVERY VALUATION v THAT SATISFIES ALL FORMULAE IN Γ

$$\Gamma \models \varphi \text{ IFF } \forall v \, (\text{IF } v \models \Gamma \text{ THEN } v \models \varphi)$$

- WE HAVE $\Gamma \cup \varphi \models \psi$ IFF $\Gamma \models \varphi \to \psi$
- $\varphi \models \psi$ IFF $\models \varphi \to \psi$

- SATISFIABLE FORMULA
  - THERE EXISTS v SUCH THAT $v(\varphi) = 1$, $v \models \varphi$
  - UPPERSET OF TAUTOLOGY
- TAUTOLOGY
  - EVERY v, $v(\varphi) = 1$, $\models \varphi$
  - $\top$
- CONTRADICTION
  - EVERY v, $v(\varphi) = 0$
  - $\bot$

- DECIDING SATISFIABILITY IS NP-HARD

- CLAUSE
  - DISJUNCTION OF FINITELY MANY LITERALS

- LITERAL
  - PROPOSITIONAL VARIABLE OR NEGATION
  - p
  - $\neg p$

- CONJUNCTIVE NORMAL FORM (CNF)
  - CONJUNCTION OF CLAUSES $(p_1 \vee p_2) \wedge (p_3 \vee p_4)$
- DISJUNCTIVE NORMAL FORM (DNF)
  - DISJUNCTION OF CONJUNCTIONS OF LITERALS $(p_1 \wedge p_2) \vee (p_3 \wedge p_4)$

- FOR EVERY FORMULA EXISTS FORMULA IN CNF AND DNF WHICH ARE EQUIVALENT

- DNF
  - EASY TO OBTAIN FRO TRUTH TABLES

p	q	$(p \to q) \wedge (q \to p)$
0	0	1
0	1	0
1	0	0
1	1	1

$\neg p \wedge \neg q$

$p \wedge q$

  - BUT CAN LEAD TO EXPONENTIAL INCREASE IN THE SIZE OF FORMULA

- NORMAL FORMS ARE NOT UNIQUE
  - FORMULAS CAN BE TRANSFORMED IN MANY WAYS
  - WE CAN USE TSEYTIN TRANSFORMATION
    - AVOIDS EXPONENTIAL BLOWUP
    - INTRODUCE NEW VARIABLES
      - THUS NOT EQUIVALENT
      - BUT ONLY EQUISATISFIABLE

- SAT PROBLEM
  - FORMULA IN CNF
  - DECIDE WHETHER FORMULA IS SATISFIABLE ($\varphi \stackrel{?}{\in} SAT$)
  - TRUTH TABLES ARE TOO COMPLICATED FOR BIGGER PROBLEMS
  - $\models \varphi$ IFF $\neg\varphi$ IS CONTRADICTION IFF $\neg\varphi \notin SAT$
  - $\Gamma \models \varphi$ IFF $\bigwedge \Gamma \wedge \neg\varphi$ IS CONTRADICTION IFF $\bigwedge \Gamma \wedge \neg\varphi \notin SAT$
  - EXAMPLE

    $p, p \to q, q \to r \models r$ IFF $p \wedge (p \to q) \wedge (q \to r) \wedge \neg r \notin SAT$

- RESOLUTION RULE

$$\frac{q \vee p \qquad \bar{p} \vee r}{q \vee r}$$

(INPUT CLAUSES; RESOLVENT)

- IF $v \models (q \vee p) \wedge (\bar{p} \vee r)$ THAN $v \models q \vee r$

- RESOLUTION CALCULUS
  - ONLY DEDUCTION RULE
    - RESOLUTION RULE
  - WE SAY THAT CLAUSE C IS PROVABLE FROM SET OF CLAUSES $\{C_1, \dots, C_n\}$ IF THERE IS PROOF OF C FROM $\{C_1, \dots, C_n\}$
    - $\{C_1, \dots, C_n\} \vdash C$
  - EXAMPLE

$$\{\{p\}, \{\bar{p}, q\}, \{\bar{q}, r\}, \{\bar{r}\}\}$$

$$\frac{\dfrac{\dfrac{\{p\} \qquad \{\bar{p}, q\}}{\{q\}} \qquad \{\bar{q}, r\}}{\{r\}} \qquad \{\bar{r}\}}{\square}$$

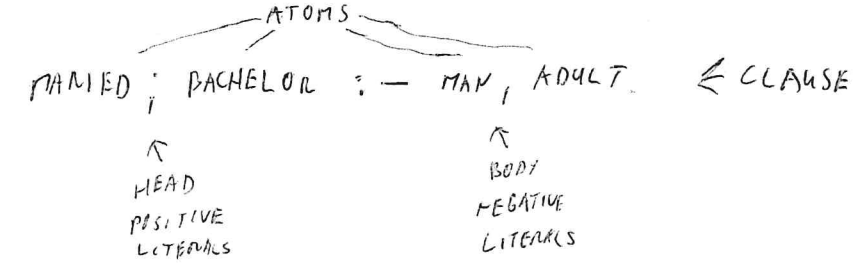
  - WE CAN'T DERIVE EVERY VALID FORMULA IN RESOLUTION CALCULUS
    - FROM EMPTY SET WE DON'T DERIVE ANYTHING
    - BUT IT IS REFUTATION COMPLETE
- IF φ (SET OF CLAUSES) IS UNSATISFIABLE, THEN $\varphi \vdash \square$
- IF $\varphi \vdash \square$ THEN φ IS UNSATISFIABLE
- TWO POSSIBILITIES
  - WE PRODUCE EMPTY CLAUSE, THEN $\varphi \notin SAT$
  - WE PRODUCE SATURATED SET OF CLAUSES, $\varphi \in SAT$
- THE ORDER HOW WE USE VARIABLES DOESN'T MATTER

- SUBSUMPTION
  - CLAUSE C_1 SUBSUMES CLAUSE C_2 IF $C_1 \leq C_2$
  - IF $C_1, C_2 \in \varphi$ AND $C_1 \leq C_2$, THEN $\varphi \in SAT$ IFF $\varphi \setminus C_2 \in SAT$

- MULTIPLE RESOLVENTS
  - IF IT IS POSSIBLE TO OBTAIN MORE DIFFERENT RESOLVENTS FROM TWO CLAUSES, THAN ALL THESE RESOLVENTS ARE TAUTOLOGIES, HENCE WE CAN IGNORE THEM

$$\frac{\{p, \bar{q}\} \quad \{\bar{p}, q\}}{\{q, \bar{q}\}} \qquad \frac{\{p, \bar{q}\} \quad \{\bar{p}, q\}}{\{p, \bar{p}\}}$$

- PROPOSITIONAL CLAUSAL LOGIC



- HERBRAND BASE
  - SET OF ATOMS
    { MARIED, BACHELOR, MAN, ADULT }

- HER-BRAND INTERPRETATION
  - SET OF TRUE ATOMS
    { MARIED, ADULT, MAN }

- CLAUSE IS FALSE IN INTERPRETATION IF ALL BODY LITERALS ARE TRUE, AND ALL HEAD LITERALS ARE FALSE
  BACHELOR :— MAN, ADULT
- AND TRUE OTHERWISE
  - INTERPRETATION IS MODEL OF THE CLAUSE

- PROPOSITIONAL RESOLUTION

  - SOUND
    - DERIVES ONLY LOGICAL CONSEQUENCES
  - INCOMPLETE
    - CANNOT DERIVE ARBITRARY TAUTOLOGIES
  - REFUTATION-COMPLETE
    - DERIVES EMPTY CLAUSE FROM ANY INCONSISTENT SET

- PROOF BY REFUTATION
  - ADD NEGATION OF ASSUMED LOGICAL CONSEQUENCE
  - PROVE INCONSISTENCY BY DERIVING EMPTY CLAUSE

- RELATIONAL CLAUSAL LOGIC

LIKES(PETER, S) :- STUDENT_OF(S, PETER). ← CLAUSE

(ATOMS)

(PETER: CONSTANT, S: VARIABLE) — TERMS

- SUBSTITUTION MAPS VARIABLE TO TERMS
- RESULTING CLAUSE IS INSTANCE OF ORIGINAL CLAUSE
- IT IS GROUND INSTANCE IF IT DOES NOT CONTAIN VARIABLES
- EACH INSTANCE OF CLAUSE IS AMONG ITS LOGICAL CONSEQUENCES
- HERBRAND UNIVERSE
  - SET OF GROUND TERMS (CONSTANTS)
    {PETER, MARIA}

——— HERBRAND BASE

- SET OF GROUND ATOMS
  - LIKES(PETER, PETER), LIKES(PETER, MARIA)...

- HERBRAND INTERPRETATION
  - SET OF TRUE GROUND ATOMS
    - LIKES(PETER, MARIA), STUDENT_OF(MARIA, PETER)

- INTERPRETATION I IS A MODEL FOR A CLAUSE IF IT MAKES ALL OF ITS GROUND INSTANCES TRUE

- FULL CLAUSAL LOGIC

LOVES (X, PERSON_LOVED_BY (X))

FUNCTOR, TERM

COMPLEX TERM

- HERBRAND UNIVERSE
  - SET OF GROUND TERMS

$\{0, s(0), s(s(0)) \ldots\}$

- HERBRAND BASE
  - SET OF GROUND ATOMS

$\{plus(0,0,0), plus(s(0),0,0) \ldots\}$

- HERBRAND INTERPRETATION
  - SET OF TRUE GROUND ATOMS

$\{plus(0,0,0), plus(s(0),0,s(0)), plus(0,s(0),s(0))\}$

- UNIFICATION
  - SUBSTITUTION
    - SUBSTITUTION MAPS VARIABLES TO TERMS
    - DENOTED BY σ, θ, η
  - UNIFIER
    - LET s AND t BY TERMS
    - UNIFIER OF s AND t IS A SUBSTITUTION σ, SUCH THAT $s\sigma$ AND $t\sigma$ ARE IDENTICAL $(s\sigma = t\sigma)$
  - MOST GENERAL UNIFIER
    - UNIFIER σ OF s AND t IS MGU IF FOR ANY UNIFIER θ OF s AND t THERE IS SUBSTITUTION η SUCH THAT $\theta = \sigma\eta$
    - θ IS COMPOSITION OF σ AND η

- UNIFICATION ALGORITHM

  - SOLVED FORM

    - SET OF EQUATIONS $\{ X_1 \doteq t_1, \dots, X_n \doteq t_n \}$

    - IF $X_1 \dots X_n$ ARE DISTINCT VARIABLES AND THEY DO NOT APPEAR IN TERMS $t_1, \dots, t_n$

  - GIVEN FINITE SET OF PAIRS OF TERMS $S = \{ s_1 \doteq t_1, \dots, s_n \doteq t_n \}$

  - ALGORITHM FINDS A SET OF EQUATIONS IN SOLVED FORM THAT DEFINES MGU σ OR IT FAILS

  - RULES

    - $S \cup \{ u \doteq u \} \rightsquigarrow S$

    - $S \cup \{ f(u_1, \dots, u_k) \doteq f(v_1, \dots v_k) \} \rightsquigarrow S \cup \{ u_1 \doteq v_1, \dots, u_k \doteq v_k \}$

    - $S \cup \{ f(u_1, \dots, u_k) \doteq g(v_1, \dots v_l) \} \rightsquigarrow$ FAIL IF $f \neq g$ OR $k \neq l$

    - $S \cup \{ f(u_1, \dots, u_k) \doteq X \} \rightsquigarrow S \cup \{ X \doteq f(u_1, \dots, u_k) \}$

    - $S \cup \{ X \doteq u \} \rightsquigarrow S\{X \mapsto u\} \cup \{ X \doteq u \}$ IF $X \notin u$ AND $X \in S$

    - $S \cup \{ X \doteq u \} \rightsquigarrow$ FAIL IF $X \in u$

  - ALGORITHM ALWAYS TERMINATES

  - FINDS MGU IF EXISTS

- FIRST ORDER LOGIC
  - ASSUMES THAT WORLD CONTAINS
    - OBJECTS
    - RELATIONS
    - FUNCTIONS
    - CONSTANTS
  - CONTAINS
    - FUNCTIONS
    - CONSTANTS
    - VARIABLES
    - PREDICATE SYMBOLS
    - BOOLEAN CONNECTIVES
    - QUANTIFIERS
  - TPTP
    - THOUSANDS OF PROBLEMS FOR THEOREM PROVERS
    - CONTEXT FREE GRAMMAR
      - VARIABLE ::= SYMBOL STARTING WITH UPPER CASE LETTER
      - FUNCTION_SYMBOL ::= SYMBOL STARTING WITH A LOWER CASE LETTER
      - TERM ::= VARIABLE | FUNCTION_SYMBOL (CONSTANT) | FUNCTION_SYMBOL (arity>0) '(' TERM$_1$ "," TERM$_2$ "," ... "," TERM$_n$
      - PREDICATE_SYMBOL ::= SYMBOL STARTING WITH A LOWER CASE LETTER
      - ATOMIC_FORMULA ::= PREDICATE_SYMBOL | PREDICATE_SYMBOL "(" TERM$_1$ "," ... "," TERM$_n$ ")"
      - FORMULA ::= ATOMIC FORMULA | "(" "~" (¬) FORMULA ")" | "(" FORMULA BINARY_BOOLEAN_CONN FORMULA ")" | "!" "[" VARIABLE "]" FORMULA (∀) | "?" "[" VARIABLE "]" FORMULA (∃)

- FORMULAE ARE TRUE WITH RESPECT TO MODEL AND INTERPRETATION
  - MODEL
    - CONTAINS OBJECTS AND RELATIONS BETWEEN THEM
  - INTERPRETATION
    - SPECIFIES REFERENTS FOR
      - CONSTAT SYMBOLS → OBJECTS
      - PREDICATE SYMBOLS → RELATIONS
      - FUNCTION SYMBOLS → FUNCTIONAL RELATIONS
- ATOMIC FORMULA $PREDICATE(TERM_1, \dots, TERM_n)$ IS TRUE IF OBJECT REFERED BY $TERM_1, \dots, TERM_n$ ARE IN RELATION SPECIFIED BY PREDICATE

- SUBSTITUTION
  - TOTAL MAPING $\sigma : V \to T$
  - FROM VARIABLES TO TERMS
  - NOTATION $\{x_1 \mapsto t_1, \dots, x_k \mapsto t_k\}$
    - MAPS x_i TO TERM t_i
    - EVERY OTHER VARIABLE MAPS TO ITSELF
    - x_i MUST BE PAIRWISE DISTINCT
  - RESULT $t\sigma$ APPLYING A SUBSTITUTION σ TO A TERM t IS CALLED AN INSTANCE OF TERM t
  - RENAMING SUBSTITUTION
    - IT IS PERMUTATION ON THE SET OF ALL VARIABLES

- RESOLUTION IN FOL
  - RESOLUTION RULE

$$\frac{\Delta \vee L \qquad \neg K \vee \Gamma}{\Delta\theta \vee \Gamma\theta}$$

    - Δ AND Γ ARE DISJUNCTIONS OF ARBITRARY MANY LITERALS
    - CLAUSES $\Delta \vee L$ AND $\neg K \vee \Gamma$ HAVE NO COMMON VARIABLES
      - OTHERWISE WE HAVE TO RENAME THEM
    - L AND K ARE ATOMIC FORMULAE
    - θ IS A MOST GENERAL UNIFIER OF L AND K

- FACTORIZATION RULE

$$\frac{\Delta \vee L \vee K}{\Delta\theta \vee L\theta}$$

  - Δ IS DISJUNCTION OF ARBITRARY MANY LITERALS
  - K AND L ARE LITERALS
  - θ IS MOST GENERAL UNIFIER OF L AND K

- SKOLEMIZATION
  - IN PRENEX NORMAL FORM WITH UNIVERSAL QUANTIFIERS ONLY
    - QUANTIFIERS FOLOWED BY REST
  - EVERY FOL FORMULA CAN BE CONVERTED INTO SKOLEM NORMAL FORM
    - IT IS NOT EQUIVALENT, BUT IT IS EQUISATISFIABLE

- TABLEAU METHODS

  - DEDUCTION METHOD FOR AUTOMATED THEOREM PROVING

  - TREE WHOSE NODES ARE LABELED BY FORMULAE

  - EXPANSION RULE TRANSFORMS SEMANTIC TABLEAU INTO ONE HAVING EQUIVALENT REPRESENTED FORMULA

  - ATEMPT TO BREAK COMPLEX FORMULAE INTO SMALLER ONES UNTIL COMPLEMENTARY PAIRS OF LITERALS ARE PRODUCED OR NO FUTHER EXPANSION IS POSSIBLE

- INPUT IS SET OF FIRST-ORDER FORMULAE

- GOAL IS TO FIND THE CONTRADICTION

- INITIAL TABLEAU IS ONLY ONE NODE CONTAINING CONJUNCTION OF ALL INPUT SET FORMULAE

- WE ITERATEVLY APPLY EXPANSION RULES

- CONJUNCTION

$$\wedge\ \frac{A \wedge B}{\begin{array}{c} A \\ B \end{array}}$$

$(a \vee \neg b) \wedge c \rightsquigarrow (a \vee \neg b) \wedge c \downarrow (a \vee \neg b) \downarrow c$

- DISJUNCTION

$$\vee\ \frac{A \vee B}{A \mid B}$$

$\neg P(a,b) \downarrow P(a,b) \vee \neg(P(a,a) \vee P(b,a)) \rightsquigarrow \neg P(a,b) \downarrow P(a,b) \vee \neg(P(a,a) \vee P(b,a)$

$P(a,b) \quad \neg(P(a,a) \vee P(b,a$

- NEGATION

  - NEGATED NORMAL FORM

    - NEGATION OPERATOR IS APPLIED TO PREDICATES ONLY

    - TRANSLATION INTO NNF IS USUALLY APPLIED BEFORE TABLEAU METHOD

    - IF WE DONT DO IT, WE HAVE TO INTRODUCE FOLLOWING RULES

$$\frac{\neg\neg A}{A} \qquad \frac{\neg(A \wedge B)}{\neg A \vee \neg B} \qquad \frac{\neg(A \vee B)}{\neg A \wedge \neg B} \qquad \frac{\neg(\forall x\, \varphi)}{\exists x \neg \varphi}$$

$$\frac{\neg\exists x\, \varphi}{\forall x \neg \varphi}$$

- UNIVERSAL QUANTIFICATION

$$\forall \frac{\forall x\, \varphi(x)}{\varphi(x')}$$

WHERE x' IS NEW FRESH VARIABLE THAT DOES NOT OCCUR ANY WHERE IN THE CURRENT TABLEAU

$\forall x\,(\neg t(a, x, c) \vee p(a) \vee p(x))$

↓

$\neg p(a)$

⇝

$\forall x\,(\neg t(a, x, c) \vee p(a) \vee p(x))$

↓

$\neg p(a)$

↓

$\neg t(a, y, c) \vee p(a) \vee p(y)$

- EXISTENTIAL QUANTIFICATION

$$\exists \frac{\exists x\, \sigma(x)}{\sigma(f(x_1, \ldots, x_m))}$$

WHERE f IS A NEW FUNCTION SYMBOL AND $x_1, \ldots, x_m$ ARE FREE VARIABLES IN FORMULA σ

- CLOSED BRANCH
  - IF THERE EXISTS TWO COMPLEMENTARY LITERALS L AND K ON SOME BRANCH B SUCH THAT THERE IS MGU θ OF L AND $\neg K$ THAT $L\theta \equiv \neg K\theta$
  - THAN APPLY θ ON ALL NODES OF TABLEAU AND LABEL BRANCH B AS CLOSED
  - CLOSED BRANCHES DON'T NEED FUTHER EXPANSION
  - TABLEAU IS CLOSED IF ALL BRANCHES ARE CLOSED
  - CLOSED TABLEAU IS WAY TO PROVE UNSATISFABILITY OF INPUT SET
  - ROOT OF TABLEAU IMPLIES EVERY NODE IN TABLEAU

- EXAMPLE

$q(c)$

$\downarrow$

$\neg p(c, d)$

$\downarrow$

$(\forall x_1 \neg q(x_1) \vee (\forall x_2\, r(x_1, x_2)))$

$\downarrow$

$\neg q(c) \vee (\forall x_3\, r(c, x_3))$

$(\forall x_3\, r(c, x_3))$ $\qquad$ $\neg q(c)$

$\downarrow$

$r(c, d)$

- LEAN TAP
  - ONE OF THE SHORTEST COMPLETE FIRST-ORDER PROVER
  - BASED ON TABLEAU METHOD
  - 5 CLAUSE PROLOG PROGRAM
  - INPUT IS CONJUNCTION OF SKOLEMIZED CLOSED FORMULAE IN NNF
  - CONJUNCTION, DISJUNCTION, NEGATION, ALL, PROLOG VARIABLES AND FUNCTION.
  - PROVE(⟨CONJUNCTION OF SKOLEMIZED FORMULAE IN NNF⟩, [], [], [], ⟨MAX NUMBER OF FREE VARIABLES IN TABLEAU⟩)

- MODEL FINDING METHODS
  - INTERPRETATION
    - I
    - NON-EMPTY SET OF ELEMENTS OF D_I
    - FOR EVERY FUNCTION SYMBOL f OF ARITY n WE DEFINE A TOTAL FUNCTION $f_I : D_I^n \to D_I$
    - FOR EVERY PREDICATE SYMBOL p OF ARITY n WE DEFINE RELATION $p_I \in D_I^n$
      - OR IT CAN BE SEEN AS FUNCTION $f_I : D_I^n \to \{TRUE, FA$
  - VARIABLE ASSIGNMENT
    - FOR INTERPRETATION I IS A MAPPING FROM VARIABLES TO ELEMENTS OF D_I
  - FOR GIVEN INTERPRETATION M AND VARIABLE ASSIGNMENT ξ WE CAN COMPUTE ALL FREE VARIABLES OF GIVEN FORMULA φ, THAN COMPUTE ALL VALUES OF SUB- AND TERMS t_M, COMPUTE VALUES OF PREDICATES AND FINALY COMPUTE THE TRUTH VALUE OF THE WHOLE FORMULA φ
    IF φ IS TRUE IT IS DENOTED AS $M, \xi \models \varphi$

- EVALUATION OF TRUTH VALUES

  - VARIABLES

    - EACH VARIABLE x EVALUATES TO $g(x)$

  - FUNCTIONS

    - GIVEN TERMS $t_1, \ldots, t_n$ THAT HAVE BEEN EVALUATED TO $v_1, \ldots v_n$ OF DOMAIN D_I

    - TERM $f(t_1, \ldots, t_n)$ EVALUATES TO $f(v_1, \ldots, v_n)$

  - ATOMIC FORMULAS

    - FORMULA $p(t_1 \ldots t_n)$

    - ASSOCIATED TRUE OR FALSE

    - DEPENDS OF WHETHER $p(v_1 \ldots v_n)$ HOLDS WHERE VALUES $v_1, \ldots, v_n$ ARE THE EVALUATION OF THE TERMS $t_1 \ldots t_n$

    - FORMULA $t_1 = t_2$ IS TRUE IF t_1 AND t_2 EVALUATES TO SAME OBJECT OF D_I

  - LOGICAL CONNECTIVES

    - $\wedge, \vee, \neg \ldots$

  - EXISTENTIONAL QUANTIFIER

    - TRUE IF THERE IS WAY TO CHOOSE VALUE

  - UNIVERSAL QUANTIFIER

    - TRUE IF EVERY POSSIBLE VALUE CAN BE SELECTED

- IF φ IS TRUE UNDER INTERPRETATION $\mathcal{M}$ AND ALL POSSIBLE VARIABLE ASSIGNMENTS
  - $\mathcal{M}$ SATISFIES φ
  - $\mathcal{M} \models \varphi$

- FIRST ORDER ~~MODEL~~ STRUCTURE THAT SATISFIES ALL FORMULAE IN GIVEN THEORY
  - MODEL OF THEORY

- LOGICALLY VALID FORMULA
  - TRUE IN EVERY INTERPRETATION
  - LIKE TAUTOLOGY IN PROPOSITIONAL LOGIC

- LOGICAL CONSEQUENCE
  - ψ IS L.C. OF Ψ IF EVERY INTERPRETATION THAT MAKES Ψ TRUE ALSO MAKES ψ TRUE

- LET $I \models \varphi$ WHERE I IS DEFINED ON SET D
  - LET D' BE A SET
  - π IS BIJECTION $D \leftrightarrow D'$
  - THAN WE CAN CONSTRUCT INTERPRETATION I' ON D' SUCH THAT
    - $(\forall x_1 \dots x_m \in D')\left(P_{I'}(x_1, \dots, x_m) = P_I(\pi^{-1}(x_1) \dots \pi^{-1}(x_m))\right)$
    - $(\forall x_1 \dots x_m \in D')\left(f_{I'}(x_1, \dots, x_n) = \pi(f_I(\pi^{-1}(x_1) \dots \pi^{-1}(x_m)))\right)$
  - NOW IT ALSO HOLDS $I' \models \varphi$
  - I AND I' ARE ISOMORPHIC IN φ
  - THE ONLY IMPORTANT PROPERTY OF D IS ITS CARDINALITY
    - NOT THE CONCRETE CONTENT

- WE CAN SEARCH MODELS BY DPLL ALGORITHM
  - BASICALLY DF SEARCH

- TRANSLATION TO SAT
  - EFFICIENT WAY HOW TO FIND MODELS
  - FOR EVERY PREDICATE SYMBOL p AND FOR EVERY ITS ARGUMENTS $d_1 \dots d_{ARITY(p)}$ WE INTRODUCE PROPOSITIONAL VARIABLE $p(d_1, \dots, d_{ARITY(p)})$
    - IT REPRESENTS $p(d_1 \dots d_{ARITY(p)}) = TRUE$
  - FOR EVERY FUNCTION SYMBOL f, FOR EVERY ITS ARGUMENTS $d_1, \dots, d_{ARITY(f)}$ WHERE $d_i \in D$ AND FOR EVERY RESULTING VALUE $d \in D$ WE INTRODUCE PROPOSITIONAL VARIABLE $f(d_1, \dots, d_{ARITY(f)}) = d$
    - IT REPRESENTS f APPLIED ON $d_1, \dots, d_{ARITY(f)}$ IS EQUAL TO d

- LITERAL IS SHALLOW WHEN IT IS IN ONE OF FOLLOWING FORMS
  - $p(x_1, \dots, x_m)$
  - ~~$\neg p(x)$~~
  - $\neg p(x_1, \dots, x_m)$
  - $f(x_1, \dots, x_m) = y$
  - $f(x_1, \dots, x_m) \neq y$
  - $x = y$

  - IF WE CAN TRANSLATE ALL CLAUSES AND ITS LITERALS TO SUCH FORM, THAN WE CAN USE SAT ENCODING AND FIND MODEL BY SAT SOLVER
  - SUCH TRANSLATION IS FLATTENING

- TRANSLATION OF FLATTENED CLAUSES TO SAT

  - FOR EVERY FLATTENED FIRST ORDER CLAUSE C

  - AND FOR EVERY ITS POSSIBLE INSTANTIATION DEFINED BY SUBSTITUTION $\sigma : FV(C) \to D$

  - WE GENERATE PROPOSITIONAL CLAUSE C_σ

  - FV GIVES ALL FREE VARIABLES OCCURING IN CLAUSE

  - ALL EQUALITIES $d_1 \simeq d_2$

    - PROPAGATE BY DELETION THE EQUALITY IF $d_1 \neq d_2$

    - OR BY DELETION THE WHOLE CLAUSE IF $d_1 \simeq d_2$

  - FOR EVERY FUNCTION SYMBOL f

  - FOR EVERY INSTANTIATION OF ITS ARGUMENTS $d_1, \dots d_{ARITY(f)}$

  - AND FOR EVERY $d, d' \in D$ SUCH THAT $d \neq d'$

  - WE GENERATE PROPOSITIONAL CLAUSE

    $$f(d_1, \dots, d_{ARITY(f)}) \neq d \vee f(d_1, \dots, d_{ARITY(f)}) \neq d'$$

    - EACH FUNCTION RETURNS FOR THE SAME RESULT AT MOST ONE RESULTING VALUE

  - FOR EVERY FUNCTION SYMBOL f

  - FOR EVERY INSTANTIATION OF ITS ARGUMENTS $d_1, \dots, d_{ARITY(f)}$

  - WE GENERATE PROPOSITIONAL CLAUSE

    $$f(d_1, \dots, d_{ARITY(f)}) \simeq 1 \vee \dots \vee f(d_1, \dots, d_{ARITY(f)}) \simeq SIZE\_OF(D)$$

    - f IS TOTAL, IT RETURNS AT LEAST ONE RESULTING VALUE FOR ANY INPUT

- CLAUSE FLATTENING
  - TWO CASES WHERE LITERAL NOT SHALLOW
    - ONE SUBTERM NOT VARIABLE IN IT AT LEAST
    - IT IS IN FORM $X \neq y$ WHERE X AND Y ARE VARIABLES

- C CONTAINS SUB TERM t, WHICH IS NOT VARIABLE
  - TRANSFORMATION

$$C[t] \longrightarrow x \neq t \vee C[x]$$

    - x IS FRESH VARIABLE
      - IF THERE IS MORE OCCURANCES OF t IN C, WE SUBSTITUTE ALL OF THEM BY X
      - TRANSFORMATION IS LOGICALY CORRECT, BECAUSE C IS SUBSTITUED BY

$$(\forall x)(x = t \Rightarrow C[x])$$

- CLAUSE E CONTAINS LITERAL $x \neq y$
  - E HAS FORM $C \vee x \neq y$
  - WE APPLY TRANSFORMATION

$$C[x_{|y}] \vee x \neq y \rightsquigarrow C[x, x]$$

- BY ITERATIVELY APPLICATION OF RULES WE OBTAIN CLAUSE CONTAINING ONLY SHALLOW LITERALS

- REDUCTION OF VARIABLES
  - INSTANCES TO BE GENERATED GROWS EXPONENTIALY TO NUMBER OF VARIABLES (S^λ, λ - NUMBER OF VARIABLES, S - IS IDI)
  - SPLITTING OF CLAUSES

$$p(x,y) \vee q(x,y) \longrightarrow (p(x,y) \vee r(x)) \wedge (\neg r(x) \vee q(x,z))$$

    - WE DECREASED NUMBER OF FREE VARIABLES BY 1 IN EACH CLAUSE

- FORMAL DEFINITION OF BINARY SPLIT
  - GIVEN $C[\mathbb{X}] \vee D[\mathbb{Y}]$
    - C AND D CONSTITUTE PROPER BINARY SPLIT IF
      - EXISTS AT LEAST ONE $X \in \mathbb{X}$ SUCH THAT $X \notin \mathbb{Y}$
      - AND EXISTS AT LEAST ONE $Y \in \mathbb{Y}$ SUCH THAT $Y \notin \mathbb{X}$
    - THE RESULTING CLAUSES ARE

$$r(\mathbb{X} \cap \mathbb{Y}) \vee C[\mathbb{X}] \wedge \neg r(\mathbb{X} \cap \mathbb{Y}) \vee D[\mathbb{Y}]$$

    WHERE r IS A FRESH SYMBOL

- SOMETIMES WE CAN INTRODUCE FRESH CONSTANTS AS NAMES OF TERMS
  - EXAMPLE $p(f(a,b), f(b,a))$ YIELDS CLAUSE: $a \neq x \vee f \neq y \vee f(x,y) \neq z \vee f(y,x) \neq$ $\vee p(z,w)$ WHICH CANNOT BE SPLIT
  - BUT WE CAN INTRODUCE t_1 AND t_2 : $t_1 = f(a,b) \wedge t_2 = f(b,a) \wedge p(t_1, t_2$

AFTER FLATTENING WE HAVE:

$$a \neq x \vee b \neq y \vee f(x,y) \neq z \vee t_1 = z$$
$$\wedge$$
$$a \neq x \vee b \neq y \vee f(y,x) \neq z \vee t_2 = z$$
$$\wedge$$
$$t_1 \neq x \vee t_2 \neq y \vee p(x,y)$$

- FORMALIZATION OF EQUALITY IN FIRST ORDER LOGIC

  - GIVEN ANY X AND Y, $X=Y$

    IF AND ONLY IF

    GIVEN ANY PREDICATE P, $P(X) \Leftrightarrow P(Y)$

- STANDARD METHOD TO ADD PROPERTIES OF EQUALITY AS AXIOMS TO INPUT PROBLEM

  1. REFLEXIVITY: $(\forall X)(X=X)$

  2. SYMMETRY: $(\forall X)(\forall Y)(X=Y \rightarrow Y=X)$

  3. TRANSITIVITY: $(\forall x)(\forall y)(\forall z)((x=y \wedge y=z) \rightarrow x=z)$

  4. CONGRUENCE:

     FOR EVERY FUNCTION SYMBOL IN PROBLEM INTRODUCE

     $$(\forall X_1 \dots X_m)(\forall Y_1 \dots Y_m)((X_1=Y_1 \wedge \dots \wedge X_m=Y_m) \rightarrow (f(X_1 \dots X_m)=f(Y_1 \dots Y_m))$$

     FOR EVERY PREDICATE SYMBOL IN PROBLEM INTRODUCE

     $$(\forall X_1 \dots X_m)(\forall Y_1 \dots Y_m)((X_1=Y_1 \dots X_m=Y_m) \rightarrow (P(X_1 \dots X_m) \rightarrow P(Y_1 \dots Y_m))$$

  - BUT THE COMPLEXITY GROWS FAST WITH NUMBER OF FUNCTORS AND PREDICATES

- PARAMODULATION

$$\frac{A \vee (s=t) \quad B[w]}{A\theta \vee B\theta[t\theta]}$$

  - θ IS MGU OF s AND w
  - $B\theta[t\theta]$ IS OBTAINED BY REPLACING A SINGLE OCCURRENCE OF $w\theta$ IN $B\theta$ BY $t\theta$
  - INFERRED CLAUSE IS BINARY PARAMODULANT

- REFLEXIVITY RESOLUTION RULE

$$\frac{A \vee \neg(s \approx t)}{A\theta}$$

- WHERE θ IS MGU OF s AND t

- SUBSUMPTION
  - C SUBSUMES D IFF
    - THERE IS SUBSTITUTION θ
    - SUCH THAT $C\theta \subseteq D$
    - WE DENOTE $C \sqsubseteq D$
  - IF $C \sqsubseteq D$ THEN $C \models D$
  - FOR SETS A AND B
    - $A \sqsubseteq B$ IF
      - FOR EACH CLAUSE $B \in B$ EXISTS $A \in A$ SUCH THAT $A \subseteq B$
  - EXAMPLES

$P(x) \sqsubseteq P(c)$

$P(x) \sqsubseteq P(x) \vee q(x,y)$

$P(x) \vee q(x) \not\sqsubseteq P(x) \vee q(z)$

- SUBSUMPTION IN RESOLUTION

  - IF WE HAVE RESOLUTION PROOF FOR SET B

  - AND HOLDS $A \sqsubseteq B$

  - THAN THERE EXISTS RESOLUTION PROOF OF SET A THAT IS NOT LONGER THAN PROOF OF SET B

  - IDEA OF PROOF

    - ALL CLAUSES A HAVE THE SAME (AT LEAST) POWER AS CLAUSES B

    - SO IT CAN'T BE HARDER

  - IF WE INFER TWO CLAUSES A AND B, AND $A \sqsubseteq B$, WE CAN KEEP ONLY A WITHOUT LOSS OF REFUTATION COMPLETENESS

- ANL LOOP

  - USED IN PROVERS

  - WE ASSUME THAT THE INPUT CONJECTURE HAVE TO BE PART OF THE RESULTING REFUTATION PROOF

  - GUARANTEES EXPLORATION OF ALL NEEDED COMBINATIONS OF CLAUSES FOR COMPLETE RESOLUTION

  - TRIES TO AVOID REDUNDANT INFERENCES AS MUCH A POSSIBLE

  - INDEPENDENT OF CHOOSEN CLAUSE SELECTION STRATEGY

SOS := INPUT CLAUSE "SET OF SUPPORTS" - WAITING TO BE USED FOR INFERENCE

USABLE := EMPTY SET

WHILE (SOS IS NOT EMPTY AND NO REFUTATION HAS BEEN FOUND)

{

1. LET GIVEN_CLAUSE BE THE "BEST" CLAUSE IN SOS;

2. MOVE GIVEN_CLAUSE FROM SOS TO USABLE;

3. INFER AND PROCESS NEW CLAUSES USING THE INFERENCE RULES IN EFFECT WHERE

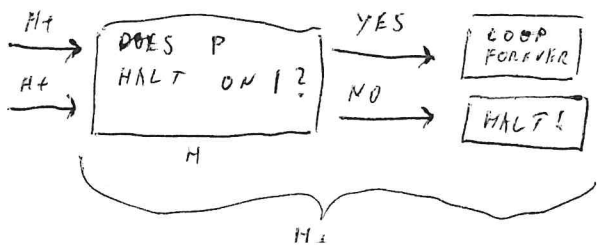
- EACH NEW CLAUSE MUST HAVE
  - THE GIVEN_CLAUSE AS ONE OF ITS PARENTS AND
  - MEMBERS OF USABLE AS ITS OTHER PARENTS;

4. NEW CLAUSES THAT PASS THE RETENTION TESTS ARE APPENDED TO SOS;

}

- SELECTION STRATEGIES
  - DFS, BFS, BEST-FS
- WE CAN USE SUBSUMPTION IN ANL LOOP

- LIMITS OF FORMAL METHODS
  - HALTING PROBLEM
    - DOES PROGRAM TERMINATES OR WILL IT RUN FOREVER FOR GIVEN INPUT
    - IT IS UNDECIDABLE OVER TURING MACHINES
    - PROOF BY CONTRADICTION
      - ASSUME SUCH PROGRAM H(P,I) EXISTS



- WE CONNECT H TO ITSELF
- IF IT HALTS, IT DOESN'T HALT
- IF IT DOESN'T HALT, IT HALTS
- CONTRADICTION ASSUMPTION IS NOT

- FIRST INCOMPLETE THEOREM
  - ANY CONSISTENT FORMAL SYSTEM F WHITHIN WHICH A CERTAIN AMOUNT OF ELEMENTAR ARITHMETIC CAN BE CARRIED OUT IS INCOMPLETE
    - THIS MEANS THAT THERE ARE STATEMENTS OF LANGUAGE F WHICH CAN NEITHER BE PROVED NOR DISPROVED IN F