KLEENE ALGEBRA WITH TESTS

LECTURE 3

YESTERDAY: KA(T)

TODAY: ↳ SEMANTICS

↳ EXAMPLES

- NETKAT (SYNTAX + EXAMPLES)

KA:

- DENOTATIONAL SEMANTICS WITH REGULAR LANGUAGES
  - ALLOWS REASONING SYNTACTICALLY
- OPERATIONAL SEMANTICS WITH DFAs
  - ALLOWS REASONING MECHANICALLY

KAT SYNTAX:

PROGRAM:

$$e ::= 0 \mid 1 \mid p \in P \mid e + e \mid e ; e \mid e^* \mid \underbrace{b \in B}_{\text{"assert } b\text{"}}$$

BOOLEAN:

$$b ::= \underbrace{t \in T}_{\text{BASIC TESTS}} \mid 0 \mid 1 \mid \underbrace{b \vee b}_{(+)} \mid \underbrace{b \wedge b}_{(;)} \mid \overline{b}$$

ALPHABET $A = T \uplus P$

ASSERTION TELLS ME ABOUT THE STATE OF MY VARIABLES

VARIABLES $t_1, \ldots, t_n, \overline{t_1}, \ldots, \overline{t_n}$

$$\alpha := \underbrace{t_1 \overline{t_2} t_3 \ldots \overline{t_{n-1}} t_n}_{\text{ONE FOR EACH VARIABLE}} \leftarrow \text{FULL TEST / VALUATION}$$

THESE ARE THE ATOMS OF BA GENERATED BY T.

SUPPOSE WE HAVE $t_1, t_2, \overline{t_1}, \overline{t_2}$

WHAT INFORMATION CAN I HAVE?

$\alpha_0 = t_1 t_2$

$\alpha_1 = t_1 \overline{t_2}$

$\alpha_2 = \overline{t_1} t_2$

$\alpha_3 = \overline{t_1}\, \overline{t_2}$

EACH ATOM TELLS YOU EXACTLY WHAT VARIABLES WE HAVE.

ATOMS $\cong 2^T \subseteq B$
At

SEMANTICS OF BOOLEANS $[\![b]\!] = 2^{2^T}$

REGULAR EXPRESSIONS ~ TRACES

TRACE FOR KAT PROGRAMS:

$\alpha_0 p_0 \alpha_1 p_1 \alpha_2 p_2 \ldots \alpha_k p_k \alpha_{k+1}$

ACTIONS MAY CHANGE THE STATE OF VARIABLES

$A^* \mapsto (At \cdot P)^* \cdot At$

FOR EXAMPLE: p $\boxed{x := 1}$ UNINTERPRETED

$[\![p]\!] = \alpha \mapsto \alpha[x = 1]$

POUS (POPL'15): SYMBOLIC PROGRAM EQUIVALENCE

- TESTS AS BDDs (BOOLEAN DECISION DIAGRAMS)
- PROGRAMS AS FDDs (BDDs + VARIABLES)

$$[\![e]\!] : 2^{\overbrace{(At\ P)^* \cdot At}^{\text{GUARDED STRINGS}}}$$

$$[\![b]\!] = \{\alpha \mid \alpha \leq b\}$$

$$[\![p]\!] = \{\alpha p \beta \mid \alpha, \beta \in At\}$$ TRANSFORM ANY α TO ANY β

- DENOTATIONAL SEMANTICS
- RELATIONAL SEMANTICS $(R(p) : 2^{At \times At})$ ALLOWS FOR FURTHER REFINDMENT.

(BACK TO DENOTATIONAL SEMANTICS)

$$[\![e+f]\!] = [\![e]\!] \cup [\![f]\!]$$

$$[\![e;f]\!] = [\![e]\!] \diamond [\![f]\!]$$

$$\alpha_0 p_0 \alpha_1 p_1 \cdots \alpha_k \diamond \beta_0 q_0 \beta_1 \cdots$$

$$= \alpha_0 p_0 \ldots \alpha_k q_0 \beta_1 \cdots \quad (\text{IF } \alpha_k = \beta_0)$$

- DELETE β_0 AND COMBINE IF $\alpha_k = \beta_0$
  - PARTIAL, UNDEFINED OTHERWISE

NOTE: $\alpha \leq \beta \Rightarrow \alpha = \beta$ FOR $\alpha, \beta \in At$

$$[\![\text{if } b \text{ then } p \text{ else } q]\!] = [\![b;p]\!] \cup [\![\bar{b};q]\!]$$

$(b;p + \bar{b};q)$

$$= [\![b]\!] \diamond [\![p]\!] \cup [\![\bar{b}]\!] \diamond [\![q]\!]$$

$$= \{\alpha \mid \alpha \leq b\} \diamond \{\alpha p \beta \mid \alpha, \beta \in At\} \cup \cdots$$

$$= \{\alpha p \beta \mid \alpha \leq b\} \cup \{\alpha q \beta \mid \alpha \leq \bar{b}\}$$

$[\![\text{while } b \text{ do } p]\!]$

$(b;p)^* \bar{b}$

$= \{ \underset{\leq \bar{b}}{\beta}, \underset{\leq b}{\alpha_0} p \beta, \alpha_0 p \alpha_1 p \beta, \alpha_0 p \alpha_1 p \alpha_2 p \beta, \dots \}$

$\alpha_i \leq b, \quad \beta \leq \bar{b}$

while true do skip, $\equiv 0$

$;p$ ← CAN NEVER SEE THE EFFECTS

while true do $p \equiv 0$

STILL CAN'T OBSERVE EFFECTS OF p

CONNECTION TO HOARE TRIPLES:

$\vdash \{b\} C \{c\}$

- UNDER PRECONDITION b, IF C TERMINATES, IT HAS POST-CONDITION c.

$\iff b C \bar{c} \equiv 0$

- THERE ARE NO TRACES OF bC THAT DON'T SATISFY c.

$\iff bC \leq Cc$

HOMEWORK PARTIAL SOLUTIONS:

$$(x+y)^* \overset{(\leq)}{\underset{(\geq)}{\equiv}} (x^*y)^*x^*$$

$$(x+y)^* \leq (x^*y)^*x^*$$

- $1 \leq (x^*y)^*x^* \overset{\text{SLIDE}}{=} x^*(yx^*)^*$

$\forall z,\ 1 \leq z^* :\quad 1 \leq x^*,\quad 1 \leq (x^*y)^*,$

$\qquad 1;1 \leq (x^*y)^*x^*$

- $xx^*(yx^*)^* \leq x^*(yx^*)^*$

$xx^* \leq \underbrace{x^*}_{\text{UNFOLD}}$ NOTE: $e \leq f \Rightarrow [\![e]\!] \leq [\![f]\!]$

INSTANCE OF

$xx^* \leq 1 + xx^*$

- $(yx^*)(yx^*)^* \leq (yx^*)^* \leq x^*(yx^*)^*$

$$1 + (x+y)\underbrace{\boxed{x^*(yx^*)^*}}_{\mathcal{X}} \leq \underbrace{\boxed{x^*(yx^*)^*}}_{\mathcal{X}}$$

$$\xRightarrow{\text{FIXPOINT}} (x+y)^* \leq \mathcal{X} = x^*(yx^*)^* = (x^*y)^*x^*$$

- DECIDING WITH AXIOMS IS EQUIVALENT TO DECIDING WITH DFAs, BUT DFAs IS BETTER FOR MECHANIZATION
- KAT GIVES USEFUL INTUITION FOR WORKING WITH PROGRAMS

KAT

- SOUNDNESS + COMPLETENESS
  KA + BA
- AUTOMATON MODEL

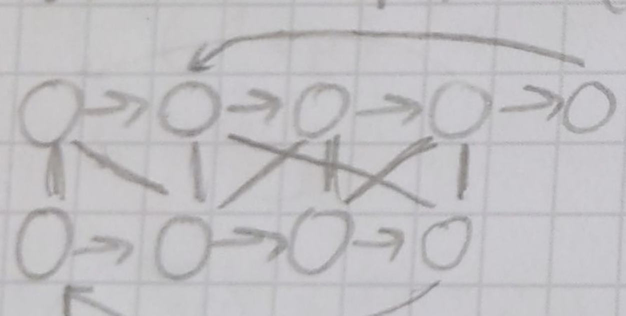
$$\bigcirc \xrightarrow{\alpha, p} \bigcirc \quad \text{KAT AUTOMATA}$$
$$\Downarrow$$
$$\{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_k\}$$

- DECISION PROCEDURE FOR EQUIVALENCE
  - BDDs (POUS) - BINARY DECISION DIAGRAMS
  - MATRICES (KOZEN)
  - IN PSPACE

→ UNION-FIND DATA STRUCTURE (HOPCROFT, TARJAN)

- $O(n \underbrace{\lg_c}_{\text{VERY SMALL}} n)$

COINDUCTION UP-TO (NFA, DFA, BRZ DER)



- STOP PROCEDURE EARLIER BASED ON STRUCTURE
- SOUND, WEAKER WAY OF CHECKING
- WORST CASE, CAN'T STOP EARLY, BUT CAN IN MANY CASES
- (BONCHI / POUS, POPL '14)

EXAMPLE:

while b do
    p;
    while c do
        q;

$\equiv$

if b then
    p;
    while $b \vee c$ do
        if c then q
        else p

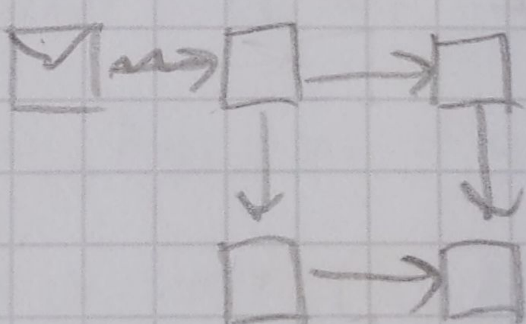
$$(bp(\underline{cq)^*\bar{c}})^*\bar{b} \equiv b;p;((b+c)(\underline{cq+\bar{c}p}))\bar{b}\bar{c}+$$

- DISTRIBUTE, DENESTING, SLIDING

NETKAT IS A SPECIAL KAT (OFFICIAL CAT: CARBON, POPL '15/16)

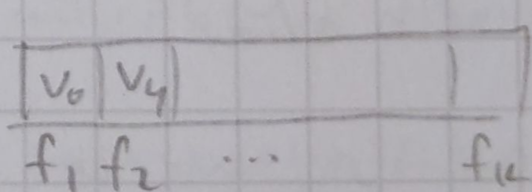
(◉)

- ZOOM IN ON SEQUENTIAL COMPOSITION: CARBON EYES
- PREVIOUSLY, NETCORE
  - REASONING ABOUT NETWORKS



FIELDS $= \{f_1, f_2, \dots\}$

VALUES $= \{v_0, \dots, v_k\}$



  - NODES CAN TEST/SET VALUES IN PACKETS

NET KAT

$p \quad f \leftarrow n$ INTERPRETED!

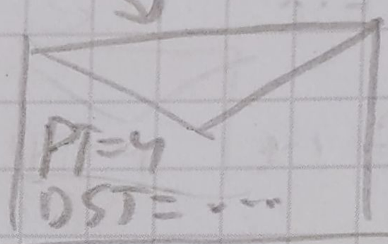
$t \quad f = n$

EXAMPLE:

- SW - SWITCH
- TYPE - $\{ \text{SSH}, \ldots \}$
- PT - PORT
- DST - DESTINATION

PACKET FILTER:

$(sw = 2);(type = SSH);$
$(pt \leftarrow 4);$
$(dst \leftarrow 10.2.10.2)$



- INTERPRETED:
  - MORE EQUATIONS HOLD

$$f \leftarrow n ; f \leftarrow m \equiv f \leftarrow m$$

$$f = n ; f \leftarrow n \equiv f = n$$

$$f \leftarrow n ; f = n \equiv f \leftarrow n$$

$\vdots$