... $\sqrt{a}$ is ... irrational

CS 30 Homework #3

Arun Hari Anand

① Claim: $\forall_x \exists_y ((y > x) \land \forall_z (((z \neq y) \land (z > x)) \Rightarrow (z > y)))$

statement	justification
1. Let x be arbitrary	Assumption
2. $x+1 > x$	Property of $\mathbb{Z}$ (integers)
3.1 Let z be arbitrary	Assumption
3.2 $z > x \land z \neq x+1 \land z, x \in \mathbb{Z} \Rightarrow z > x+1$	Property of integers
4. $\forall_{x,z \in \mathbb{Z}} ((z > x \land z \neq x+1) \Rightarrow z > x+1)$	Universal generalization: 3.1, 3.2
5. $x+1 > x \land \forall_z \{(z \neq x+1) \land (z > x)) \Rightarrow (z > x+1)\}$	From 2, 4
6. $\exists_y ((y > x) \land \forall_z (((z \neq y) \land (z > x)) \Rightarrow (z > y)))$	From 5; Existential generalization: 5

The claim thus follows from 1 and 6 by universal generalization

② a) Claim If $5n+6$ is odd, then n is odd

statement	justification
1. Assume n is even	Assumption
2. $n = 2k$ for some $k \in \mathbb{Z}$	Definition of even
3. ~~5(2k)+6~~ $5n+6 = 5(2k)+6 = 10k+6$	Algebra; $2k$ substituted for n in $5n+6$, according to 2
4. $10k+6 = 2(5k+3)$	Algebra: 3
5. $5n+6 = 10k+6 = 2x$ for some $x \in \mathbb{Z}$	3, 4
6. $5n+6$ is even	Definition of even: 5

The claim thus follows from the principle of proof by contraposition.

(b) Claim: If $5x+2$ is rational, then x is rational

1. Assume $5x+2 \in \mathbb{Q} \land x \notin \mathbb{Q}$	-	Assumption
2. $5x+2 = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, such that p, q have no common factors	-	By definition of rational
3. $5qx + 2q = p$	-	Algebra: 2
4. $x = \frac{p-2q}{5q}$	-	Algebra: 3
5. $p-2q \in \mathbb{Z} \land 5q \in \mathbb{Z}$	-	From 2, and definition of integer
6. $x \in \mathbb{Q}$	-	From 4, 5 and definition of rational
7. $x \in \mathbb{Q} \land x \notin \mathbb{Q}$	-	From 6 and 1
8. F	-	From 7

The claim thus follows from the principle of proof by contradiction

c) Claim $\sqrt{2} + \sqrt{3}$ is irrational

1. Assume $\sqrt{2}+\sqrt{3}$ is rational	-	Assumption
2. $\sqrt{2}+\sqrt{3} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, p and q have no common factors, $p \neq 0$	-	Definition of rational
3. $\sqrt{3} = \frac{p}{q} - \sqrt{2}$	-	Algebra: 2
4. $3 = \frac{p^2}{q^2} - 2\sqrt{2}\frac{p}{q} + 2$	-	Algebra: 3
5. $1 = \frac{p^2}{q^2} - 2\sqrt{2}\frac{p}{q}$	-	Algebra: 4

6. $1 = \frac{p^2 - 2\sqrt{2}pq}{q^2}$ - Algebra : 5

7. $q^2 = p^2 - 2\sqrt{2}pq$ - Algebra : 6

8. $\frac{p^2 - q^2}{2pq} = \sqrt{2}$ - Algebra : 7

9. $p^2 - q^2 \in \mathbb{Z} \wedge 2pq \in \mathbb{Z}$ - From 2 and definition of integers.

10. $\sqrt{2}$ is rational - From 8 and definition of rational

11. $\sqrt{2}$ is rational $\wedge$ $\sqrt{2}$ is irrational - From 10 and earlier proof established in class

12. False - From 11

13. The claim thus follows from the principle of proof by contradiction.

d) Claim: If p is a prime, $\sqrt{p}$ is a irrational

Assume that p is a prime and that $\sqrt{p}$ is ~~ratio~~ rational. Thus, $\sqrt{p} = \frac{a}{b}$ for some a, b such that $a, b \in \mathbb{Z}$, a and b have no common factors, as follows from the definition of rational. p can thus be expressed as $\frac{a^2}{b^2}$, and a^2 can be expressed as pb^2. Thus $a^2 = pb^2$. Since a^2 is a perfect square, it must have an even number of prime factors. As an example of this, we can show that 4 (a perfect square) $= 2 \times 2$. The prime factorization of 4 therefore has an even number of prime factors (2). However pb^2 has an odd number of prime factors, because b^2 has an even number of prime factors, and ~~at~~ thus the extra p in the prime factorization of pb^2 means it must have an odd number of prime factors. Since every number has a unique prime factorization, a^2 cannot equal to pb^2. However, it was previously stated that $a^2 = pb^2$. Thus, the assumption that p is a prime and $\sqrt{p}$ is rational must have been false. Thus, the claim follows from the principle of proof by contradiction.

Claim: the set of prime numbers is infinite.

2 e) Assume that there is a finite set of all primes $P = \{p \mid p \text{ is a prime number}\}$. The largest element of P is the largest prime number. Now let us consider the number Y, such that $Y = \left(\prod_{p \in P} (p)\right) + 1$. That is, Y is the product of all elements of P with 1 added to it at the end. We know that Y must be a prime, because $\frac{Y}{p}$, $p \in P$ would result in a remainder of 1 for all elements of P. Since that means that Y has no prime factors, Y must be a prime. Also, we know that the largest element of P is smaller than Y, because of the nature of multiplication of natural numbers and addition by 1. So, Y must be the largest prime number. ~~T~~ Since this contracts our original assumption that the largest prime is ~~the~~ an element of P, the claim follows from proof by contradiction: the set of prime numbers is infinite.

2f) There exists no rational solution r such that $r^3+r+1=0$ - Claim

Proof: Assume that a rational number r exists such that $r^3+r+1=0$. r can be ~~pre~~ represented as $\frac{p}{q}$, $p, q \in \mathbb{Z}$, p and q have no common factors and $p \neq 0$, by the definition of rational number. When we substitute $\frac{p}{q}$ in for r, $\frac{p^3}{q^3} + \frac{p}{q} + 1 = 0$. Simplifying, $\frac{p^3+pq^2+q^3}{q^3} = 0$. This equation is 0 when $p^3+pq^2+q^3=0$. Let us approach the parity of p and q as being one of the following cases:

Case I: p is even, q is odd, Case II: p is odd, q is even, case III: p is odd, q is odd, Case IV: p and q are both even.

Let us now consider all 4 cases:

~~case I: p^3 is odd~~

case I: p^3 is even, pq^2 is even, q^3 is odd. Even + Even + Odd = Odd. As such, an even number cannot be formed by the sum of ~~even~~ two even numbers and an odd number. So case I is not possible

Using similar reasoning,

Case II: odd + even + even = odd, and thus cannot be zero.

$(p^3) + (pq^2) + (q^3)$

Case III: odd + odd + odd = odd, and thus cannot be zero

(p^3) (pq^2) (q^3)

Case IV: even + even + even = even, which can be zero

$(p^3) + (pq^2) + (q^3)$

As such, case IV is the only possibility. But if p and q are both even, they have a common factor of 2, which ~~is a contradiction~~ contradicts our original assumptions about p and q. So, the claim thus follows from the principle of proof by contradiction.

3. Claim: There exists a one-to-one function from A ~~to~~ B $\Rightarrow$ There exists an onto function from B to A, assuming that $A \neq \phi$ and $B \neq \phi$.

Proof: Assume that a one-to-one function, f, exists from $A \to B$. Now consider the following function g

$$g(b) = \begin{cases} a, \text{ such that } f(a) = b & \text{if } \exists_{a \in A} (f(a) = b) \\ \text{an arbitrary } a \in A & \text{if } \neg \exists_{a \in A} (f(a) = b) \end{cases}$$

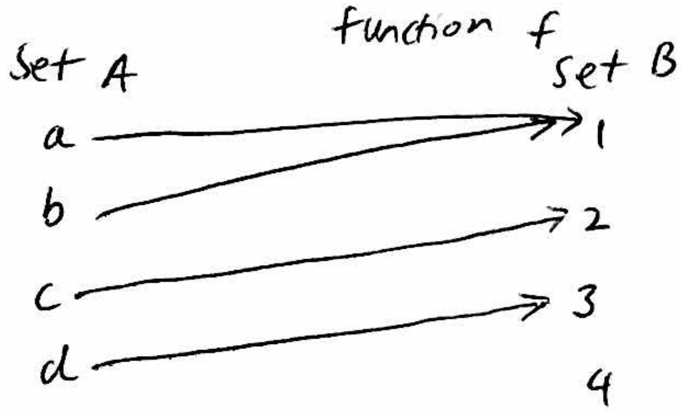
It can be shown that g is a function:

i) every element in B ~~is~~ can either be represented as $f(a), a \in A$ or it cannot. The function g maps each b to some $a \in A$ in either case, so every element in B must be mapped to some $a \in A$. Since some elements of B might be mapped to an arbitrary $a \in A$, we can also show that such a mapping will always exist because $A \neq \phi$.

ii) Since f is a one-to-one function from $A \to B$ it cannot be that $f(a_1) = b_1$ and $f(a_2) = b_2$ for 2 distinct a_1 and a_2 such that $b_1 = b2$. Thus g cannot map a single b to 2 distinct elements of A.

From the above, it follows that g is a function. It is an onto function because f maps every $a \in A$ to a distinct $b \in B$ (by the definition of a one-to-one function), and so g must map some $b \in A$ to each element in A. In other words $\forall_{a \in A} \exists_{b \in B} (g(b) = a)$. From the definition of an onto function, g is an onto function from $B \to A$. The claim thus follows from existential generalization the claim follows from the above.

4. The statement is not true. consider the following mapping from set A to set B, denoted f.



consider the set $S \subseteq A = \{a, c, d\}$. $f(S) = \{1, 2, 3\}$. $f^{-1}(f(S)) = f^{-1}(\{1, 2, 3\}) = \{a, b, c, d\}$. $f^{-1}(f(S)) \neq S$. Thus, the statement is false.

5. Claim $\equiv P(n) \equiv \sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$; where $P(n)$ is a predicate

Base case; when $n=1$:

$$1^3 = \left(\frac{1(2)}{2}\right)^2 = 1^2 = 1$$

$$1^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Thus, ~~the~~ $P(1)$ is true, and the base case holds

Induction step

Let $k \geq 1$ be arbitrary, and assume $P(k)$. Thus

$$\sum_{i=1}^{k} i^3 = \left(\frac{n(n+1)}{2}\right)^2 = \left(\frac{k(k+1)}{2}\right)^2.$$ This is the induction hypothesis

using the above, we attempt to prove $P(n+1)$:

$$\sum_{i=1}^{k+1} i^3 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$

$$= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$$, by combining terms

$$= \frac{(k+1)^2(k^2 + 4(k+1))}{4}$$, factoring out a $(k+1)^2$ from both terms in the numerator

$$= \frac{(k+1)^2(k+2)^2}{4}$$, because k^2+4k+4 factors to $(k+2)^2$

$$= \left(\frac{(k+1)((k+1)+1)}{2}\right)^2$$, by algebra

$$= \left(\frac{n(n+1)}{2}\right)^2$$, since $n = k+1$

The claim thus follows from the principle of mathematical induction

⑥ ~~Pr~~ Claim : $4^n < n!$ if $n \in \mathbb{Z} > 8$; $P(n) \equiv 4^n < n!$

Base case : when ~~n=8~~ $n=9$ $4^9 = 262144$. $9! = 362880$. since $262144 < 362880$, $4^n < n!$. $P(9)$ is true, and thus the base case holds.

Induction step: for a k that is arbitrary and greater than or equal to 9, assume that $P(k)$ is true. That is, $4^k < k!$; this is the induction hypothesis. We now attempt to prove that $4^{k+1} < (k+1)!$

1. $4^k < k!$, ~~give~~ assumption, IH
2. $4 \cdot 4^k < 4 \cdot k!$, multiplication by 4 of both sides
3. $4^{k+1} < 4 \cdot k!$, because $4^{k+1} = 4 \cdot 4^k$
4. $4 \cdot k! < (k+1) \cdot k!$, because for $k \geq 9$, $k+1 > 4$
5. $4^{k+1} < (k+1) \cdot k!$, because $4^{k+1} < 4 \cdot k! < (k+1) \cdot k!$, from ③, ④
6. $4^{k+1} < (k+1)!$, because $(k+1) \cdot k! = (k+1)!$

We have shown than $4^{k+1} < (k+1)!$. The claim thus follows from the principle of mathematical induction

⑦ Claim: Any number higher than or equal to 12 can be expressed in the form $7n_1 + 3n_2$, such that $n_1, n_2 \in \mathbb{W}$.

$P(n) \equiv n = 7n_1 + 3n_2$ for $n_1, n_2 \in \mathbb{W}$

Base Case : when $n=12$, allow n_1 and n_2 to be 0 and 4 respectively. Thus $(7)(0) + (4)(3) = 12$, and so $P(12)$ is true, and the base case holds.

~~Induction : There are 2 cases~~

~~Assu Case I : Assumin~~

Induction : for any arbitrary $k \geq 12$, assume $P(k)$ is true. That is, $k = 7n_1 + 3n_2$ for some $n_1, n_2 \in \mathbb{W}$. This is the induction hypothesis

We now attempt to prove, using the induction hypothesis, that $P(k+1)$ holds.

Case I : Assuming that ~~$n_2 \geq 2$~~ $n_1 \geq 2$, let us attempt to show that we may construct $k+1$ and show $P(k+1)$:

$k = 7n_1 + 3n_2$, $n_1 \geq 2$

$k - 14 = 7(n_1 - 2) + 3n_2$, legal because $n_1 \geq 2$, so $n_1 - 2 \in \mathbb{W}$

$k - 14 + 15 = 7(n_1 - 2) + 3(n_2 + 5)$, by algebra

$k+1 = 7(n_1 - 2) + 3(n_2 + 5)$, $n_1 - 2 \in \mathbb{W} \wedge n_2 + 5 \in \mathbb{W}$

Thus $P(k+1)$ is true.

Case II : ~~If $n_1 < 2$, then $n_2 \geq 4$. This is because the lowest number that we are considering, 12, is only possible if $n_2 = 4$, assuming~~

Case II: If $n_1 < 2$, then $n_2 \geq 2$. This is because the maximum that n_1 can be is 1, and in this case, $n_2 \geq 2$ in order for $(n_1)7 + (n_2)3$ to be higher than or equal to 12.

1. $K = 7n_1 + 3n_2$, $n_1 < 2$, $n_2 \geq 2$
2. $K - 6 = 7n_1 + 3(n_2 - 2)$, by algebra. This is legal because $n_2 \geq 2$, and so $n_2 - 2 \in \mathbb{W}$
3. $K - 6 + 7 = 7(n_1 + 1) + 3(n_2 - 2)$ by algebra
4. $K + 1 = 7(n_1 + 1) + 3(n_2 - 2)$, $n_1 + 1 \in \mathbb{W} \wedge n_2 - 2 \in \mathbb{W}$

Thus $P(K+1)$ is true in this case as well.

The claim thus follows from the principle of mathematical induction.

(b) Claim $\equiv \left(\bigvee_{i\in I} P(i)\right) \Rightarrow Q \equiv \bigwedge_{i\in I} (P(i) \Rightarrow Q)$ for all sets I of finite size greater than zero.

$A(n) \equiv \left(\bigvee_{i\in I} P(i)\right) \Rightarrow Q \equiv \bigwedge_{i\in I} (P(i) \Rightarrow Q)$ for all sets I of size n.

Base case: when $n=1$, $A(n) \equiv (P(1) \Rightarrow Q \equiv P(1) \Rightarrow Q)$. Since the right side and left side of the ~~equation~~ predicate are identical, they are logically equivalent. Thus $A(1)$ holds and the base case is true.

Inductive step: Assume, for an arbitrary $k \geq 1$, that $A(k)$ holds. That is

$$\left(\bigvee_{i\in I} P(i)\right) \Rightarrow Q \equiv \bigwedge_{i\in I} (P(i) \Rightarrow Q) \text{ for all sets of size } k.$$

We now attempt to show that $A(k+1)$ is true. Assume that the $k+1^{th}$ element of set I is a. Thus, we are trying to show the below:

$$P(a) \vee \left(\bigvee_{i\in I-\{a\}} P(i)\right) \Rightarrow Q$$

$$\equiv (P(a) \Rightarrow Q) \wedge \left(\left(\bigvee_{i\in I-\{a\}} P(i)\right) \Rightarrow Q\right), \text{ because } p \vee q \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$$

$$\equiv P(a) \Rightarrow Q \wedge \left(\bigwedge_{i\in I-\{a\}} (P(i) \Rightarrow Q)\right), \text{ by the inductive hypothesis}$$

$$\equiv \bigwedge_{i\in I} (P(i) \Rightarrow Q), \text{ combining}$$

Since I is a set of size $k+1$, we have shown that $P(k+1)$ holds. The claim thus follows from the principle of mathematical induction.

(7) $\exists m \in \mathbb{N}\ \forall n \in \mathbb{N},\ ((n \geq m) \Rightarrow (2^n > n^3))$

n	2^n		n^3
1	2	>	1
2	4	<	8
3	8	<	27
4	16	<	64
5	32	<	125
10	1024	>	1000

Since when $n = 10$, $2^n > n^3$, let us assume that 10 is ~~the~~ an m that satisfies the claim above. We now attempt to rigorously prove that $m = 10$ satisfies the claim.

$P(n) \equiv$ for all $n \geq 10$, $2^n > n^3$

Base case: When $n = 10$, $2^n = 1024$, $n^3 = 1000$. ~~We~~ Thus $2^n < n^3$, because $1024 < 1000$. ~~Rea~~ $P(10)$ is thus true, and the base case holds.

Induction step: Assume that for an arbitrary $k \geq 10$, $P(k)$ holds. That is, $2^k > k^3$. We now use this to prove that $P(k+1)$ holds - that is, $2^{k+1} > (k+1)^3$.

1. $2^k > k^3$, IH
2. $2 \cdot 2^k > 2 \cdot k^3$, by multiplying both sides by 2
3. $2^{k+1} > 2 \cdot k^3$, because $2 \cdot 2^k = 2^{k+1}$
4. $2 \cdot k^3 > k^3\left(1+\frac{3}{10}+\frac{3}{10^2}+\frac{1}{10^3}\right)$, because $1+\frac{3}{10}+\frac{3}{10^2}+\frac{1}{10^3} = 1.331$ and ~~1.331 < 2~~ $2 > 1.331$.
5. $k^3\left(1+\frac{3}{10}+\frac{3}{10^2}+\frac{1}{10^3}\right) \geq k^3\left(1+\frac{3}{k}+\frac{3}{k^2}+\frac{1}{k^3}\right)$, because $k \geq 10$
6. $k^3\left(1+\frac{3}{k}+\frac{3}{k^2}+\frac{1}{k^3}\right) = k^3+3k^2+3k+1 = (k+1)^3$, by algebra
7. $k^3\left(1+\frac{3}{10}+\frac{3}{10^2}+\frac{1}{10^3}\right) \geq (k+1)^3$, by 5 and 6
8. $2^{k+1} > 2 \cdot k^3 > k^3\left(1+\frac{3}{10}+\frac{3}{10^2}+\frac{1}{10^3}\right) \geq (k+1)^3$, by 3, 4, 7
9. $2^{k+1} > (k+1)^3$, by 8

The claim thus follows from the principle of mathematical induction.

Since we have shown that $m=10$ satisfies the claim ~~as~~ presented, ~~by~~ the overall claim that $\exists_{m \in \mathbb{N}} \forall_{n \in \mathbb{N}} ((n \geq m) \Rightarrow (2^n > n^3))$ follows from existential generalization.