A. V. Gerbessiotis CS435

Dec 22, 2015 Spring 2016

Brief Discrete Mathematics Review Handout 3

TABLE OF CONTENTS.

1 Sample Quiz

Start doing this quiz. It will give you a guidance on where you stand re your DISCRETE MATH background. The more questions you don't know the more time you need to review this and other handouts, and your favorite discrete math book.

1) How much is the following sum if $x \neq 1$?

$$1 + x + x^2 + x^3 + \ldots + x^n = ?$$

2) What if $x = 1$ below?

$$1 + x + x^2 + x^3 + \ldots + x^n = ?$$

3) How much is the following sum?

$$\sum_{i=1}^{n} i = ?$$

4) How much is the following sum?

$$\sum_{i=1}^{n} i^2 = ?$$

5) Let $a + b = 100000$, for some $0 \leq a, b \leq 100000$. What are the values a, b that maximize the product $a \cdot b$?

6) For $x \in R$, we define $y = \lg(x)$ such that $2^y = x$. Answer the following.

- $\lg(1) = ?$
- $\lg(128) = ?$
- $\lg(2^{(x+y)}) = ?$
- $\lg(32 \cdot 2^{(x+y)}) = ?$

7) For $x \neq 1$, let $1 + x + x^2 + \ldots + x^n = f(x)$. Let us assume that the first derivative of f with respect to x is known, ie $f'(x)$ is known. Express the following sum in terms of $x, f(x)$ and $f'(x)$.

$$x + 2x^2 + 3x^3 + \ldots + nx^n = ?$$

8) How many times is the statement $x = x + 1$ of line 3 executed? Express the result in terms of n. Operator / divides two numbers x and y so that x/y is the quotient of the division, i.e. the result of 10/4 is 2.

```
1.  int i,x=0;
2.  for(i=1;i<=n;i++)
3.    if ( (i-(i/5)*5) == 0) x=x+1;
```

2 Sample Quiz Solutions

1) How much is the following sum if $x \neq 1$?

$$1 + x + x^2 + x^3 + \ldots + x^n = \frac{x^{n+1} - 1}{x - 1}$$

2) What if $x = 1$ below?

$$1 + x + x^2 + x^3 + \ldots + x^n = n + 1$$

3) How much is the following sum?

$$\sum_{i=1}^{n} i = n(n+1)/2$$

4) How much is the following sum?

$$\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$$

5) The product ab is maximized for $a = b = 100000/2 = 50000$. One way to prove it is solve for b in $a + b = 100000$, ie $b = 100000 - a$, substitute for b in ab to get a function $f(a) = a(100000 - a)$. The first derivative $f'(a) = 100000 - 2a$ and has a root for $a = 100000/2 = 50000$. This root is maximum as the second derivative at $a = 50000$ of $f(a)$ is negative ($f^{''}(a) = -2$).

6) For $x \in R$, we define $y = \lg(x)$ such that $2^y = x$. Answer the following.

- $\lg(1) = 0$
- $\lg(128) = 7$
- $\lg(2^{(x+y)}) = (x + y)$
- $\lg(32 \cdot 2^{(x+y)}) = \lg 32 + \lg 2^x + \lg 2^y = (x + y + 5)$

7) Start from $1+x+x^2+\ldots+x^n = f(x)$. Take the first derivative of both sides. We get $0+1+2x+\ldots+nx^{n-1} = f'(x)$. Multiply both sides by x and the answer follows.

8) The test term $(i - (i/5) * 5)$ computes the remainder of the division of i by 5. It is zero for $i = 5, 10, 15, \ldots$. Therefore the number of times $x = x + 1$ will be executed is floor(n/5) i.e. $\lfloor n/5 \rfloor$.

A formula collection.

The mathematics (not discrete mathematics) that you need can be summarized in the following one-page summary.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \qquad \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

$$\text{For } a \neq 1, \quad \text{and } \mid b \mid < 1 \quad \text{we have that}$$

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}, \qquad \sum_{i=0}^{n-1} ia^i = \frac{(n-1)a^{n+1} - na^n + a}{(1-a)^2},$$

$$\sum_{i=0}^{\infty} b^i = \frac{1}{1-b}, \qquad \sum_{i=1}^{\infty} b^i = \frac{b}{1-b}, \qquad \sum_{i=0}^{\infty} ib^i = \frac{b}{(1-b)^2}.$$

$$H_n = \sum_{i=1}^{n} \frac{1}{i}, \quad \sum_{i=1}^{n} iH_i = \frac{n(n+1)}{2} H_n - \frac{n(n-1)}{4}.$$

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + \Theta\left(\frac{1}{n}\right)\right), \qquad n! \approx \left(\frac{n}{e}\right)^n, \qquad a^{\log_b n} = n^{\log_b a},$$

$$e \approx 2.718281, \qquad \pi \approx 3.14159, \qquad \gamma \approx 0.57721, \qquad \phi = \frac{1+\sqrt{5}}{2} \approx 1.61803, \qquad \hat{\phi} = \frac{1-\sqrt{5}}{2} \approx -.61803.$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \qquad \sum_{k=0}^{n} \binom{n}{k} = 2^n, \qquad \binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

L1.

$$\lg(ab) = \lg a + \lg b, \quad \lg(a/b) = \lg a - \lg b, \quad \lg(a^b) = b \lg a, \quad 2^{\lg(a)} = a,$$

L2.

$$a^x\ a^y = a^{x+y}, \quad a^x/a^y = a^{x-y}, \quad (a^x)^y = a^{xy}.$$

D1.

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x), \qquad \left(\frac{f(x)}{g(x)}\right)' = \frac{f'(x)g(x) - f(x)g'(x)}{g^2(x)}, \quad (c^x)' = \ln(c)\, c^x.$$

S1.

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots + x^i + \ldots = \sum_{i=0}^{\infty} x^i,$$

S2.

$$\frac{x}{(1-x)^2} = x + 2x^2 + \ldots + ix^i + \ldots = \sum_{i=0}^{\infty} ix^i,$$

S3.

$$e^x = 1 + x + \frac{x^2}{2!} + \ldots + \frac{x^i}{i!} + \ldots = \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

3 Logarithms and Exponentials

When we describe the performance of computer algorithms we frequently use logarithms base two and powers of two. A brief review of topics related to logarithms and exponentials is given below. For more details, one can review section 3.2 (starting on page 53).

F1. **The floor function** $\lfloor x \rfloor$ **:** denotes the largest integer smaller than or equal to x, i.e. $\lfloor 3.5 \rfloor = 3$, $\lfloor -3.5 \rfloor = -4$, and $\lfloor 3.0 \rfloor = 3$.

C1. **The ceiling function** $\lceil x \rceil$ **:** denotes the smallest integer greater than or equal to x, i.e. $\lceil 3.5 \rceil = 4$, $\lceil -3.5 \rceil = -3$, and $\lceil 3.0 \rceil = 3$.

Exponentials.

Let a, m, n be real numbers such that $a \neq 0$.

E1. $a^0 = 1, \qquad a^1 = a, \qquad a^{-1} = 1/a.$

E2. $a^m \cdot a^n = a^{n+m}, \qquad a^m / a^n = a^{m-n}.$

E3. $(a^m)^n = (a^n)^m = a^{(mn)}$.

E4. Let $c > 1, d \geq 1$ be constants. There is a constant n_0 such that for all $n \geq n_0$ we have that $c^n > n^d$.

E5. For all real x, $e^x \geq 1 + x$, where $2.7172\ldots$, the base of the Neperian logarithms.

E6. For all x such that $|x| < 1$, $1 + x \leq e^x \leq 1 + x + x^2$.

Logarithms.

L1. **Neperian Logarithms.** The natural (Neperian) logarithm log (also ln) of x denoted by $\log x$ is the real number y such that $e^y = x$. e is the well known constant $e = 2.7172\ldots$. In this course we **prefer to write and use** $\log x$ over $\ln x$; moreover we prefer logarithms base two even more!

L2. **Base-two Logarithms.** The base-2 logarithm of x, denoted by $\lg x$ (or sometimes $\log_2 x$), is the real number y such that $2^y = x$, i.e. the power we need to raise two to get x.

Properties of Logarithms.

Properties of base-2 logarithms (See page 56 for generalization to any base other than two).

L3. $\lg^k n = (\lg n)^k$. Note that $\lg^{(k)} n$ with a parenthesized exponent means something else (see page 58 of CLRS on the iterated logarithm function).

L4. $\lg \lg n = \lg (\lg n)$.

L5. For all $a > 0, b > 0, c > 0$ and n we have that

a. $a = 2^{\lg a}$,

b. $\lg (ab) = \lg a + \lg b$,

c. $\lg (a/b) = \lg a - \lg b$,

d. $\lg a^n = n \ \lg a$,

e. $\lg a = \frac{\log a}{\log 2}$.

Asymptotics.

Fact 1 *The expression "for large enough n " means "there is a positive constant n_0 such that for all $n > n_0$ ".*

Fact 2 *For any positive constant k, m and integer $n > 0$, we have that $n^m > \lg^k n$ for large enough n.*

Fact 3 *For any positive constant m and integer $n > 0$, we have that $2^n > \ n^m$ for large enough n.*

Example 1 $\lg 1 = 0$ *as* $2^0 = 1$. $\lg 2^x = x$. $\lg 2^{x+y} = x + y$.

Example 2 *How much is* $(n^{1/\lg n})$*?*

As we don't know the answer, let $x = n^{1/\lg n}$. We take logarithms of both sides of this equality. We get $\lg x = (1/\lg n)\ \lg n = 1$ by rule (L5.d), ie $\lg x = 1$. We then take powers of two for both sides i.e. $\lg x = 1$ implies that $2^{\lg x} = 2^1$. The left hand side is x by the definition of the logarithm base two, i.e. $x = 2$. Since $x = n^{1/\lg n}$, we have that $n^{1/\lg n} = 2$. □

Example 3 *For any integer $n > 0$ and constant $k > 0$, show that for large enough n $2^n > n^k$, ie show that there is a constant n_0 such that for all $n > n_0$, we have that $2^n > n^k$.*

4 How to find sums without using induction?

Proposition 1 *For all $n \geq 0$,*

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Proof. One can show this proposition by using induction. But what if we don't know how much the sum is? How can we find the answer $n(n+1)/2$?

We use the following trick to find sums of the following form

$$S_k = \sum_{i=1}^{n} i^k.$$

First consider $(i+1)^{k+1}$ and expand it. Substitute in the expansion $i = 1$, $i = 2, \ldots$, $i = n$, a total of n times and write the resulting n equalities one after the other. Then, sum these n equalities by summing up the left hand sides and the right hand sides. Solve for S_k and S_k can then be found as a function of n.

For the sum in question $k = 1$. Therefore we consider

$$(i+1)^2 = i^2 + 2i + 1$$

We substitute for $i = 1, 2, \ldots, n$ writing one equality after the other

$$\begin{aligned}
(1+1)^2 &= 1^2 + 2 \cdot 1 + 1 \\
(2+1)^2 &= 2^2 + 2 \cdot 2 + 1 \\
(3+1)^2 &= 3^2 + 2 \cdot 3 + 1 \\
(4+1)^2 &= 4^2 + 2 \cdot 4 + 1 \\
\ldots &= \ldots \\
(n+1)^2 &= n^2 + 2 \cdot n + 1
\end{aligned}$$

When we sum up the n equalities we realize that say, $(3+1)^2$ of the third line is equal to 4^2 of the fourth line and therefore.

$$(1+1)^2 + (2+1)^2 + \ldots + (n+1)^2 = (1^2 + 2^2 + 3^2 + \ldots + n^2) + 2 \cdot (1 + 2 + \ldots + n) + (1 + \ldots + 1)$$

We note that $2 \cdot (1 + 2 + \ldots + n) = 2S_1$ and $(1 + \ldots + 1) = n$ (number of ones is number of equations). Then,

$$(n+1)^2 = 1 + 2S_1 + n$$

Solving for S_1 we get that $S_1 = ((n+1)^2 - n - 1)/2$, ie $S_1 = (n^2 + 2n + 1 - n - 1)/2 = (n^2 + n)/2 = n(n+1)/2$, which proves the desired result.

Example 4 *For all $n \geq 0$, find*

$$\sum_{i=0}^{i=n} i^2$$

Example 5 *For all $n \geq 0$, find*

$$\sum_{i=0}^{i=n} i^3$$

5 Propositions, Theorems and Proofs

Definition 1 *The $\forall$ quantifier is also called the* **universal quantifier**. *It means* **"for all"**.

Definition 2 *The $\exists$ quantifier is also called the* **existential quantifier** *and it means* **there exist(s)**.

Definition 3 *Symbol $\in$ is the* **belongs to** *set membership symbol.*

Definition 4 *N is the set of natural (non negative integer) numbers.*

Definition 5 *$X \Rightarrow Y$ is also known as implication and can be stated otherwise as "X implies Y".*

In computer science we prove statements. Such statements need to be expressed/stated precisely.

An axiom is a statement (or proposition) accepted to be true without proof.
An axiom forms the basis for logically deducing other statements.

A proposition is a statement that is either true or false.
We can also define an axiom as,

An axiom is a proposition that is assumed or accepted to be true.

A proof is a verification of a proposition by a sequence of logical deductions derived from a base set of axioms.

A theorem is a proposition along with a proof of its correctness.

Every proposition is true or false with reference to a space we first define axiomatically and then build on by establishing more theorems.

Axioms of Arithmetic.

For example, Peano's axioms, on whose inductive proofs are based, define natural (non negative) numbers. The set of natural (or non-negative integers) numbers is also denoted by N.

Axiom 1 (Peano). 0 is a natural number.
Axiom 2 (Peano). If n is a natural number, then its successor $s(n)$, which we prefer to write as $n+1$ is also a natural number.

Theorems in mathematics are true because the space to which these theorems apply are based on simple axioms that are usually true.
We give the first proposition.

Proposition 2 *$\forall n \in N$, $n^2 + 7$ is prime.*

This proposition states that for all natural (non-negative) numbers $n = 0, 1, \ldots,$ the number $n^2 + 7$ is a prime number, i.e. it is a number divisible only by 1 and itself.
This proposition can be easily shown to be false by counterexample.
For $n = 3$, $n^2 + 7 = 3^2 + 7 = 16$ and one divisor of 16 other than 1 and 16, is 2. Therefore 16 is not a prime number, it is in fact a composite number and therefore this simple counterexample shows that Proposition 2 is false because it is not true for $n = 3$. □
Counterexample. To prove that this proposition is false it suffices to find a single integer of the form $n^2 + 7$ that is not a prime number. Thus determining that for $n = 3$, $3^2 + 7$ is not prime, completes the proof that the proposition is FALSE.

Proposition 3 *$\exists n \in N$ such that $n^2 + 7$ is prime.*

In order to prove that Proposition 3 is true, we only need prove it for a single value of n. For $n = 2$, we can easily establish that $2^2 + 7 = 11$ is a prime number. □. Proposition 3 is not, however, very interesting.

6 Induction: An introduction

Induction is a principle (or proof technique) that can be used to prove theorems that depend on a variable that runs through the natural numbers (non-negative integers). An induction is a three-step process: it consists of a base case and an inductive step to form a conclusion i.e. the proof of a proposition $P(n)$ that depends on a natural number n.

(Base Case) If one can prove that some proposition $P(i)$ is true for $i = 1$,

(Inductive Step) and one can prove that "if proposition $P(i)$ is true for any (natural number) i, then it is also true for its successor, $i + 1$, i.e. $P(i + 1)$ is also true,"

(Conclusion) then, **one has proved that proposition $P(i)$ is true for all the natural numbers** $i = 1, 2, \ldots$.

Note. The base case does not have to be 1. It can be 0. It can also be, say, 2000. Then if the inductive step is established, the property will hold for all natural numbers $i = 2000, 2001, \ldots$, i.e. for "large enough" values of i, where by "large enough" we mean $i \geq 2000$.

Axiom 3 (Induction). Let $P(n)$ be a predicate.

A1. If $P(1)$ is true, and

A2. $\forall n \in N \; P(n) \Rightarrow P(n + 1)$,

A3. then $\forall n \in N$, $P(n)$ is true. (i.e. $P(n)$ is true for all n greater than or equal to the base case value, which is 1).

Axiom 3 in other words states the following, quite reasonable, observation.

A1 If I can prove that $P(1)$ is true (BASE CASE),

A2 and show that for all n "$P(n)$ is true" implies "$P(n + 1)$ is true" (INDUCTIVE STEP),

A3 then I have shown that $P(n)$ is true for all n.

Why is this so?

"Proof" why induction works.

Step 1. By way of A1 we have, $P(1)$ is true,

Step 2. By way of A2 for $n = 1$ we have, $P(1) \Rightarrow P(2)$, i.e. that $P(2)$ is true, given that $P(1)$ is true by Step 1.

Step 3. By way of A2 for $n = 2$ we have, $P(2) \Rightarrow P(3)$, i.e. that $P(3)$ is true, given that $P(2)$ is true by Step 2.

Step 4. By way of A2 for $n = 3$ we have, $P(3) \Rightarrow P(4)$, i.e. that $P(4)$ is true, given that $P(3)$ is true by Step 3.

Step .... Similarly,

Conclusion. From Steps $1, 2, 3, 4, \ldots$ we have shown that $P(1), P(2), P(3), P(4), \ldots$ are all true, ie. that $P(n)$ is true for all $n \geq 1$.

Note 1. Step 1 is that starting point i.e. it establishes the minimal value n for the case case of predicate P to be true. If it is not 1, we cannot say '$n \geq 1$' as a conclusion.

Note 2. A subtle point with induction is the inductive step. What we show with the inductive step is the following: if $P(n)$ is true then $P(n + 1)$ is also true. Thus by just proving the inductive step it does not mean that $P(n)$ is true for all $n \in N$. This is because we have got to establish the trueness of $P(n)$. This trueness is (usually) established through the base case $P(1)$. The base case is always shown directly. The base case above (Step 1) along with a single application of the inductive step (Step 2) jointly establish the trueness of $P(2)$. The trueness of $P(2)$ and the inductive step (Step 3 above) establish the trueness of $P(3)$. Instead of repeating the whole process ∞ amount of times we developed a two step process: A1 (base case) and A2 (inductive step) to show A3 (Conclusion).

6.1 Setting-up induction: An example

The first step in induction is to identify in a proposition a predicate that depends on a natural-valued variable and also that same natural-valued variable). An example proposition is given below. Let $S_k(n) = 1^k + 2^k + \ldots + n^k$ for any integer $k > 0$. We also write $S_k(n) = \sum_{i=1}^{n} i^k$. The latter term $\sum_{i=1}^{n} i^k$ indicates a sum that runs from $i = 1$ through (inclusive) $i = n$. Each term of the sum is a function of i. In our case the i-th term of the sum is i^k. We shall show that $S_1(n) = 1 + \ldots + n = n(n+1)/2$. **Here $S_1(n)$ is an alias for $1 + \ldots + n$.**

Proposition 4 *For all natural number $n \geq 1$, we have that $S_1(n) = 1 + 2 + \ldots + n = n(n+1)/2$.*

Proof of Proposition 4.

Let us call $P(n)$ the predicate $S_1(n) = n(n+1)/2$**.** We are going to show that $S_1(n) = n(n+1)/2$ i.e. we are going to show that the predicate $P(n)$ is true for all n. The proof is by induction.

1. Base case: Show that $P(1)$ is true. The left hand side sum of $P(1)$ is $S_1(1)$ i.e. the sum of one term (and that term is 1), which is 1. The right hand side of $P(1)$ is $1(1+1)/2$ which is also 1. Therefore $P(1)$ is true since the left and right hand sides of = are equal to zero and thus equal to each other.

2. Inductive Step: $\forall n \in N \ P(n) \Rightarrow P(n+1)$. That is, we show that if $P(n)$ is true then $P(n+1)$ is true. Show that $P(n) \Rightarrow P(n+1)$ for all $n \geq 1$. To prove so, we start from (assume it is true) the left-hand side (the induction hypothesis) to reach the right hand side (show that the conclusion is true).

Induction hypothesis. Let us assume that $P(n)$ is true, i.e. $S_1(n) = 1 + 2 + \ldots + n = \sum_{i=1}^{n} i = n(n+1)/2$.

We need to prove that $P(n+1)$ is then true i.e. $1 + 2 + \ldots + (n+1) = \sum_{i=1}^{n+1} i = (n+1)(n+2)/2$.

We start from the left-hand side of the latter equality to derive the right-hand side utilizing the induction hypothesis, i.e. the assumption that $P(n)$ is true which is equivalent to $S_1(n) = n(n+1)/2$.

$$\begin{aligned} 1 + 2 + \ldots + (n+1) &= \sum_{i=1}^{n+1} i \\ &= \left(\sum_{i=1}^{n} i \right) + (n+1) \\ &= n(n+1)/2 + (n+1) \\ &= n(n+1)/2 + 2(n+1)/2 \\ &= (n+1)(n+2)/2 \end{aligned}$$

We got the third equality from the second one by observing that the sum in the former equality is the one in the induction hypothesis. ■.

This completes the induction. We proved two things

- We first proved that $P(1)$ is true.
- and then showed that $P(n) \Rightarrow P(n+1)$ for all $n \geq 1$.

The two are equivalent to steps A1 and A2 of Axiom 3, and thus conclusion A3 then follows.

An alternative would have been to show

- that $P(1)$ is true,
- and then show that $P(n-1) \Rightarrow P(n)$ for all $n \geq 2$.

In the latter, we just changed indices. In induction we can go from n to $n+1$ or $n-1$ to n or from any value to its successor value.

6.2 Another example

Below, we prove the following more elaborate theorem. Note that the base case is now 0 not 1, and the variable that takes natural values is m not n.

Theorem 1 *Show that for all integer $m \geq 0$, $1 + x + \ldots + x^m = \frac{x^{m+1}-1}{x-1}$, for any $x \neq 1$.*

We relabel the natural variable in this example m instead of n.

Proof. We prove the theorem **by induction**. The natural variable in the theorem is m. The predicate $P(m)$ in the theorem that depends on m is

$P(m)$: $\quad 1 + x + \ldots + x^m = \frac{x^{m+1}-1}{x-1}$, for any $x \neq 1$.

There are various ways to represent the sum; one is $1 + x + \ldots + x^m$, another one is $\sum_{i=0}^{i=m} x^i$ or

$$\sum_{i=0}^{i=m} x^i$$

We proceed to presenting the inductive proof.

Base case. We show that $P(0)$ is true. The series $1 + x + \ldots + x^m$ for $m = 0$ has as its last term $x^m = x^0 = 1$, i.e. the first term of the sum is also the last one. This means that the series collapses into a single term. On the other hand the right hand side for $m = 0$ gives

$$\frac{x^{0+1}-1}{x-1} = \frac{x-1}{x-1} = 1$$

Therefore,

$$1 + \ldots + x^0 = 1 = \frac{x^{0+1}-1}{x-1} = \frac{x-1}{x-1}$$

which is obviously true for any $x \neq 1$ (this is required to avoid division be zero problems).

Inductive Step. We show that for all $m \geq 0$, if $P(m)$ is true, then $P(m+1)$ is also true. Our **induction hypothesis** is "$P(m)$ is true".

If $P(m)$ is true, then the following equality will hold.

$$1 + x + \ldots + x^m = \frac{x^{m+1}-1}{x-1}$$

We then need to prove that $P(m+1)$ is also true, i.e. we need to prove that

$$1 + x + \ldots + x^{m+1} = \frac{x^{m+2}-1}{x-1}$$

To prove this we start from the left hand side of $P(m+1)$ and we rewrite it so that we can use the fact that $P(m)$ is true.

$$\begin{aligned} 1 + x + \ldots + x^{m+1} &= 1 + x + \ldots + x^m + x^{m+1} \\ &= (1 + x + \ldots + x^m) + x^{m+1} \end{aligned}$$

We observe that the term $(1 + x + \ldots + x^m)$, by the trueness of $P(m)$, is known.

$$\begin{aligned} 1 + x + \ldots + x^{m+1} &= 1 + x + \ldots + x^m + x^{m+1} \\ &= (1 + x + \ldots + x^m) + x^{m+1} \\ &= \frac{x^{m+1}-1}{x-1} + x^{m+1} \end{aligned}$$

By completing the calculations we get that

$$\begin{aligned} 1 + x + \ldots + x^{m+1} &= \frac{x^{m+1}-1}{x-1} + x^{m+1} \\ &= \frac{(x^{m+1}-1) + x^{m+1}(x-1)}{x-1} \\ &= \frac{(x^{m+1}-1) + x^{m+2} - x^{m+1}}{x-1} \\ &= \frac{x^{m+2}-1}{x-1}, \end{aligned}$$

which proves that $P(m+1)$ is true. We proved the base case and the inductive step and this concludes the induction. $\blacksquare$.

Just because we set up Axiom 3 with n representing the natural number, it doesn't mean that we should always use n or have n in the Proposition. In this example m was the natural number, and the proposition dependend on m (i.e. we had $P(m)$).

6.3 Exercises

Do for practice the following examples.

Example 1. Show that for any $n \geq 0$

$$\sum_{i=0}^{i=n} i^2 = n(n+1)(2n+1)/6$$

Example 2. Show that for any $n > 1$, $n^2 - 1 > 0$.
Example 3. Show that for any $n \geq 2$, $\sum_{i=1}^{n} i \leq 3n^2/4$.
Example 4. Show that for any $x \geq 3$, $\sum_{i=0}^{n-1} x^i \leq x^n/2$.
Example 5. Show that for any $n \geq 1$, $\sum_{i=0}^{n} i^2 \leq (n^3 + 2n^2)/3$.
Example 6. What is wrong with the proof of Theorem 2 below? Explain.

Theorem 2 *All horses of the world are of the same color.*

Proof. The proof is by induction on the number of horses n.

P(n): In any set of $n \geq 1$ horses, all the horses of the set are of the same color.

1. Base Case: Show $P(1)$ is true. $P(1)$ is always true as in a set consisting of a single horse, all the horses (there is only one) of the set have the same color.

2. Inductive step : $\forall n \in N \ P(n) \Rightarrow P(n+1)$.

Let us assume (induction hypothesis) that for any $n \geq 1$, $P(n)$ is true. Since we assume $P(n)$ to be true, every set of n horses have the same color. Then we will prove that $P(n+1)$ is also true (inductive step), i.e. we will show that in every set of $n+1$ horses, all of them are of the same color.

To show the inductive step, i.e. that $P(n+1)$ is true let us consider ANY set of $n+1$ horses $H_1, H_2, \ldots H_n, H_{n+1}$.

The set of horses $H_1, H_2, \ldots, H_n$, consists of n horses, and by the induction hypothesis any set of n horses are of the same color. Therefore color(H_1) =color(H_2) $= \ldots =$color(H_n).

The set of horses $H_2, H_3, \ldots, H_{n+1}$, consists of n horses, and by the induction hypothesis any set of n horses are of the same color. Therefore color(H_2) =color(H_3) $= \ldots =$color(H_{n+1}).

Since from the first set of horses color(H_2) =color(H_n), and from the second set color(H_2) =color(H_{n+1}), we conclude that the color of horse H_{n+1} is that of horse H_2, and since all horses $H_1, H_2, \ldots, H_n$ are of the same color, then all horses $H_1, H_2, \ldots, H_n, H_{n+1}$ have the same color. This proves the inductive step.

The induction is complete and we have thus proved that for any n, in any set of n horses all horses (in that set) are of the same color.

EndofProof.

(Hint: The key to this proof is the existence of horse H_2. More details at the end of this document.)

7 Ordinary vs Strong Induction

The induction proof technique we have described is sometimes called **ordinary** or **weak induction**. It can be summarily described by the inductive step $P(n) \Rightarrow P(n+1)$.

Sometimes this does not suffice to show that $P(n)$ is true. We can then use **strong induction**.

Axiom 4 (Strong Induction). For any predicate $P(n)$, if

- $P(1)$ is true
- and $\forall n \in N \; (P(1) \wedge P(2) \wedge \ldots \wedge P(n)) \Rightarrow P(n+1)$,
- then we have shown that $\forall n \in N$, $P(n)$ is true.

Therefore in strong induction, the trueness of $P(n+1)$ is a consequence of the trueness of all preceding predicates $P(1), P(2), \ldots, P(n)$, not just of $P(n)$. As in (weak) induction, the base case can be $P(0)$ or some value other than 0 or 1. Although in Axiom 4 we have $1, \ldots, n$ induces $n+1$, we can alternately have $1, \ldots, n-1$ induces n, i.e. instead of n induces $n+1$ we can have $n-1$ induces n.

7.1 An Example.

A **recursive function** is a function that invokes itself. In **direct recursion** a recursive function f invokes directly itself, whereas in **indirect recursion** function f invokes function g that invokes f. A quite well-known recursive function from discrete mathematics is the Fibonacci function F_n. The Fibonacci function is defined as follows.

$$F_n = F_{n-1} + F_{n-2} \;\text{ if }\; n > 1$$

where

$$F_0 = 0 \;\text{ and }\; F_1 = 1$$

Proposition 5 *For any $n \geq 0$, we have that $F_n \leq 2^n$.*

Proof. Proof is by strong induction. Let the predicate $P(n)$ be $F_n \leq 2^n$.

Base case: Show $P(0)$ is true. We have a base case for $n = 0$ i.e. we show that $F_0 \leq 2^0 = 1$. Since $F_0 = 0$, and we have that $0 \leq 1$ the base case follows.

Inductive Step. Show that $P(0) \wedge \ldots \wedge P(n-1) \Rightarrow P(n)$. Not only was our base case 0 and not 1, but our induction hypothesis will be of the type "$n-1$ induces n". We shall show that if $F_i \leq 2^i$ for all $i = 0, 1, \ldots, n-1$, then $F_n \leq 2^n$, i.e. that if $P(i)$ is true for all $i = 0, 1, \ldots, n-1$, then $P(n)$ is also true.

In order to prove the inductive step we assume the induction hypothesis i.e. that for all $i < n$ we have indeed $P(i)$ true, i.e. $F_i \leq 2^i$. Since $n-1$ and $n-2$ are less than n by the induction hypothesis we thus have that

$$F_{n-1} \leq 2^{n-1}$$

and

$$F_{n-2} \leq 2^{n-2}.$$

The inductive step is then shown by using the recurrence.

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &\leq 2^{n-1} + F_{n-2} \\ &\leq 2^{n-1} + 2^{n-2} \\ &\leq 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n \end{aligned}$$

The second and third line are by the way of the induction hypothesis for $n-1$ and $n-2$ respectively. Therefore we have shown that if $F_i \leq 2^i$ for all $i = 0, \ldots, n-1$, then $F_n \leq 2^n$. This completes the strong induction. ■

We have thus shown that $F_n \leq 2^n$ for all $n \geq 0$.

We can do a little better with the upper bound on F_n.

Example 4. Show that for any $n \geq 0$

$$F_n \leq 2^{n-1}.$$

Example 5. Show that for any $n \geq 1$

$$F_n \geq 2^{(n-1)/2}.$$

Note. The method of solving recurrences through induction and in particular strong induction is known as the substitution or the guess-and-check method. In order to use it we need to know what to show, i.e. the predicate must be given to us in advance, eg $F_n \leq 2^n$. The inductive proof is straightforward and is shown in two steps : (a) Show the base case by using the boundary values of the recurrence (i.e. F_0, F_1), (b) Show the inductive step by using the induction hypothesis for the terms on the right hand side of the recurrence (i.e. use the induction hypothesis on F_{n-1} and F_{n-2}) and then combine the conclusion for the terms on the right hand side of the recurrence using the recurrence itself (in our case $F_n = F_{n-1} + F_{n-2}$).

7.2 A more complicated example : Recurrences and the substitution method.

A recurrence

$$T(n) = 2T(n/2) + n$$

where, n is a power of two, and a boundary condition

$$T_1 = 1$$

This is sometimes referred to as the divide-and-conque merge-sort recurrence and shows up in the analysis of merge-sort. We can formalize the solution $T(n)$ of the recurrence in the following proposition.

Proposition 6 *For any $n \geq 1$, we have that $T(n) \leq n \lg n + n$, where $\lg n$ is the base two logarithm of n.*

Proof. Proof is by strong induction. Let $P(n)$ be $T(n) \leq n \lg n + n$, where $T(n)$ is the solution of the recurrence $T(n) = 2T(n/2) + n$, for $n > 1$ and power of two, and $T(1) = 1$ is its base case.

Base case: Show $P(1)$ is true? We will attempt to show that $P(1)$ is true i.e. that for $n = 1$ $T(n) \leq n \lg n + n$ which is equivalent to showing that $T(1)$ is at most $1 \lg 1 + 1$.

We know that $T(1) = 1$ by assumption (boundary condition of the recurrence) and $1 \lg 1 + 1$ is 1 as well. Therefore $T(1) \leq 1 \lg 1 + 1$, and this completes the base case.

Inductive Step:$P(1) \wedge \ldots \wedge P(n-1) \Rightarrow P(n)$**, for all** $n \geq 2$**.** We shall show that if $T(i) \leq i \lg i + i$ for all $i = 0, 1, \ldots, n-1$, then $T(n) \leq n \lg n + n$.

Since $P(i)$ is true for all $i < n$ it is true for $i = n/2$ since $n/2 < n$ for $n \geq 2$. Therefore we have $P(n/2)$ to be true (induction hypothesis) and thus

$$T(n/2) \leq (n/2) \lg (n/2) + n/2 = n/2 \lg n - n/2 + n/2 = n \lg n/2.$$

$T(n/2)$ is a term on the right-hand side of the recurrence and according to a prior note, we did right by applying the inductive step to that term. Using the advice of the note again, we use the induction hypothesis and the recurrence to establish $P(n)$.

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &\leq 2(n \lg n/2) + n \\ &\leq n \lg n + n \end{aligned}$$

Therefore we have shown that $P(n)$ is true, i.e. $T(i) \leq i \lg i + i$ for all $i = 0, \ldots, n-1$, then $T(n) \leq n \lg n + n$. This completes the inductive step and thus the strong induction as well. ■.

We have thus shown that $T(n) \leq n \lg n + n$ for all $n \geq 1$.

Example 6. Show that for any $n \geq 1$

$$T(n) = T(n/2) + T(n/4) + n$$

is such that $T(n) \leq 20n$ for all $n \geq 1$. Let $T(1) = 1$.

Hint. Apply the induction hypothesis twice to $T(n/2)$ and $T(n/4)$ and then use the recurrence for the inductive step.

Example 7. Show that there exist constant $n_0 > 0$ and $c > 0$ such that for any $n \geq n_0$

$$T(n) = T(n/2) + T(n/4) + n$$

is such that $T(n) \leq cn$ for all $n \geq n_0$. Let $T(1) = 100$.

Hint. If we change the boundary condition in Example 6 from $T(1) = 1$ to say $T(1) = 100$ as we did in Example 7, things might break down. $T(1) \leq 20 \cdot 1$ is not true any more since $T(1) = 100$. Therefore we need to try something else other than 20.

On horses, cows, and tricky inductive arguments.

In a previous example we "showed" by induction that all horses are of the same color. Where is the bug? Particularly, we showed that

A1. $P(1)$ was true,
and

A2. $P(n) \Rightarrow P(n+1)$ for all n,

where $P(n)$ is the predicate

P(n): In any set of $n \geq 1$ horses, all the horses of the set are of the same color.

Many may argue that the error is in the logic of the inductive step.

The logic is fine, the quantification "for all n" is not, since the assumption of alwyas having horse H_2 might not be true. The crux of the inductive step is the existence of three horses H_1, H_2, H_{n+1}. We first form a set of n horses $H_1, H_2, \ldots, H_n$ and apply the induction hypothesis and then form another set of n horses, $H_2, \ldots H_n, H_{n+1}$, and apply the induction hypothesis again. Crucial to the proof is that $c(H_1) = c(H_2)$ from the first application of the induction hypothesis, and $c(H_2) = c(H_{n+1})$ from the second along with $c(H_1) = c(H_2) = \ldots = c(H_n)$ (also derived from the first). These claims however must be true for all values of n greater than or equal to the value of the base case i.e. ≥ 1.

Let's see what happens for $n = 2$, i.e. let's try to show that $P(1) \Rightarrow P(2)$, i.e. show the inductive step for a certain value of n equal to 1. Consider the set of $n+1 = 2$ horses. In this set we can not identify three distinct horses like H_1, H_2, H_{n+1}, and therefore our previous inductive step argument fails completely (cf. What is the color of a "empty horse" or "no horse"). We can only have two horses H_1 and H_{n+1} for $n+1 = 2$. The non-existence of H_2 breaks the whole argument.

Therefore the inductive step that "we proved" before $P(n) \Rightarrow P(n+1)$ is not true for all n (which was supposed to mean $n \geq 1$) but only for $n \geq 2$. This however can not establish the trueness of $P(n)$ for all $n \geq 1$ because $P(2)$ may or may not be true.

What is $P(2)$?

$P(2)$ **is "in any set of two horses, both horses are of the same color".**

We know from nature that this predicate is false because there are white horses, black horses etc, i.e. there exist two horses not of the same color and thus $P(2)$ is not true for all pairs of horses.

$P(2)$ breaks down the whole "inductive proof", since "$P(n) \Rightarrow P(n+1)$ for all $n \geq 2$" is not very useful by itself. It could become useful if $P(2)$ were true and became the base case of the induction, but $P(2)$ is never true, as of this writing anyway! Thus it cannot be used as the base case, and induction requires both a true base case (A1) and an true inductive step (A2) to derive a true conclusion (A3).

In conclusion, the whole "horsy argument" breaks down because

A2. $P(n) \Rightarrow P(n+1)$ for all n,
was not shown, for all $n \geq 1$, i.e., the

A2. $P(n) \Rightarrow P(n+1)$ for all $n \geq 1$,
was never shown to be true: it was only proved for all $n \geq 2$, i.e.

A2. $P(n) \Rightarrow P(n+1)$ for all $n \geq 2$,

and thus the base case "$P(1)$ is true" can not be used with the latter version of the inductive step; for the latter we need $P(2)$ to be true WHICH IS NOT!