

$N, P, R, a, b, f$   
+ enu dhynd limit  $\leq \frac{f}{1}$

$P(x), P(a), P(b)$

$R(x, y), R(x, x), R(a, x), R(x, a)$

$R(b, x), R(x, b), R(a, a), R(b, b)$

$R(a, b), R(b, a)$

$\neg R(x, y) \cup \neg R(y, x) \cup R(x, x)$

$\neg R(x, y) \cup \neg R(y, z) \cup R(x, z)$

$\neg R(x, x) \cup \neg R(x, z) \cup R(x, z)$

3v9w

Introduces  $M, K$   
 $enc(k, m)$   $dec(k, m)$

$\rightarrow M(enc(x, y)) \rightarrow K(x) \cup K(y)$

$\rightarrow K(x) \cup K(y) \cup K(\underline{enc(x, y)})$

$enc(y, enc(x, z)) \approx enc(x, enc(y, z))$   
 $\uparrow$

Restricted number of variables in chains!

$$\neg R(x, y) \vee \neg R(y, z) \vee R(x, z)$$

$$N \cup \left\{ \underbrace{\neg R(x, y)}_{\text{in}} \vee \underbrace{\neg R(y, z)}_{\text{sat}} \vee R(x', z') \right\}$$

$$N \cup \left\{ \underbrace{\neg R(x, y)}_{\text{ov}} \vee \underbrace{\neg R(y, z)}_{\text{if}} \right\} \text{ sat}$$

$$N \cup \left\{ R(x', z') \right\} \text{ sat}$$

Split

Sup v d e t e r i c f o r S L M T I

(i)  $\neg S(t) \vee C \vee B$   $t$  not var

select  $\neg S(t)$

(iv)  $\neg S(x) \vee T(x)$   
select  $\neg S(x)$

(ii)  $\neg S(x) \vee C \vee B$   $x$  not in  $B$   
select  $\neg S(x)$  and in  $M$  (i)

(iii)  $\neg S_1(x_1) \vee \neg S_2(x_2) \vee \dots \vee T(f(x_1, x_2, \dots))$

then  $T(f(x_1, \dots, x_n))$  is max

(i) + (iii) unita is a model  $\{x_i \rightarrow t_i\}$   $\text{depth}(f) > \text{depth}(t_i)$

$\neg S_1(t_1) \vee \neg S_2(t_2) \vee \dots \vee C \vee B$

(i) + (iii)  $\{x \rightarrow f(x_1, \dots, x_n)\} \neg S_1(x_1) \vee \dots \vee C \vee B$

$\Box \perp$

$\Diamond \perp$

LTL  
Linear  
Temporal  
Logic

System

$\Box \rightarrow \Box$   
 $P \rightarrow Q$

Semantics

$\Box \rightarrow \Box \rightarrow \Box$

R

$\Box$

Possible World  
Semantics

$\Box \perp$

$\perp$  holds everywhere

$\Diamond$

$\perp$  holds somewhere in future

$\Box \perp \rightarrow \Diamond \perp$

GIF

$\forall x. (\Box P \rightarrow P(x))$

$\exists x. (R(y,x) \wedge P(x))$