DOMAIN THEORY

A TUTORIAL

C.A.R. HOARE

FIND X s.t X = F(X)

1. e.g X = <u>if</u> b <u>then</u>

<u>begin</u> P; X <u>end</u>

Ans. X = <u>while</u> b <u>do</u> P

2. e.g X = <u>if</u> b <u>then</u>

<u>begin</u> P; X; Q <u>end</u>

Ans X =

$$X = F(X)$$

Problem: solve for X if possible

Example: **while** b **do** P solves

```
X = if b then begin P; X end
```

Implementation:

```
loop: if not b then goto end;
        ...P...; goto loop;
end: ...
```

$X = F(X)$

Implementation:

Let apol = print "sorry"; stop

Try F(apol) – if it stops, start again

with F(F(apol)) – & if necessary,

again with ...

F(F(... (F(apol)...)))

... – until it works.

$$X = F(X)$$

Examples:

$$0 = 2 \times 0 = -0 = 0/2 = 0^2 = \sqrt{0}$$

Define: $g(x) = x/2 + 1/x$

$$\begin{aligned} g(\sqrt{2}) &= \sqrt{2}/2 + 1/\sqrt{2} \\ &= \sqrt{2}/2 + \sqrt{2}/2 \\ &= \sqrt{2} \end{aligned}$$

$$g(x) = x/2 + 1/x$$

$$g(1) = 1/2 + 1/1 = 3/2$$

$$g(1)^2 = 9/4 = 2 + 1/4$$ red

$$g(g(1)) = (3/2)/2 + 1/(3/2) = 17/12$$

$$g(g(1))^2 = 289/144 = 2 + 1/144$$ red

$$g(g(g(1))) = 577/408$$

$$g(g(g(1)))^2 = 2 + 1/332928$$

o o o

What can go wrong ...

1. $X = X + 1$ has no solution
2. $X = -X$ is not solvable by

   $-1, -(-1), -(-(-1)), \ldots$
3. $X = X^2$ has two solutions $0, 1$.

Let $X \sqsubseteq Y$ mean

select X rather than Y

as a solution to $F(X) = X$

$\sqsubseteq$ is a partial order

i.e., for all x, y and z

$x \sqsubseteq x$

if $x \sqsubseteq y$ and $y \sqsubseteq z$ then $x \sqsubseteq z$

if $x \sqsubseteq y$ and $y \sqsubseteq x$ then $x = y$

$\perp \sqsubseteq x$

$\perp$ is solution chosen for

$$X = X$$

MAXIMUM

$\mathrm{Max}(S)$ is in S, and

$x \sqsubseteq \mathrm{Max}(S)$ for all x in S.

Example: if $x \sqsubseteq y$, $\mathrm{Max}\{x, y\} = y$.

But if x and y are incomparable

(i.e., neither $x \sqsubseteq y$ nor $y \sqsubseteq x$)

then $\{x, y\}$ has no maximum.

DIRECTED SETS

S is directed **means**

S is not empty

and for all x and y in S

there is a z in S such that

$x \sqsubseteq z$ and $y \sqsubseteq z$.

S is a chain **means**

every pair in S is comparable.

CHAINS

S is a chain means

S is a nonempty series

$\{s_0, s_1, s_2, \ldots s_n, s_{n+1}, \ldots\}$

in ascending order

$s_0 \sqsubseteq s_1 \sqsubseteq s_2 \sqsubseteq \ldots \sqsubseteq s_n \sqsubseteq s_{n+1} \sqsubseteq \ldots$

LEAST UPPER BOUND

y is an upper bound of S means

$x \sqsubseteq y$ for all x in S

lub(S) is least of upper bounds of S

Theorem: $\text{lub}(S) = \text{lub}(S \cup \{\bot\})$

DOMAINS

D is a domain **means**

it is partially ordered by $\sqsubseteq$

it contains $\perp$

and contains lub(S) for every ascending chain S of D

MONOTONY

f is monotonic means

$$f(\mathrm{Max}(S)) = \mathrm{Max}\{f(x) \mid x \text{ is in } S\}$$

If $x \sqsubseteq y$ then $y = \mathrm{Max}\{x, y\}$

so $f(y) = \mathrm{Max}\{f(x), f(y)\}$

and $f(x) \sqsubseteq f(y)$

Examples: $2 \times x$, x^2, $\sqrt{x}$ (on +ve nos)

$$\mathrm{trunc}(x) = \mathrm{Max}\{i \mid i \text{ is an integer} \leq x\}$$

CONTINUITY

f is continuous means

$$f(\mathrm{lub}(S)) = \mathrm{lub}\{f(x) \mid x \text{ is in } S\}$$

Continuous functions are monotonic

but $\mathrm{trunc}(\mathrm{lub}\{x \mid x < 2\}) = \mathrm{trunc}(2) = 2$

$$\mathrm{lub}\{\mathrm{trunc}(x) \mid x < 2\} = \mathrm{trunc}(1) = 1$$

CONSTRUCTION

Define $f^0(x) = x$

$f^{n+1}(x) = f(f^n(x))$ all $n \geq 0$.

$\text{fix } f = \text{lub}\{f^0(\perp), f^1(\perp), f^2(\perp), \ldots, f^n(\perp), \ldots\}$

Theorems: $f^n(\perp) \sqsubseteq f^{n+1}(\perp)$ for all n

$f(\text{fix } f) = \text{fix } f$

If $f(y) = y$ **then** $\text{fix } f \sqsubseteq y$

$f^n(\bot) \sqsubseteq f^{n+1}(\bot)$ for all n.

Proof: by induction on n

if $n = 0$: $f^0(\bot) = \bot$ def. f^0

$\bot \sqsubseteq f^1(\bot)$ def. $\bot$

Assume: $f^n(\bot) \sqsubseteq f^{n+1}(\bot)$ by induct.

$\therefore\ f(f^n(\bot)) \sqsubseteq f(f^{n+1}(\bot))$ f monotonic

$\therefore\ f^{n+1}(\bot) \sqsubseteq f^{n+2}(\bot)$ def. f^n

$F(\text{fix } F) = \text{fix } F$

$f(\text{fix } f)$: solve for X if possible

$\equiv f(\text{lub}\{\bot, f(\bot), \ldots, f^n(\bot), \ldots\})$ so **defs fix f**

$= \text{lub}\{f(\bot), f(f(\bot)), \ldots, f^{n+1}(\bot), \ldots\}$ **f contin.**

$\equiv \text{lub}\{\bot, f(\bot), f(f(\bot)), \ldots, f^{n+1}(\bot), \ldots\}$ **proved**

$= \text{fix } f$ **def fix f**

example

loop: while b do P

implementation

loop: if not b then goto end;

... P ...; goto loop;

end: ...

If $f(y) = y$ then $\mathrm{fix}\, f \sqsubseteq y$

By induction: $f^n(\bot) \sqsubseteq y$

If $n = 0$:	$f^0(\bot) = \bot \sqsubseteq y$	def f^0, $\bot$
Assume:	$f^n(\bot) \sqsubseteq y$	by induction
$\therefore$	$f(f^n(\bot)) \sqsubseteq f(y)$	f monotonic
$\therefore$	$f(f^n(\bot)) \sqsubseteq y$	y is fixpoint
$\therefore$	$f^{n+1}(\bot) \sqsubseteq y$	def f^n

Why should you be interested in

DOMAIN THEORY?

(due to Dana Scott)

INTRODUCTION

by Tony Hoare

Problems

1. No f.p. $x = x+1$
2. f.p. non-approximable $x = -x$
3. f.p non-unique $x = x^2$

so choose "least" answer

A partial order $\sqsubseteq$ is

1. reflexive $x \sqsubseteq x$
2. transitive if $x \sqsubseteq y$ and $y \sqsubseteq z$ then $x \sqsubseteq z$
3. antisymmetric if $x \sqsubseteq y$ and $y \sqsubseteq x$ then $x = y$
4. has bottom $\bot \sqsubseteq x$

A CHAIN

$x_0, x_1, \ldots, x_n, \ldots$ is a sequence

such that $x_0 \sqsubseteq x_1 \sqsubseteq x_2 \ldots \sqsubseteq x_n \sqsubseteq x_{n+1} \ldots$

y is an upper bound of C

if $x \sqsubseteq y$ for all x in C

lub(C) = least upper bound(C)

lub($x_1, x_2, \ldots, x_n$) $= x_n =$ max(C)

Functions with fixed points

f is <u>monotonic</u> means

$$f(\max(x_1, \ldots x_n))$$

$$= \max(fx_1, \ldots, fx_n) = fx_n$$

f is <u>continuous</u> means

$$f(\mathrm{lub}(x_1, x_2, \ldots))$$

$$= \mathrm{lub}(fx_1, fx_2, \ldots))$$

To find <u>least</u> X s.t. $X = f(X)$

Let $C = \perp, f(\perp), f(f(\perp)), \ldots$

Let $X = \mathrm{lub}(C)$

We need to prove

1. C is a chain
2. $f(\mathrm{lub}(C)) = \mathrm{lub}(C)$
3. if $Y = f(Y)$ then $X \sqsubseteq Y$

1. C is a chain

Base $\bot \sqsubseteq f(\bot)$

Ind: assume $f^n(\bot) \sqsubseteq f^{n+1}(\bot)$

then $f(f^n(\bot)) \sqsubseteq f(f^{n+1}(\bot))$

i.e., $f^{n+1}(\bot) \sqsubseteq f^{n+2}(\bot)$

2. $F(\mathrm{lub}(C)) = \mathrm{lub}(C)$

$$F(\mathrm{lub}(\bot, F(\bot), F(F(\bot)), \ldots))$$

$$= \mathrm{lub}(F(\bot), F(F(\bot)), F(F(F(\bot))), \ldots)$$

$$= \mathrm{lub}(C)$$

3 Assume $Y = f(Y)$

base: $\bot \sqsubseteq Y$

induc: assume $f^n(\bot) \sqsubseteq Y$

so $f(f^n(\bot)) \sqsubseteq f(Y)$

$= Y$

therefore $f^{n+1}(\bot) \sqsubseteq Y$

conclude Y is an upper bound of C

so least upper bound$(C) \sqsubseteq Y$