COMP122/20 - Data Structures and Algorithms

11 Mathematical Induction

Instructor : Ke Wei 〖柯韋〗

➽ A319 ✆ Ext. 6452 ✉ wke@ipm.edu.mo

http://brouwer.ipm.edu.mo/COMP122/20/

Bachelor of Science in Computing, School of Applied Sciences, Macao Polytechnic Institute

February 24, 2020

Outline

Textbook §3.4.

Mathematical Induction

Purpose We use mathematical induction to prove that a property P holds for all integers n starting from a base integer n_0.

Structure

- *Base case* : To prove that P holds for the base integer n_0.
- *Induction step* : Assuming P holds for integer $n_0 \leqslant k < n$, then to prove that P also holds for integer n.

Example Every natural number is either $2m$ or $2m+1$, for some m. We induct on n.

- Base case: $0 = 2 \times 0$, that is $2m$, for $m = 0$.
- Induction step: if for all $0 \leqslant k < n$, k is either $2m'$ or $2m'+1$, for some m', then we have

$$n = (n-1)+1 = \begin{cases} 2m'+1 & \text{if } n-1 = 2m'\text{, that is } 2m+1\text{, for } m = m', \\ 2(m'+1) & \text{if } n-1 = 2m'+1\text{, that is } 2m\text{, for } m = m'+1. \end{cases}$$

Geometric Series

For real number $x \neq 1$ and integer $n \geqslant 0$, we prove by induction on n that

$$x^0 + x^1 + \cdots + x^n = \sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}.$$

- Base case: $x^0 = 1 = \dfrac{1-x^{0+1}}{1-x}$.
- Induction step: for $n \geqslant 1$,

$$\begin{aligned} \sum_{i=0}^{n} x^i &= \left(\sum_{i=0}^{n-1} x^i\right) + x^n && [\text{by } \textstyle\sum] \\ &= \frac{1-x^{(n-1)+1}}{1-x} + x^n && [\text{by induction hypothesis}] \\ &= \frac{(1-x^n)+(x^n-x^{n+1})}{1-x} = \frac{1-x^{n+1}}{1-x}. && [\text{by arithmetic}] \end{aligned}$$

Validity of Mathematical Induction

With the base case $P(0)$ and the induction step

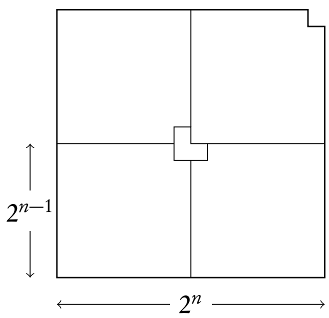
$$(\text{for } n \geqslant 1)\ P(0) \text{ and } P(1) \text{ and } \ldots \text{ and } P(n-1) \Longrightarrow P(n),$$

we can generate the entire proof of $P(n)$ for any finite integer $n \geqslant 1$:

$$\left.\begin{array}{r} \left.\begin{array}{r} \left.\begin{array}{r} P(0) \Longrightarrow P(1) \\ P(0) \end{array}\right\} \Longrightarrow P(2) \\ P(1) \\ P(0) \end{array}\right\} \Longrightarrow \cdots \Longrightarrow P(n-1) \\ P(n-2) \\ \vdots \\ P(1) \\ P(0) \end{array}\right\} \Longrightarrow P(n).$$

A Checkerboard with One Corner Removed

A $2^n \times 2^n$ checkerboard ($n \geqslant 1$) with one corner square removed can be covered by one or more L-shaped tiles.



Reasoning about Recursive Functions — Integer Powers

For the tail recursive method to compute integer powers:

$$pow\_sq(x,n,p) = \begin{cases} p & \text{if } n = 0, \\ pow\_sq(x^2,k,p) & \text{if } n = 2k \geqslant 2, \\ pow\_sq(x^2,k,px) & \text{if } n = 2k+1 \geqslant 1. \end{cases}$$

We prove by induction on n that $pow\_sq(x,n,p) = px^n$, for $n \geqslant 0$.

- Base case: $pow\_sq(x,0,p) = p = px^0$.
- Induction step: 1) for $n = 2k \geqslant 2$, we have $0 \leqslant 1 \leqslant k < n$, and

$$\underset{\text{[by } pow\_sq\text{]}}{pow\_sq(x,n,p) = pow\_sq(x^2,k,p)} \underset{\text{[by induction hypothesis]}}{=} p(x^2)^k \underset{\text{[by arithmetic]}}{=} px^{2k} = px^n.$$

2) for $n = 2k+1 \geqslant 1$, we have $0 \leqslant k < n$, and

$$\underset{\text{[by } pow\_sq\text{]}}{pow\_sq(x,n,p) = pow\_sq(x^2,k,px)} \underset{\text{[by induction hypothesis]}}{=} px(x^2)^k \underset{\text{[by arithmetic]}}{=} px^{2k+1} = px^n.$$

Fibonacci Numbers

- Since the argument to prove is used as induction hypothesis, sometimes we have to prove something *stronger*.
- Let $F_0, F_1, \ldots, F_n$ be the Fibonacci numbers, and

$$fib\_t(n,a,b) = \begin{cases} a & \text{if } n = 0, \\ b & \text{if } n = 1, \\ fib\_t(n-2, a+b, b+(a+b)) & \text{if } n \geqslant 2. \end{cases}$$

- To prove $fib\_t(n,F_0,F_1) = F_n$, we need to prove $fib\_t(n,F_i,F_{i+1}) = F_{i+n}$, for $n \geqslant 0$ and $i \geqslant 0$.
- Base cases: $fib\_t(0,F_i,F_{i+1}) = F_i = F_{i+0}$ and $fib\_t(1,F_i,F_{i+1}) = F_{i+1}$.
- Induction step: for $n \geqslant 2$,

$$\begin{aligned} fib\_t(n,F_i,F_{i+1}) &= fib\_t(n-2, F_i+F_{i+1}, F_{i+1}+(F_i+F_{i+1})) && \text{[by } fib\_t\text{]} \\ &= fib\_t(n-2, F_{i+2}, F_{i+3}) && \text{[by Fibonacci]} \\ &= F_{(i+2)+(n-2)} = F_{i+n}. && \text{[by induction hypothesis]} \end{aligned}$$

Reasoning about Loops — Summation

Given an integer $n \geqslant 1$, prove that the following loop $L(n)$ computes $\sum_{i=1}^{n} i$ in variable s.

```
s = 0
for j in range(1, n+1):
    s += j
```

The loop can be → transformed to

```
1 s = 0
2 for j in range(1, n):
3     s += j
4 s += n
```

- Base case: after $L(1)$, we have $s = 1$.
- Induction step: for $n \geqslant 2$, by induction hypothesis, after $L(n-1)$, we have $s = \sum_{i=1}^{n-1} i$, thus after line 4, we have $s = \sum_{i=1}^{n} i$.

Finding the Maximum Element

Given an integer $n \geqslant 1$, prove that the following loop $L(a,n)$ computes $\max\{a[0], a[1], \ldots, a[n-1]\}$ in variable m.

```
m = a[0]
for j in range(1, n):
    if m < a[j]:
        m = a[j]
```

$\xrightarrow[\text{transformed to}]{\text{When } n\geqslant 2\text{, the loop can be}}$

```
1 m = a[0]
2 for j in range(1, n-1):
3     if m < a[j]:
4         m = a[j]
5 if m < a[n-1]:
6     m = a[n-1]
```

We induct on n.

- Base case: after $L(a,1)$, we have $m = a[0] = \max\{a[0]\}$.
- Induction step: for $n \geqslant 2$, by induction hypothesis, after $L(a,n-1)$, we have $m = \max\{a[0], a[1], \ldots, a[n-2]\}$, thus after line 3, we have $m = \max\{\max\{a[0], a[1], \ldots, a[n-2]\}, a[n-1]\}$.

Euclid's Algorithm for Finding GCD

Given integers $m > n \geqslant 0$, prove that the following loop $L(m^\circ, n^\circ)$ computes the greatest common divisor of the initial m and n (denoted as m° and n°, respectively) — $\gcd(m^\circ, n^\circ)$, and stores the result in variable m.

```
while n != 0:
    m, n = n, m%n
```

$\xrightarrow[\text{transformed to}]{\text{The loop can be}}$

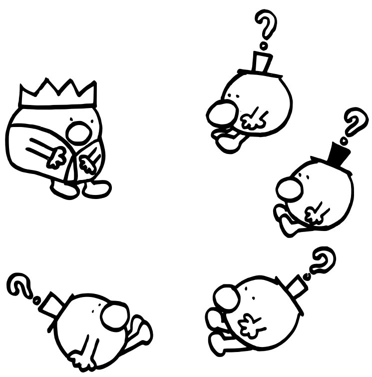
```
1 if n != 0:
2     m, n = n, m%n
3     while n != 0:
4         m, n = n, m%n
```

We induct on n°.

- Base case: after $L(m^\circ, 0)$, we have $m = m^\circ = \gcd(m^\circ, 0)$.
- Induction step: for $n^\circ \geqslant 1$, after line 2, we have $m = n^\circ$ and $n = m^\circ \,\%\, n^\circ$ with $m = n^\circ > m^\circ \,\%\, n^\circ = n \geqslant 0$, by induction hypothesis, after $L(n^\circ, m^\circ \,\%\, n^\circ)$, we have $m = \gcd(n^\circ, m^\circ \,\%\, n^\circ) = \gcd(m^\circ, n^\circ)$.

Mathematicians and Hats

- The King placed 10 hats on 10 mathematicians, one on each head. None of the mathematicians knew the color of his own hat, however, they could see all others' hats.
- The King told the mathematicians that all hats were either *black* or *white* and *at least one* of them was white.
- The King said that he would ask them once every minute, those who knew the color of his own hat should stand up.
- On the first asking, there was no one standing up; so as on the second asking, the third, ... But on the 10^{th} asking, all mathematicians stood up and claimed that their hats were all white.



✍ Why?