

376 Prove the following; quantifications are over nat unless stated otherwise.

- (a) $\neg \exists i, j: j \neq 0 \wedge (i/j)^2 = 2$ The square roots of 2 are irrational.
- (b) $\forall n \cdot (\sum i: 0..n \cdot 1) = n$
- (c) $\forall n \cdot (\sum i: 0..n \cdot i) = n \times (n-1)/2$
- (d) $\forall n \cdot (\sum i: 0..n \cdot i^2) = n \times (n-1) \times (2 \times n - 1)/6$
- (e) $\forall n \cdot (\sum i: 0..n \cdot i^3) = (\sum i: 0..n \cdot i)^2$
- (f) $\forall n \cdot (\sum i: 0..n \cdot 2^i) = 2^{n+1} - 1$
- (g) $\forall n \cdot (\sum i: 0..n \cdot i \times 2^i) = (n-2) \times 2^{n+1} + 2$
- (h) $\forall n \cdot (\sum i: 0..n \cdot (-2)^i) = (1 - (-2)^{n+1}) / 3$
- (i) $\forall n \cdot n \geq 3 \Rightarrow 2 \times n^3 > 3 \times n \times (n+1)$
- (j) $\forall n \cdot n \geq 4 \Rightarrow 3^n > n^3$
- (k) $\forall n \cdot n \geq 4 \Rightarrow n! > 2^n$ where ! is factorial
- (l) $\forall n \cdot n \geq 10 \Rightarrow 2^n > n^3$
- (m) $\forall a, d \cdot \exists q, r \cdot d \neq 0 \Rightarrow r < d \wedge a = q \times d + r$
- (n) $\forall a, b \cdot a \leq b \Rightarrow (\sum i: a..b \cdot 3^i) = (3^{b+1} - 3^a) / 2$
- (o) $\forall n \cdot (n+1)^{\text{nat}} : \text{nat} \times n + 1$
- (p) $\forall n \cdot (\sum i: 0..n \cdot i \times (i+1)) = (n-1) \times n \times (n+1) / 3$
- (q) $\forall n \cdot (\sum i: 0..n \cdot (-1)^i \times i^2) = -(-1)^n \times (n-1) \times n / 2$
- (r) $\forall n \cdot (\sum i: 0..n \cdot 1 / ((i+1) \times (i+2))) = n / (n+1)$

After trying the question, scroll down to the solution.

(a) $\neg \exists i, j. j \neq 0 \wedge (i/j)^2 = 2$ The square roots of 2 are irrational.

§ For this question only, I define $f: \text{nat} \rightarrow \text{xnat}$ so that $f n$ is the number of times that 2 is a factor of n .

$$f(2 \times n) = 1 + f n$$

$$f(2 \times n + 1) = 0$$

From that definition we easily see $f 0 = \infty$, $f 1 = 0$, $f 2 = 1$, $f 3 = 0$, $f 4 = 2$, and so on. Now I need to prove a lemma:

$$f(x \times y) = f x + f y$$

The proof of the lemma uses induction.

if even x

then $\exists n. x = 2 \times n$

$$\wedge f(x \times y)$$

$$= f(2 \times n \times y)$$

$$= 1 + f(n \times y) \quad \text{either } n \times y = 2 \times n \times y = 0 \text{ and we apply a base case, or}$$

else $n \times y < 2 \times n \times y$ and we use the induction hypothesis

$$= 1 + f n + f y$$

use definition of f again

$$= f(2 \times n) + f y$$

$$= f x + f y$$

else if even y

then by a similar proof $f(x \times y) = f x + f y$

else $\text{odd } x \wedge \text{odd } y$

$$\Rightarrow \exists n, m. x = 2 \times n + 1 \wedge y = 2 \times m + 1$$

$$\wedge f(x \times y)$$

$$= f(4 \times n \times m + 2 \times n + 2 \times m + 1)$$

use definition of f

$$= 0$$

use definition of f twice more

$$= f(2 \times n + 1) + f(2 \times m + 1)$$

$$= f x + f y \quad \mathbf{fi \ fi}$$

Now the main theorem:

$$\neg \exists i, j. j \neq 0 \wedge (i/j)^2 = 2$$

duality

$$= \forall i, j. (i/j)^2 = 2 \Rightarrow j = 0$$

$$= \forall i, j. i^2 = 2 \times j^2 \Rightarrow j = 0$$

Now work inside the quantification, starting with the equation.

$$i^2 = 2 \times j^2$$

$$\Rightarrow f(i^2) = f(2 \times j^2)$$

now use the lemma

$$= 2 \times (f i) = f 2 + 2 \times (f j)$$

$$= 2 \times (f i) = 1 + 2 \times (f j)$$

we can't have an even number equal to an odd number

$$= f i = f j = \infty$$

$$= i = j = 0$$

(b) $\forall n. (\sum i: 0..n. 1) = n$

§ $\forall n. (\sum i: 0..n. 1) = n$

induction

$$\Leftarrow (\sum i: 0..0. 1) = 0 \wedge \forall n. (\sum i: 0..n. 1) = n \Rightarrow (\sum i: 0..n+1. 1) = n+1$$

sum over empty domain; divide domain of final sum; simplify

$$= \forall n. (\sum i: 0..n. 1) = n \Rightarrow (\sum i: 0..n. 1) + 1 = n+1 \quad \text{use antecedent as context then drop}$$

$$\Leftarrow \forall n. n+1 = n+1$$

identity

$$= \top$$

$$(c) \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i) = n \times (n-1) / 2$$

$$\begin{aligned} \S & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i) = n \times (n-1) / 2 && \text{induction} \\ \Leftarrow & \quad (\Sigma i: 0, ..0 \cdot i) = 0 \times (0-1) / 2 \\ & \quad \wedge \forall n \cdot (\Sigma i: 0, ..n \cdot i) = n \times (n-1) / 2 \Rightarrow (\Sigma i: 0, ..n+1 \cdot i) = (n+1) \times (n+1-1) / 2 \\ & \quad \text{sum over empty domain; divide domain of final sum; simplify} \\ = & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i) = n \times (n-1) / 2 \Rightarrow (\Sigma i: 0, ..n \cdot i) + n = (n+1) \times n / 2 \\ & \quad \text{use antecedent as context, then drop antecedent} \\ \Leftarrow & \quad \forall n \cdot n \times (n-1) / 2 + n = (n+1) \times n / 2 && \text{arithmetic} \\ = & \quad \top \end{aligned}$$

$$(d) \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i^2) = n \times (n-1) \times (2 \times n - 1) / 6$$

$$(e) \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i^3) = (\Sigma i: 0, ..n \cdot i)^2$$

$$\begin{aligned} \S & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i^3) = (\Sigma i: 0, ..n \cdot i)^2 && \text{induction} \\ \Leftarrow & \quad (\Sigma i: 0, ..0 \cdot i^3) = (\Sigma i: 0, ..0 \cdot i)^2 \\ & \quad \wedge (\forall n \cdot (\Sigma i: 0, ..n \cdot i^3) = (\Sigma i: 0, ..n \cdot i)^2 \Rightarrow (\Sigma i: 0, ..n+1 \cdot i^3) = (\Sigma i: 0, ..n+1 \cdot i)^2) \\ & \quad \text{sum over empty domain; divide domain of final two sums into } 0, ..n \text{ and } n \\ = & \quad 0=0 \wedge (\forall n \cdot (\Sigma i: 0, ..n \cdot i^3) = (\Sigma i: 0, ..n \cdot i)^2 \Rightarrow (\Sigma i: 0, ..n \cdot i^3) + n^3 = ((\Sigma i: 0, ..n \cdot i) + n)^2) \\ & \quad \text{use antecedent as context; drop antecedent} \\ \Leftarrow & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i)^2 + n^3 = ((\Sigma i: 0, ..n \cdot i) + n)^2 && \text{arithmetic} \\ = & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i)^2 + n^3 = (\Sigma i: 0, ..n \cdot i)^2 + 2 \times (\Sigma i: 0, ..n \cdot i) \times n + n^2 && \text{subtract } (\Sigma i: 0, ..n \cdot i)^2 \\ = & \quad \forall n \cdot n^3 = 2 \times (\Sigma i: 0, ..n \cdot i) \times n + n^2 && \text{use Lemma 295(c)} \\ = & \quad \forall n \cdot n^3 = 2 \times n \times (n-1) / 2 \times n + n^2 && \text{arithmetic} \\ = & \quad \top \end{aligned}$$

$$(f) \quad \forall n \cdot (\Sigma i: 0, ..n \cdot 2^i) = 2^n - 1$$

$$\begin{aligned} \S & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot 2^i) = 2^n - 1 && \text{induction} \\ \Leftarrow & \quad (\Sigma i: 0, ..0 \cdot 2^i) = 2^0 - 1 \\ & \quad \wedge \forall n \cdot (\Sigma i: 0, ..n \cdot 2^i) = 2^n - 1 \Rightarrow (\Sigma i: 0, ..n+1 \cdot 2^i) = 2^{n+1} - 1 \\ & \quad \text{sum over empty domain; divide domain of final sum; simplify} \\ = & \quad 0=1-1 \wedge \forall n \cdot (\Sigma i: 0, ..n \cdot 2^i) = 2^n - 1 \Rightarrow (\Sigma i: 0, ..n \cdot 2^i) + 2^n = 2^{n+1} - 1 \\ & \quad \text{use antecedent as context then drop it} \\ \Leftarrow & \quad \forall n \cdot 2^n - 1 + 2^n = 2^{n+1} - 1 && \text{law of exponents, identity} \\ = & \quad \top \end{aligned}$$

$$(g) \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i \times 2^i) = (n-2) \times 2^n + 2$$

$$\begin{aligned} \S & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i \times 2^i) = (n-2) \times 2^n + 2 && \text{induction} \\ \Leftarrow & \quad (\Sigma i: 0, ..0 \cdot i \times 2^i) = (0-2) \times 2^0 + 2 \\ & \quad \wedge \forall n \cdot (\Sigma i: 0, ..n \cdot i \times 2^i) = (n-2) \times 2^n + 2 \Rightarrow (\Sigma i: 0, ..n+1 \cdot i \times 2^i) = (n+1-2) \times 2^{n+1} + 2 \\ & \quad \text{sum over empty domain; divide domain of final sum; simplify} \\ = & \quad \forall n \cdot (\Sigma i: 0, ..n \cdot i \times 2^i) = (n-2) \times 2^n + 2 \Rightarrow (\Sigma i: 0, ..n \cdot i \times 2^i) + n \times 2^n = (n+1-2) \times 2^{n+1} + 2 \\ & \quad \text{use antecedent as context, then drop antecedent} \\ \Leftarrow & \quad \forall n \cdot (n-2) \times 2^n + 2 + n \times 2^n = (n+1-2) \times 2^{n+1} + 2 && \text{law of exponents and simplify} \\ = & \quad \top \end{aligned}$$

$$(h) \quad \forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3$$

$$\begin{aligned} \S & \quad \forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3 && \text{induction} \\ \Leftarrow & \quad (\sum i: 0..0. (-2)^i) = (1 - (-2)^0) / 3 \\ & \quad \wedge (\forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3 \Rightarrow (\sum i: 0..n+1. (-2)^i) = (1 - (-2)^{n+1}) / 3) \\ = & \quad 0=0 && \text{reflexive, identity} \\ & \quad \wedge (\forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3 \Rightarrow (\sum i: 0..n. (-2)^i) + (-2)^n = (1 - (-2)^{n+1}) / 3) && \text{use this context in consequent} \\ = & \quad \forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3 \\ & \quad \Rightarrow (1 - (-2)^n) / 3 + (-2)^n = (1 - (-2)^{n+1}) / 3 && \text{arithmetic} \\ = & \quad \forall n. (\sum i: 0..n. (-2)^i) = (1 - (-2)^n) / 3 \\ & \quad \Rightarrow \top \\ = & \quad \top \end{aligned}$$

$$(i) \quad \forall n. n \geq 3 \Rightarrow 2 \times n^3 > 3 \times n^2 + 3 \times n$$

$$(j) \quad \forall n. n \geq 4 \Rightarrow 3^n > n^3$$

$$(k) \quad \forall n. n \geq 4 \Rightarrow n! > 2^n \text{ where } ! \text{ is factorial}$$

$$(l) \quad \forall n. n \geq 10 \Rightarrow 2^n > n^3$$

$$(m) \quad \forall a, d. \exists q, r. d \neq 0 \Rightarrow r < d \wedge a = q \times d + r$$

$$(n) \quad \forall a, b. a \leq b \Rightarrow (\sum i: a..b. 3^i) = (3^b - 3^a) / 2$$

$$(o) \quad \forall n. (n+1)^{nat} : nat \times n + 1$$

$$\begin{aligned} \S & \quad \forall n. (n+1)^{nat} : nat \times n + 1 && \text{bunch-element conversion} \\ = & \quad \forall n. \forall m. \exists i. (n+1)^m = i \times n + 1 && \text{induction on } m \\ \Leftarrow & \quad \forall n. (\exists i. (n+1)^0 = i \times n + 1) \\ & \quad \wedge (\forall m. (\exists i. (n+1)^m = i \times n + 1) \Rightarrow (\exists i. (n+1)^{m+1} = i \times n + 1)) \\ & \quad \text{In the first } \exists i, \text{ generalize. In the last } \exists i, \text{ rename } i \text{ to } j \text{ and then distribute outward.} \\ \Leftarrow & \quad \forall n. ((n+1)^0 = 0 \times n + 1) \\ & \quad \wedge (\forall m. (\exists i, j. (n+1)^m = i \times n + 1 \Rightarrow (n+1)^{m+1} = j \times n + 1)) \\ & \quad \text{The base case disappears by arithmetic. The step case uses the law of exponents.} \\ = & \quad \forall n, m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow (n+1)^{m \times (n+1)} = j \times n + 1 \\ & \quad \text{In the implication, use context.} \\ = & \quad \forall n, m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow (i \times n + 1) \times (n+1) = j \times n + 1 && \text{arithmetic} \\ = & \quad \forall n, m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow i \times n^2 + i \times n + n = j \times n \\ & \quad \text{Split the domain of } n \text{ into } 0 \text{ and } nat+1. \\ = & \quad (\forall m. \exists i, j. 1^m = 1 \Rightarrow 0+0+0=0) \\ & \quad \wedge (\forall n: nat+1. \forall m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow i \times n^2 + i \times n + n = j \times n) \\ & \quad \text{The top conjunct disappears by arithmetic. In the bottom conjunct, divide by } n. \\ = & \quad \forall n: nat+1. \forall m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow i \times n + i + 1 = j \\ & \quad \text{Generalize } \exists i \\ \Leftarrow & \quad \forall n: nat+1. \forall m. \exists i, j. (n+1)^m = i \times n + 1 \Rightarrow i \times n + i + 1 = i \times n + i + 1 \\ & \quad \text{reflexivity, base, idempotence} \\ = & \quad \top \end{aligned}$$

$$(p) \quad \forall n. (\sum i: 0..n. i \times (i+1)) = (n-1) \times n \times (n+1) / 3$$

$$(q) \quad \forall n \cdot (\sum_{i: 0, \dots, n} (-1)^i \times i^2) = -(-1)^n \times (n-1) \times n / 2$$

$$(r) \quad \forall n \cdot (\sum_{i: 0, \dots, n} 1/((i+1) \times (i+2))) = n/(n+1)$$