15.09.05.

Hilbert proof system

$$\vdash_{ph} \underbrace{(\neg X \Rightarrow X)}_{\beta} \Rightarrow X$$

$$(\beta_1 \Rightarrow X) \Rightarrow \Big((\beta_2 \Rightarrow X)\Big) \Rightarrow (\beta \Rightarrow X).$$

1. $\big((\neg\neg X \Rightarrow X) \Rightarrow (X \Rightarrow X)\big) \Rightarrow \big((\neg X \Rightarrow X) \Rightarrow X)\big)$
2. $\neg\neg X \Rightarrow X.$
3. $(X \Rightarrow X) \Rightarrow ((\neg X \Rightarrow X) \Rightarrow X).$
4. $(X \Rightarrow X).$

$P \wedge Q$

<u>Defn</u> Given $X \in PROP$ a set $S \subset PROP$ is 'X-Hilbert inconsistent' if $S \vdash_{ph} X$.

~~S F~~ S is X-hilbert consistent if $S \nvdash_{ph} X$ (all sets from which X cannot be proved, no meaning with consistency

Let $\mathcal{C}_X$ be called X-hilbert con...

AX 3 $\perp \Rightarrow X$

AX 4 $X \Rightarrow T$

AX 5 $\neg\neg X \Rightarrow X$

:

AX 9 $(\beta_1 \Rightarrow X)$
$\Rightarrow ((\beta_2 \Rightarrow X) \Rightarrow (\beta...$

Lemma: $\mathcal{C}_X$ is a PCP.

Proof: Let $S \in \mathcal{C}_X$.

(a) $\perp \notin S$.

~~Ass~~ Assume to contrary.

$\perp \in S$, $S \vdash_{ph} X$.

① $\perp \Rightarrow X$ {AX 3}.

② $\perp$ {Premise}.

③ X (MP)

(b) $\{\beta\} \cup S \in \mathcal{C}_X$ then

$S \cup \{\beta_1, \beta\} \in \mathcal{C}_X$ or
$S \cup \{\beta_2, \beta\} \in \mathcal{C}_X$.
(By def.^{n} of PCP)

$S \cup \{\beta_1, \beta\} \notin \mathcal{C}_X$

Given
$S \cup \{\beta_1, \beta\} \vdash_{ph} X$

$S \cup \{\beta_2, \beta\} \vdash_{ph} X$

We show $S \cup \{\beta\} \vdash_{ph} X$

1) Ax 9 $\left(\left((\beta_1 \Rightarrow x) \Rightarrow (\beta_2 \Rightarrow x)\right) \Rightarrow (\beta \Rightarrow x)\right)$

$\therefore S \cup \{\beta_2, \beta_1\} \vdash_{ph} x.$

$\therefore S \cup \{\beta\} \vdash_{ph} \beta_1 \Rightarrow x$, by deduction thm.

2) $\beta_1 \Rightarrow x.$

3) $(\beta_2 \Rightarrow x) \Rightarrow (\beta \Rightarrow x)$

4) $\beta_2 \Rightarrow x$ (deduction thm)

5) $\beta \Rightarrow x.$

6) β

7) x (Completeness)

$\therefore$ Every x-hilbert consistent set is satisfiable. ($\forall \ddot{c}p$)

Strong hilbert ~~consistent~~ compleness.

If $S \models x$ then $S \vdash_{ph} x$.

a) If $S \nvdash_{ph} x$.

$\therefore S \in \mathcal{C}_x \quad \therefore S \cup \{\neg x\} \in \mathcal{C}_x.$

~~$\therefore S$ is satisfiable, by Model existance~~

Assume to contrary.

$\therefore S \cup \{\neg X\} \vdash_{Ph} X$.

iff.

$\therefore S \vdash_{ph} \neg X \Rightarrow X$

$\therefore (\neg X \Rightarrow X) \Rightarrow X$.

MP : $S \vdash X$.

(If $S \cup \{\neg X\}$ S is PCP, then is also PCP).

$S \cup \{\neg X\}$ is satisfiable by E_X is PCP $\Rightarrow$ Model existence.

$\therefore S \not\models X$. $\{\exists$ valuation for which S is true, X is false$\}$

<u>Gentzen's ~~Sequent~~ sequent Calculus</u>

A sequent is a pair ~~...~~ (Γ, Δ)

$\therefore$ Convention: we will use $\Gamma, \Delta \subseteq_{Fin} PROP$.

$\Gamma \rightarrow \Delta$

$\{A_1, \ldots, A_n\} \longrightarrow \{\beta_1, \ldots, \beta_n\}$

We will treat this as sets.

<u>Defn</u> $v \models \Gamma \longrightarrow \Delta$

if either $v \not\models X$ for some $X \in \Gamma$

or $v \models Y$ for some $Y \in \Delta$

if $\quad v \models A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow \beta_1 \vee \beta_2 \ldots \vee \beta_m$.

There is an implicit AND between elements of Γ,
an impicit OR between elements of Δ.

$\models \Gamma \longrightarrow \Delta$.

$\models X$ iff $\models \;\longrightarrow X$ iff $\models T \rightarrow X$

empty set.

Conjunction of set of empty set, always taken to be True.
Disjunction " " " " " " False

formula is equivalent to a sequent when there is nothing on L.H.S. (empty set).

Gentzen's Sequent Calculus.

Axioms $\quad X \to X$

$\bot \to$

Language Syntax X. $\hat{v}(x)$.

Semantics $v \models X$

$S \models X$.

$S \models X$ logical consequence.

Functional Completeness, normal forms

Axiomatization (proof system)

$S \vdash_{pr} X$.

Soundness & Completeness Model Existence

Decision procedure

$S \overset{?}{\models} X$ algorithmically find S.

$\vdash \longrightarrow \Delta$

$v \models \Gamma \longrightarrow \Delta$

$\overset{?}{\models} \Gamma \longrightarrow \Delta$

$A_1 \cdots A_n \rightarrow B_1 \cdots B_n$

[empty set on R.H.S. is equivalent to empty set on L.H.S. is equivalent to

Axiom

ⓐ $X \longrightarrow X$

ⓑ $\perp \longrightarrow$

ⓒ $\longrightarrow T$

Rules

Thinning — If $\Gamma_1 \subseteq \Gamma_2$ and $\Delta_1 \subseteq \Delta_2$ then if $\Gamma_1 \rightarrow \Delta_1$, $\Gamma_2 \rightarrow \Delta_2$

Strengthened the antecidant & weaken the conclusion.

Thinning
$$A_1 \wedge \cdots \wedge A_n \Rightarrow B_1 \vee \cdots \vee B_m$$
$$A \wedge A_1 \wedge \cdots \wedge A_n \wedge A_{n+1} \Rightarrow B_1 \vee \cdots \vee B_m \vee B_{m+1}$$

$\perp \rightarrow$

Negation Rules

$$\frac{\Gamma \rightarrow \Delta, X}{\Gamma, \neg X \rightarrow \Delta} \qquad \frac{\Gamma, X \rightarrow \Delta}{\Gamma \rightarrow \Delta, \neg X}$$

Conjunction
$$\frac{\Gamma, X, Y \rightarrow \Delta}{\Gamma, X \wedge Y \rightarrow \Delta}$$

$\models \Gamma \rightarrow \Delta, X \wedge Y$ (Soundness proof)

$\models (\Gamma \rightarrow \Delta, X)$ and $(\Gamma \rightarrow \Delta, Y)$

Disjunction

$$\frac{(\Gamma, X \to \Delta) \;\&\; (\Gamma, Y \to \Delta)}{\Gamma, X \vee Y \to \Delta}$$

$$\left.\begin{array}{l} \Gamma \to \Delta, X, Y \\ \Gamma \to \Delta, X \vee Y \end{array}\right\} \text{Checking Soundness}$$

$$\frac{\dfrac{\Gamma, X \Rightarrow Y \to \Delta}{\Gamma, \neg X \to \Delta, \quad \Gamma, Y \to \Delta}}{\Gamma, X \to \Delta, X}$$

$$\Gamma, X \to \Delta, Y$$

Rule R

$$\frac{\Gamma_1 \to \Delta_1, \; \Gamma_2 \to \Delta_2, \; \dots, \; \Gamma_n \to \Delta_n}{\Gamma \to \Delta}$$

R is sound iff

$\models \Gamma_1 \to \Delta_1$ ... and $\models \Gamma_n \to \Delta_n$.

$\Rightarrow \;\; \models \Gamma \to \Delta$

Sequent Proof Tree

(Basically tree ~~a~~ sequent ~~as~~ as label, root ~~of~~ under all ~~...~~ no

Seq : Proof of X is true

$\longrightarrow X$

Example

thinning

(7.1) $P \rightarrow P$ (7.2) $Q \rightarrow Q$.

(8.1) $P \rightarrow P, \neg Q$ (6.2) $Q \rightarrow Q, \neg P$.

(5.1) $\rightarrow P, \neg P, \neg Q$ (5.2) $\rightarrow Q, \neg P, \neg Q$.

(4) $\rightarrow P \wedge Q, \neg P, \neg Q$

(3) $\rightarrow P \wedge Q, \neg P \vee \neg Q$

(2) $\neg(P \wedge Q) \rightarrow (\neg P \vee \neg Q)$

(1) $\longrightarrow \neg(P \wedge Q) \Rightarrow (\neg P \vee \neg Q)$.

Write down the soundness ~~&~~ / completeness of sequent proof

Tableaux

Propositional Logic.

Proof Systems

Davis - Putnam Logemann & Loveland (DPLL)

www.satlive.org

formula X in CNF

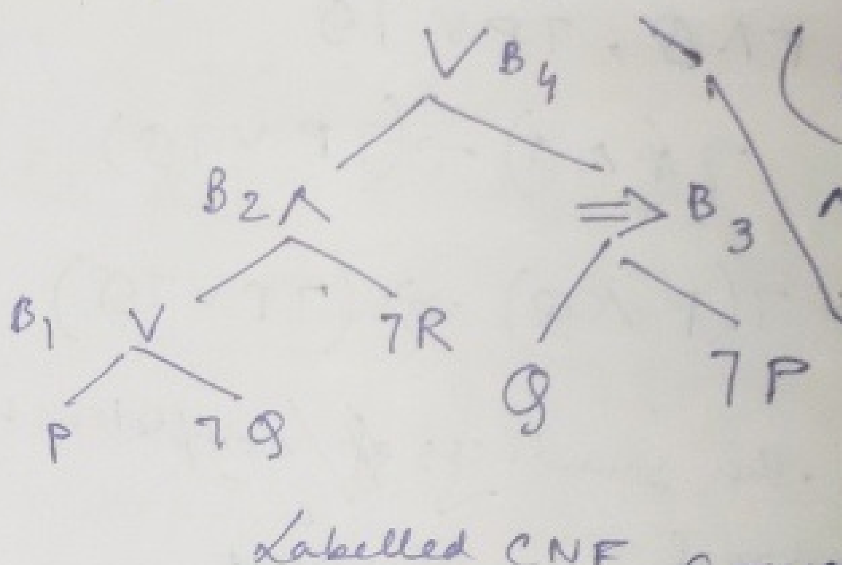
$$\bigwedge_{j=1}^{n}\left(\bigvee_{k=1}^{m_j} L_{jk}\right)$$

$L_{jk} = P \mid \neg P$.

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

Zhang & Mallik.

"The quest for efficient satisfiability solvers"



$(B_1 \Leftrightarrow (P \vee \neg Q))$
$\wedge (B_2 \Leftrightarrow B_1 \wedge \neg R)$
$\wedge (B_3 \Leftrightarrow Q \Rightarrow \neg P)$
$\wedge (B_2 \Leftrightarrow (B_2 \vee B_3$
$\wedge\ B_4$

Labelled CNF conversion

$\mu = \{P, \neg Q, \neg R\}$

Partial Assignment → few literals will be assigned.

$\mu_{\text{Partial}} = \{P, \neg Q\}$

- Function DPLL (ϕ, μ)

if $\phi = T$
then return true (μ)

if $\phi = \neg\bot$
then return false

if {a unit clause occurs in ϕ}
then return
DPLL(assign(l, ϕ), $\mu \cup \{l\}$).
(boolean constraint propagation)

- $\mu = \{\ \}$

$a \wedge (\neg a \vee \neg b \vee \neg c)$
$\wedge (b \vee \neg c)$
$\wedge (a \vee \neg b)$.

$$\boxed{\begin{array}{c} \mu = \{a\} \\ \hline (\neg b \vee \neg c) \wedge (b \vee \neg c) \end{array}}$$

if {a literal l occurs purely in ϕ}
then DLL(assign(l, ϕ), $\mu \cup \{l\}$) [doing this also satisfiability is undisturbed

$\mu = \{a, \neg c\}$ T

[heuristics

else

$p := \text{Choose-literal}(\phi)$.

return

DPLL(assign(l, ϕ), $\mu \cup \{l\}$)

or DPLL(assign$(\neg l, \phi)$, $\mu \cup \{\neg l\}$).

(1) $\mu = \{\}$ $\phi = (a \vee \neg b \vee c) \wedge (\neg a \vee b \vee d)$

$\wedge (a \vee b \vee \neg d) \wedge (\neg a \vee \neg d \vee \neg d)$

(2). $\mu = \{c\}$

$(\neg a \vee b \vee d) \wedge (a \vee b \vee \neg d)$

$\wedge (\neg a \vee \neg d \vee \neg d)$.

(3) $\mu = \{c, b\}$.

$\neg a \vee \neg d \neg d$.

(4) $\mu = \{c, b, \neg a\}$.

T

~~ZChaff~~

ZChaff

First Order Logic

ZFC set theory & First Order Logic

$(\forall x.(\exists y. x < y+1))$

AL = $\top, \bot, \forall, \exists, (,)$

VAR of variables. countable set

$v, v_1, v_2, w,$

Logical Connectives

$\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow, \uparrow, \downarrow$

Signature

(F, RR, C) countable

$\{-^1, -^2, +^2, *^2\} \rightarrow$ arity

$R = \{<, \text{even}\}$

$L(F, RR, C)$

the set of first order formula over sign SS.

Let $F \in F$, $R \in RR$, $c \in C$

$t \in TERM ::= v \mid c \mid F^n(t_1, \ldots, t_n)$

TERM is the smallest set has.

(a) If $v \in VAR$ then $v \in TERM$

(b)

(c) If $F \in F$ and has arity n and $t_1, \ldots, t_n \in TERM$ the $F(t_1, \ldots, t_n) \in TERM$

$atF \in ATF ::= \perp \mid \top \mid R(t_1, \ldots, t_n)$

where $R \in RR$ atomic formula

TERMS:

$+(v, 0)$

$v + 0$

$((1 \times v) + 0)$

$+(\times(1, v), 0)$

Formula (ATF)

$<(v+0, 1 * (1+1))$

$v + 0 < 1 * (1+1)$

$A, B \in FORM ::= atF \mid \neg A \mid A \circ B \mid$

$$(\forall x)(\underbrace{x < (0 + (1 * (1 + y)))}_{A} \wedge \underbrace{\top}_{B})$$

$\forall x . A \quad | \quad (\exists x . A)$

defn of a formula

$\exists z \exists y \forall x . (x < (0 + (1 * (1 + y))) \wedge \top)$

$Fv(A)$

$Fv(\bot) = \{\}$ $\qquad$ $Fv(\top) = \{\ \}$

$Fv(R(t_1, \ldots, t_n)) = var(t_1) \cup \ldots \cup var(t_n)$

$F(\neg A) = Fv(A)$

$Fv(A \circ B) = \cancel{A}\, Fv(A) \cup Fv(B)$

$Fv(\forall x . A) = Fv(A) - \{x\}$

$Fv : FORM \longrightarrow 2^{VAR}$

$Fv(\exists x . A) = Fv(A) - \{x\}$

$(\cancel{\forall x})\ \exists y - x + 1 < y$

$Fv(\exists y - x + 1 < y)$

$= Fv(x + 1 < y) - \{y\}$

$= \{x, y\} - \{y\} = \{x\}$

$(\forall x \,.\, x < y) \wedge (\exists y)(x+1) > z$

Rectified formula

$\forall x \, (x + y)$

A s.t. $F_v(A) = \{\}$ is called a sentence

Substitutions

Defn Substitute $\sigma : V \to TERM$

Ground Term

Define $t\sigma$

$\hat{\sigma}(t)$

$\hat{\sigma} : TERM \longrightarrow TERM$

$t\sigma \quad \hat{\sigma}(t)$

Inductive

$c\sigma = c$

$v\sigma = \sigma(v)$

$F(t_1, \ldots, t_n)\sigma$

$= F(t_1\sigma, t_2\sigma, \ldots, t_n\sigma)$

$q \vee | F(t_1, \dots, t_n)$

$x\sigma = F(x, y)$ $\qquad y\sigma = h(a)$.

$z\sigma = g(c, h(x))$ | Then $d(K(x), y)\sigma =$

$d(K(F(x,y)), h(a))$

~~$d(K(F(x,y)), h(a))$~~

Def^n σ, τ are substitutions.

then their composition $\sigma\tau$ is given by

$x(\sigma\tau) = (x\sigma)\tau$.

Proposition $(\sigma_1 \sigma_2)\sigma_3 = \sigma_1(\sigma_2 \sigma_3)$

support of σ is set of x

s.t. $x\sigma \neq x$.

Substitution with Finite support.

$\{x_1/t_1, x_2/t_2, \dots, x_n/t_n\}$

Proposition

$\sigma_1 = \{x_1/t_1, \dots, x_n/t_n\}$.

$\sigma_2 = \{y_1/u_1, \dots, y_k/u_k\}$.

Then $\sigma_1 \sigma_2 =$

Defn

Given σ let σ_x be s.t. $x\sigma_x = x$

$y\sigma_x = y\sigma$ if $y \neq x$

Substn ~~Format~~ Formula

Let $\sigma = \{x/a, y/b\}$.

$\forall x \, (R(x, y) \Rightarrow R(x, y))\,\sigma$

every free occurence is substitued, bound variables are not substituted.

$A\sigma$

(a) $\bot\sigma = \bot$, $\top\sigma = \top$

(b) $R(t_1, t_2, \ldots, t_n)\,\sigma$

$= R(t_1\sigma, t_2\sigma, \ldots, t_n\sigma)$.

(c) $(\neg A)\sigma = \neg(A\sigma)$

(d) $(A \circ B)\sigma = (A\sigma \circ B\sigma)$

(e) $(\forall x . A)\sigma = (\forall x)(A\sigma_x)$.

$(\forall x)(R(x,y) \Rightarrow R(x,y))$

$\{y \mid F(x)\}$

$(\forall x)\left(R(x, F(x)) \Rightarrow R(x, F(x)) \right)$

variable capture

Theorem If σ is free for $\cancel{X}$ and τ is free for $(X\sigma)$ then $(X\sigma)\tau = X(\sigma\tau)$

$(\forall x)(x < y+1)$

Mathematical Structure

$MM = (D, F^{MM}, RR^{MM}, C^{Mi})$

↑
domain

$(N, +^2, \bar{<}^2, 0, 1)$! $(\mathbb{N}, +^{N}, <^{N}, 0^{N}, 1^{N})$

$+^{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$S = (+^S, <^S, 0^S, 1^S)$

~~$(\forall x)\ \exists y$~~

$\forall x . \exists y . x <^{s} (y +^{s} 1^{s})$.

t
$|$
F

$(BOOL, V, <^{B}, F, t)$

$F < t$

$(BOOL, V, <^{B}, F, t)$

$S = (+^{s}, <^{s}, 0^{s}, 1^{s})$.

unique homomorphic extension theorem

$sig = (F, RR, c)$.

Structure u over sig.

$(|u|, F^{u}, R^{u}, C^{u})$

Model M $= (D, I)$

D non-empty set called domain

I is a mapping interpretation

For every $c \in C$

$c^{I} \in D$

for every n-ary $F \in F$

$F^{I} : D^{n} \to D$

for every $R \in RR$

$R^I \subseteq D^n$

Assignment A

$A : V \to D$

Given this

Let $M = (D, I)$ be model of $L(F, RR, C)$ and let A be an assignment.

We define

(a) Value of a term $t \in TERM$

(b) Value of a term $t^{M,A}$

$Eval\ term_{M,A}(TERM \longrightarrow D)$

$Eval\ term_{M,A}(t)$

By induction on structure of this

$c^{M,A} = c^I$

$v^{M,A} = A(v)$

$F(t_1, \ldots, t_n) = F^I(t_1^{M,A}, \ldots, t_n^{M,A})$

(4) Truth value of $\Phi \in FORM$

$\Phi^{M,A} \in \{tt, FF\}$.

By structural Induction

$\forall x \quad y < x + 1$.

PB (presburger arithmetic). $A(y) = 0$

(a) $\top^{M,A} = tt$.

(b) $F^{M,A} = FF$

(c) $R(t_1, \dots, t_n)^{M,A} = (t_1^{M,A}, \dots, t_n^{M,A}) \in R^I$.

(d). $\neg\phi^{M,A} = Not(\phi^{M,A})$.

$(\varphi \cdot \psi)^{M.A}$

(e) $(\forall x . \phi)^{M,A} = tt$

iff $\forall$ x-variant B of A

$\phi^{M,B} = tt$. (Tarskey semantics)

$A: V \rightarrow D$

and $B : V \rightarrow D$.

Call B as x-variant of A, provided

$A(y) = B(y)$ if $y \neq x$ $\forall y \in V$