Predicate abstraction

$p : \text{State} \longrightarrow \{T, F\}$

$p \subseteq \text{States}$

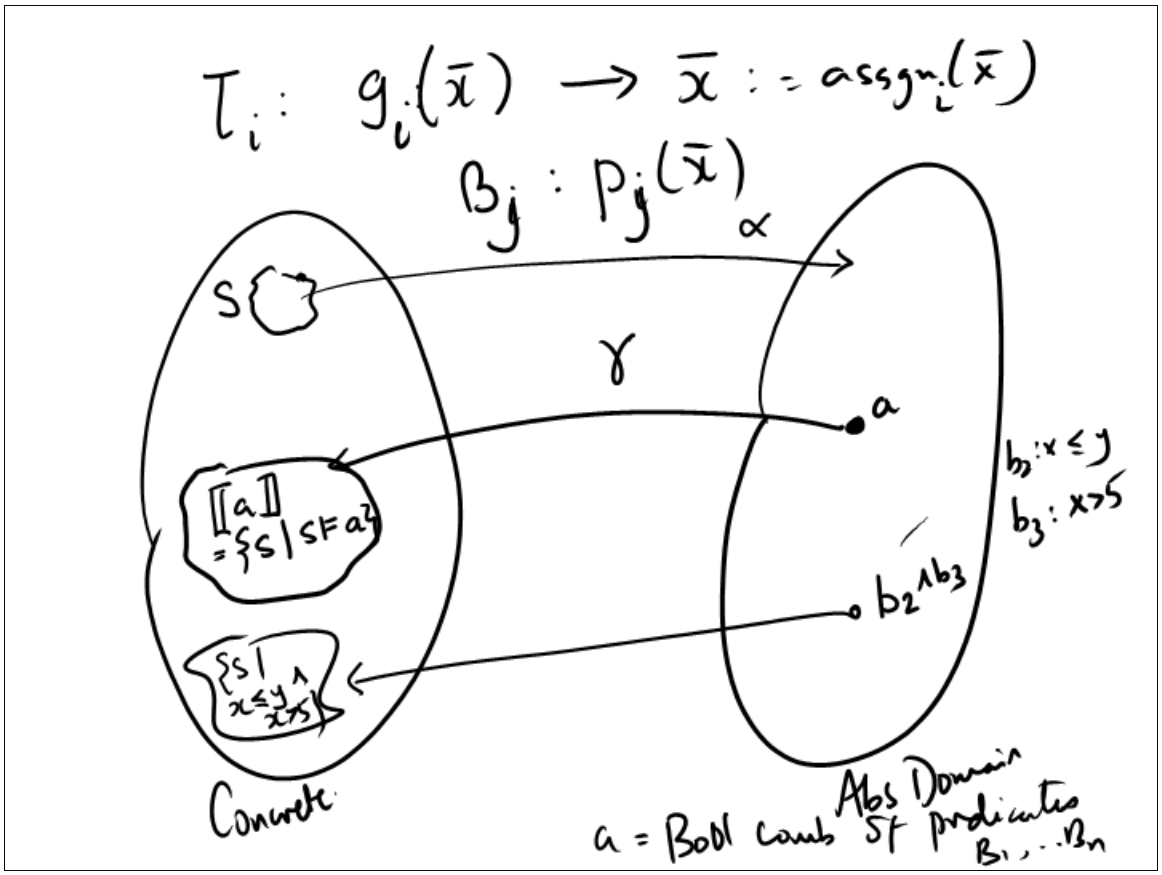
$x \leq 5 \wedge (y > 2 \vee z = 0)$

$p \wedge q$ is unsat

Floyd-Hoare style proof

$\leftarrow$ Logical statement

$p_1 \wedge (p_2 \vee p_3)$


$T_i : g_i(\bar{x}) \rightarrow \bar{x} := assgn_i(\bar{x})$
$B_j : p_j(\bar{x})$
α
γ
s
a
$[\![a]\!] = \{s \mid s \models a\}$
$\{s \mid x \leq y \wedge x > 5\}$
$b_2 \wedge b_3$
$b_2 : x \leq y$
$b_3 : x > 5$
Concrete
Abs Domain
a = Bool comb of predicates $B_1, \ldots B_n$

$P_1 : x \le y$

$P_2 : x > 5$

$P_1 \underline{\underline{\vee}} P_2$

$\neg P_2 \Rightarrow P_1$

(2,3)

(1,9) (7,2)

$P_1 : x$

$P_2 : x$

$P_1 \vee P_2 : \checkmark$

$P_1 \wedge P_2 \quad x$

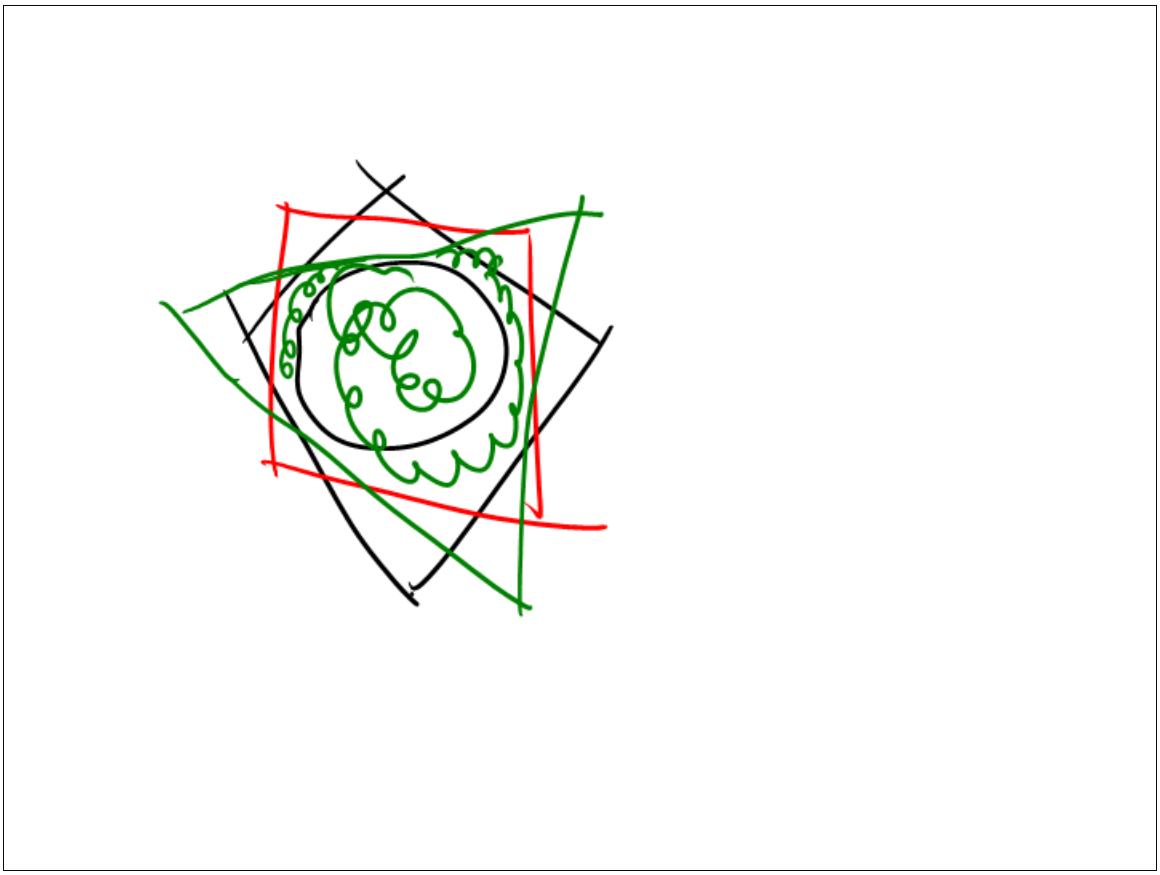
$\vdots$

$\cancel{2^{2n}}$

$2^{O(n)}$

2^{2}

$\bigwedge_{\substack{b \in \{0,1\} \\ f(b_1,\dots,b_k) \text{ walsh in } S}} f(b_1,\dots,b_k)$



$$\gamma\left(\exp(B_1, \ldots B_n)\right) = \left\{ s \mid s \text{ satisfies } \exp\left(B_1/P_1 \ldots B_n/P_n\right) \right\}$$

$$\alpha(S) = \bigwedge \left\{ \exp(B_1, \ldots B_n) \;\middle|\; \forall s \in S,\ s \text{ satisfies } \exp\left(B_1/P_1 \ldots B_n/P_n\right) \right\}$$

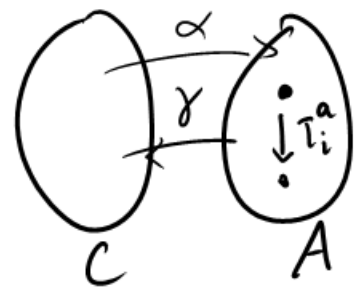
Cartesian abstraction

$$\alpha'(S) = \bigwedge_{i=1}^{n} \{ B_i \mid S \models P_i \} \wedge \bigwedge_{i=1}^{n} \{ \neg B_i \mid S \models \neg P_i \}$$

Monomials : $\eta_1 \wedge \eta_2 \ldots \wedge \eta_n$ where $\eta_i = B_j$ or $\neg B_j$

$T_i : g_i(\bar{x}) \longrightarrow assgn_i(\bar{x})$

if $(x>5)$ then $\{y := x$
$x := x+1\}$
else halt.



monomials over $\{B_1 .. B_n\}$

$b_1 : P_1 : x > 4$

$b_2 : P_2 = y = x$

$$T_i^a(\exp(B_1 .. B_n)) = \begin{cases} \text{false} & \text{if } \exp[B_i/\varphi_i] \Rightarrow \neg g_i \\ \bigwedge_{j=1}^{n} \begin{cases} B_j : post[T_i](\exp(B_i/\varphi_i)) \Rightarrow P_j \\ \neg B_j : post[T_i](\exp(B_i/\varphi_i)) \Rightarrow \neg P_j \\ \text{true} : \text{o/w} \end{cases} \end{cases}$$

T_i : true $\rightarrow x = x+1$

$T_i^a(b_1 \wedge \neg b_2)$
$= b_1$

$post[x := x+1](x > 4 \wedge \neg(y = x))$
$= b_1$

$\equiv \exists x', y' : (x' > 4 \wedge y' \neq x' \wedge x = x'+1 \wedge y' = y)$