Lec2 Notes

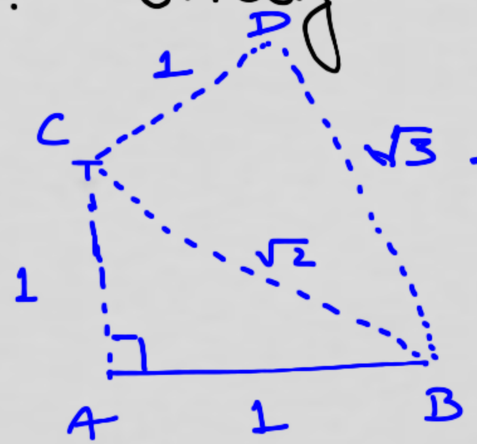
Last time we saw

1. Notion of computation, algorithm, program
2. Notion of computing tools, model of computation

Q: Is a mathematical defⁿ always representible as an algorithm?
Eg: $y = \sqrt{x}$

Let us consider some more examples:

1. Straight edge & compass: Given two pts A, B 1 unit apart, compute $\sqrt{n}$



Recipe? Justification? Prog by induction

2. Long multiplication $a \times b$

where a is comprised of a sequence of digits $a_m a_{m-1} \ldots a_0$ $\left[a = \sum_{i=0}^{m} 10^i a_i\right]$

Similiarly b is comprised of a seq. of digits $b_n b_{n-1} \ldots b$ $\left[b = \sum_{j=0}^{n} 10^j b_j\right]$

thus,

$$a \times b = a \times \sum_{j=0}^{n} 10^j b_j = ab_0 + ab_1 \cdot 10 + \ldots + ab_n \cdot 10^n$$

$$\text{LongMult}(a,b) = \begin{cases} ab_0 & \text{if } n = 0 \\ ab_0 + \text{LongMult}(a,b') \cdot 10 & \text{if } n > 0 \end{cases}$$

where $b_0 = b \text{ Rem } 10$

$b' = b \text{ Quo } 10$

Justification

for all $a > 0$ & $b \geq 0$

alg computes $a \cdot b$,

i.e. longmult $(a, b) = a \times b = a \cdot b$

Proof: Induction

Base Case:

if $b = 0$, clearly $ab_0 = 0$ = longmult (a, b)

IH

Assume longmult $(a, c) = ac$ for all c where c has less than $n+1$ digits

i.e. $0 \leq c < 10^n$

Induction Step

$\because n > 0 \Rightarrow b > 0$. Then

$b_0 = b \bmod 10$

$b' = b \operatorname{Quo} 10$

$\therefore b = 10b' + b_0 \longrightarrow (1)$

$\therefore$ longmult (a, b)

$= a b_0 +$ longmult (a, b')

$= a b_0 + a b' \cdot 10$ [from IH]

$= a (b_0 + b' \cdot 10)$

from (1)

$= a \cdot b$

[Key observation: we inducted on the length of the sequence of digits, i.e. n, comprising b]

Key understanding about algorithms

- They are finite processes
  - which means that all the computation in an algo. must terminate
  - as a result, during justification of correctness we must also argue about termination!

Our model of Computation

Primitive Sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{B}$, $\mathbb{R}$

Primitive functions:

$\mathbb{N} \longrightarrow \mathbb{N}$ [Eg: fact(n)]

$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ [Eg: + over ints]

$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ [Eg: /]

$\mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}$ [Eg: $\wedge$]

$\mathbb{B} \longrightarrow \mathbb{B}$ [Eg: $\neg$]

Primitive Relations: Expressed as 'boolean-valued' functions [though they can be general]

Eg: $\leq, \geqslant$ $[\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{B}]$

Methods of Combination

square(n) = n * n

sum-of-squares(x, y) = square(x) ⊕ square(y)

Substitution

f(n) = sum-of-squares(n+1, n+2)

↳ sig $\mathbb{N} \longrightarrow \mathbb{N}$

The Conditional

Eg: Abs(x) = $\begin{cases} x & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -x & \text{if } x < 0 \end{cases}$

$\mathbb{Z} \longrightarrow \mathbb{Z}$

PIM1 , v1

A property holds $\forall n \in \mathbb{N}$ provided

- P holds for $n = 0$
- $\forall$ P holds for arbitrary $n \geq 0$, P also holds for $n+1$

Instead of an infinitary proof we have a compact finitary proof which exploits similarity of proofs for all n except the basis

PMI v2

Basis : P holds for $k \geq 0$

Induction : P holds for arbitrary $n \geq k$,
then P holds for $n+1$

Eg : Stamps of two denom. 3 Rs, 5 Rs
Any stamp with denom. Rs 8 or more
can be made using the above stamps
$\forall n \geq 8$
i.e. , $n = 3i + 5j$ $\forall\ i, j \geq 0$

Proof :
- Basis : for $n = 8$, $n = 3 + 5$ where $i = 1, j = 1$
- Induction Hypothesis : $n = 3i + 5j$ for an $n \geq 8$, $i, j \geq 0$
- Induction : $n+1 = \begin{cases} 3(i-3) + 5(j+2) & \text{if } i \geq 3 \\ 3(i+2) + 5(j-1) & \text{otherwise} \end{cases}$

PMI v3

- Basis : P hold for 0 and
- Induction: P holds for all n

Eg:

$$F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2$$

$$F_0 = 0$$

$$F_1 = 1$$

Let $\phi = \frac{1+\sqrt{5}}{2}$

Show $F_n \leq \phi^{n-1}$

- Basis : $n = 1$ $P(0) = 1$

  indeed $1 \leq 1$

⋮

Induction

$$F_{n+1} = F_n + F_{n-1}$$

$$\leq \phi^{n-1} + \phi^{n-2} \quad (\text{By IH})$$

$$\leq \phi^{n-2}(\phi + 1)$$

$$= \phi^{n-2} \cdot \phi^2 = \phi^n$$