Summing Terms in Arithmetic

We can write the sum of first n terms of $f(k)$ in the 'dot dot dot' notation as

$$f(1) + ... + f(n)$$

A more general notation than 'dot dot dot' is $\sum_{k=1}^{n} f(k)$ or we can use

$$(+k \,|\, 1 \le k \ \le n : f(k)\,)$$

Also,we can use $(*k|1 \le k \le n : f(k))$ instead of $\prod_{k=1}^{n} f(k)$. Since the identity for $+$ is 0 and the identity for $*$ is 1,

$$(+k|False : f(k)) = 0 \text{ and } (*k|False : f(k)) = 1$$

Also $(+k \,|\, k = n : f(k)) = f(n)$
and $(*k \,|\, k = n : f(k)) = f(n)$

Predicates

Predicates have arguments from some sets and return Boolean values.
e.g. $Even(n)$ "n is even"
Predicates can have more that one argument:
e.g. $Between(x, y, z)$ "x is between y and z"
e.g. $Parent(p, c)$ "p is a parent of c"
Exercise:
Describe 'in English' the predicate, $S(x, y)$, in the following:
$Parent(p, x) \wedge Parent(p, y) \rightarrow S(x, y)$

A Predicate of no arguments may be regarded as a Proposition, i.e. its value is *True* or *False*.

Logic Quantifiers

- For All, $\forall$
  $(\forall k \mid 1 \leq k \leq n : P(k)) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$
  The quantifier, $\forall$, is a generalisation of Conjunction, $(\wedge)$.
  Some logic texts use $\wedge k$ instead of $\forall k$ but $\forall k$ is more common.
- There Exists, $\exists$
  $(\exists k \mid 1 \leq k \leq n : P(k)) = P(1) \vee P(2) \vee \cdots \vee P(n))$
  The quantifier, $\exists$, is a generalisation of Disjunction, $(\vee)$.
  Some logic texts use $\vee k$ instead of $\exists k$ but $\exists k$ is more common.

De Morgan's Laws for Quantifiers

- $(\forall k | k \in R : P(k))$ can be rewritten as $(\forall k | k \in R \rightarrow P(k))$
- $(\exists k | k \in R : P(k))$ can be rewritten as $(\exists k | k \in R \wedge P(k))$

De Morgan's Laws

- $\neg(\exists x | P(x)) = (\forall x | \neg P(x))$
  "Not Exists = For All not"
  $\neg(P(1) \vee P(2) \vee \cdots \vee P(n)) = \neg P(1) \wedge \neg P(2) \wedge \cdots \wedge \neg P(n)$
  $\neg(\exists k | k \in R : P(k)) = (\forall k | k \in R : \neg P(k))$
  i.e.$\neg(\exists k | k \in R \wedge P(k)) = (\forall k | k \in R \rightarrow \neg P(k))$
- $\neg(\forall x | P(x)) = (\exists x | \neg P(x))$
  "Not for all = Exists not"
  $\neg(P(1) \wedge P(2) \wedge \cdots \wedge P(n)) = \neg P(1) \vee \neg P(2) \vee \cdots \vee \neg P(n)$
  $\neg(\forall k | k \in R : P(k)) = (\exists k | k \in R : \neg P(k))$
  i.e.$\neg(\forall k | k \in R \rightarrow P(k)) = (\exists k | k \in R \wedge \neg P(k))$

De Morgan's Laws for Quantifiers (Cont'd)

$\neg(\forall k | k \in R : P(k))$
$= \neg(\forall k | k \in R \rightarrow P(k))$
$= (\exists k | \neg(k \in R \rightarrow P(k))$
{ From Prop. Logic: $\neg(P \rightarrow Q) = P \wedge \neg Q$ }
$= (\exists k | k \in R \wedge \neg P(k))$
$= (\exists k | k \in R : \neg P(k))$

Negation of Quantifier

Consider the sentence
P: "All soccer fans are well behaved"
Which of the following is equal to $\neg P$:

1. All soccer fans are badly behaved.
2. All non soccer fans are well behaved.
3. Some soccer fans are well behaved.
4. Some soccer fans are badly behaved.

Negation of Quantifier(cont'd)

Let the predicate $S(x)$ be "x is a soccer fan"
and $B(x)$ be "x is well behaved"
We can translate "All soccer fans are well behaved" as
$(\forall x | S(x) \rightarrow B(x))$
Translate "x is badly behaved" i.e. "x is not well behaved" as
$\neg B(x)$
$\therefore$
$\neg P$
$= \neg(\forall x | S(x) \rightarrow B(x))$
$= (\exists x | S(x) \wedge \neg B(x))$
"Some soccer fans are badly behaved"

Fool a person

Let the predicate, $f(p,t)$ be "you can fool a person, p, at time, t" where t is measured in, say, hours i.e. $t \in \mathbb{N}$. Let $p \in People$.
We can rewrite "you can fool a person, p, at time, t" as "person, p, can be fooled at time, t"

- You can fool some of the people all of the time. i.e.
  Some people are always fooled.
  $(\exists p\ \forall t | f(p,t))$
  'There are some people, p, such that for any time, t, p is fooled at t .'

Fool a person

- You can fool all of the people some of the time. i.e.
  Either
  Any person can be fooled at some time.
  $(\forall p\ \exists t |\ f(p,t))$
  'For any person, p, there is some time, t, such that person, p, can be fooled at time t'
  or
  At some time, all the people are fooled
  $(\exists t\ \forall p\,|\ f(p,t))$
  There is some time, t, such that all people are fooled at this time, t.

- You cannot fool all of people all of the time. i.e.
  It is not the case that all people are fooled all of the time.
  $\neg(\forall p \forall t\,|\,(f(p,t))$

General Form of Quantification

Let Q_1 , Q_2 etc. be a quantifiers such as: Σ or $+$, Π or $*, \forall, \exists$.
The underlying binary operators for the quantifiers have the properties:
Associativity, Commutativity and Identity elements.
e.g. The underlying binary operator for $\forall$ is $\wedge$ and this is associative, commutative with an Identity, *True*. The identity for $\vee$ is *False*. The general form is:

$$(Q_1 x \in T_1 \;\; Q_2 y \in T_2 | Range : Predicate\_exp)$$

e.g. $(\forall x \in \mathbb{R} \; \exists y \in \mathbb{R} | x \neq 0 : x * y = 1)$
This states that every real number, except for 0, has an multiplicative inverse.
The mulitiplicative inverse of x is denoted by x^{-1} or $\frac{1}{x}$.
The *Predicate_exp* may be another quantified expression.

Examples

The *Range* expression may be omitted if the quantifier is not restricted.
If the type of the quantifier is understood from the context, it can be omitted. Sometimes, $x : T$ is used instead of $x \in T$.

- $(\forall x, \exists y \mid x + y = 0)$
  Every real number has an additive inverse. The type $\mathbb{R}$ is assumed.
- Assume $n \in \mathbb{N}$.
  Let $Prime(n)$ "n is prime"
  $Between(x, y, z)$ "x is between y and z".

  $\neg(\exists p | Prime(p) \wedge Between(p, 23, 29))$
  "There is no prime between 23 and 29".

Examples (Cont'd)

$(\exists x \in \mathbb{Q} | x^2 = 2)$ is False but $(\exists x \in \mathbb{R} | x^2 = 2)$ is True.
The type of the quantified variable matters.
The (positive) Real number, x, that satisfies $x^2 = 2$ is usually denoted by $\sqrt{2}$.
i.e. $\sqrt{2}$ is a 'witness' for the quantifer, x, when $x \in \mathbb{R}$. Also, $-\sqrt{2}$ is a witness.
i.e. both $\sqrt{2}$ and $-\sqrt{2}$ satisfy the equation, $x^2 = 2$.
There is is no Rational number, q , that satisifies $x^2 = 2$, i.e. $\sqrt{2} \notin \mathbb{Q}$.

Theorem $\neg(\exists x \in \mathbb{Q} | x^2 = 2)$ i.e. $\sqrt{2}$ is not a Rational number.

(Proof by Contradiction)
Assume $(\exists x \in \mathbb{Q} | x^2 = 2)$
i.e. assume there is a fraction $\frac{a}{b}$, in lowest form, such that
$\left(\frac{a}{b}\right)^2 = 2$, $\therefore$
$2b^2 = a^2$ $\therefore$
a^2 is even.
{It can be shown that if a^2 is even then so is a . (See below)}
$\therefore$ a is even, i.e. $a = 2k$, some k .
$\therefore$ $2b^2 = 4k^2$, some k .
i.e. $b^2 = 2k^2$ $\therefore$
b^2 is even,
hence b is even.

$\sqrt{2} \notin \mathbb{Q}$ Cont'd

We have shown that if there is a fraction $\frac{a}{b}$, in lowest form, such that $\left(\frac{a}{b}\right)^2 = 2$ then both a and b are even but then $\frac{a}{b}$ is not in lowest form, hence a contradiction.

$\therefore \neg(\exists x \in \mathbb{Q} | x^2 = 2)$

i.e. $\sqrt{2} \notin \mathbb{Q}$

$\sqrt{2} \notin \mathbb{Q}$ Cont'd

Lemma:
$even(a^2) \rightarrow even(a)$

Proof.

Show $even(a^2) \rightarrow even(a)$
In logic, $p \rightarrow q = \neg q \rightarrow \neg p$
Instead, show $odd(a) \rightarrow odd(a^2)$
Assume $odd(a)$, show $odd(a^2)$
$odd(a)$
$\{\text{let } a = 2k + 1\} \therefore$

$$\begin{aligned} a^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

$\therefore odd(a^2)$. $\square$

Examples(Cont'd)

The expression
$(\exists x \in \mathbb{R} | x^2 - x - 1 = 0)$
states that their is a solution to the equation $x^2 - x - 1 = 0$.
This is True as it can be checked using the quadratic formula

$$\frac{-b \pm \sqrt{b^2 - 4*a*c}}{2*a}$$

for finding the roots of the quadratic function $a * x^2 + b * x + c$.
Using this formula we find that the roots of $x^2 - x - 1$ are

$$\frac{1+\sqrt{5}}{2} \text{ and } \frac{1-\sqrt{5}}{2} .$$

In this case there is more than one solution to the equation.

Div and Mod

- $(\forall a, b\ \exists q, r \mid b \neq 0 : (a = b * q + r) \wedge (0 \leq r < |b|))$
  Euclid's Remainder Theorem assuming the type $\mathbb{Z}$ and $|.|$ is the absolute value function.
  e.g. let $a = 14$, $b = 5$ then
  $(\exists q, r | (14 = 5 * q + r) \wedge (0 \leq r < 5))$
  Values for q and r would be 2 and 4.
  In maths, $q = a\,div\,b$ and $r = a\,mod\,b$.

The functions, $(a\,div\,b)$ and $(a\,mod\,b)$ are defined so that, for $b \neq 0$,

$$a = b * (a\,div\,b) + (a\,mod\,b)\ \wedge 0 \leq (a\,mod\,b) < |b|$$

Note: From this definition, $a\,mod\,b$ is not negative.

Checking Mod and Div

- $a = 14$ and $b = 5$
  Since $14 = 5 * 2 + 4$ and $0 \leq 4 < |5|$
  $14 \; div \; 5 = 2$ and $14 \; mod \; 5 = 4$

- $a = -14$ and $b = 5$
  Since $-14 = 5 * (-3) + 1$ and $0 \leq 1 < |5|$
  $(-14) \; div \; 5 = -3$ and $(-14) \; mod \; 5 = 1$

- $a = 14$ and $b = -5$
  Since $14 = (-5) * (-2) + 4$ and $0 \leq 4 < |-5|$
  $14 \; div \; (-5) = -2$ and $14 \; mod \; (-5) = 4$

- $a = -14$ and $b = -5$
  Since $-14 = (-5) * 3 + 1$ and $0 \leq 1 < |-5|$
  $(-14) \; div \; (-5) = 3$ and $(-14) \; mod \; (-5) = 1$

Java Mod function, %

In Java, the 'mod' function is %. e.g. in Java, 14 % 5 = 4.
An integer is odd iff (n mod 2) = 1. Consider, in Java,

```
bool is_odd(int n)
{
    return (n % 2 == 1);
}
```

In mathematics, -5 is odd but for this Java function, is_odd, the Java function call, $is\_odd(-5)$, returns False as $(-5)\,\%\,2 = -1$.
In Java (and most other 'C-like' programming languages),
$(-a)\,\%\,b = -(a\%b)$.
In mathematics, the sign of $(a\, mod\, b)$ is not negative. Using the maths definiton for $(a\, mod\, b)$ we get that
$(-5)\, mod\, 2 = 1$ as $-5 = 2 * (-3) + 1$ where
$(-5)\, div\, 2 = \lfloor \frac{-5}{2} \rfloor = -3$
In Java, $(a\, div\, b)$ is implemented as a/b, tf. in Java, $(-5)/2 = -2$.