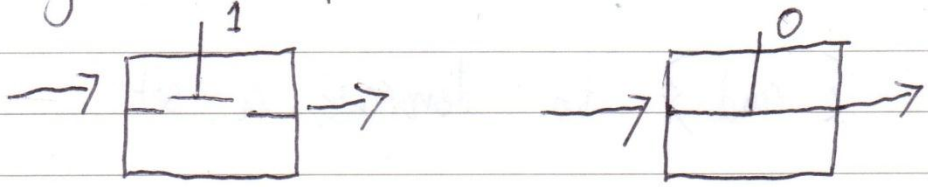
Logic and Proof notes

Jamie Balfour

10/3/2012

Notes on proofs

Logic and Proof



Input	Control	Output
0	0	0
0	1	0
1	0	1
1	1	0

Goal We shall prove that there are things that computers cannot do.

We shall prove this in the following way:

Count the max number of computer programs
Count the number of problems, anyone, anywhere wants to solve

There are less programs than the number of problems

Before we count infinitely, we need to know what it is to count.

- Set
- Bijective correspondence

A set is a collection of objects we wish to regard as a whole. The objects in a set are called its elements. Sets are usually denoted or named using capital letters (of some kind)

We use $\{$ and $\}$ to demorcate a set.

Example

1) $A = \{1, 2, 3\}$

The elements are $1, 2, 3$

"is an element of" can be abreiviated to $\in$

$1 \in A$, $2 \in A$, $3 \in A$, Doris $\notin A$

$\notin$ = "is not an element of"

A set is a bag of elements; two set are equal exactly when they contain the same element.

2) $A = \{1, 2, 3\} = \{3, 2, 1\}$ – order does not matter

3) $\{\ \} = \emptyset$, the empty set.

The number of elements in a set is called its cardinality.

We write $|A|$ to mean the cardinality of A.

Examples

1) $|\emptyset| = 0$

2) $|\{1, 2, 3\}| = 3$

3) $|\{a, b, c, \ldots, x, y, z\}| = 26$

4) $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ <u>natural numbers</u>

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ <u>integers</u>

($\mathbb{Z}$ahl)

$\mathbb{Q}$ $\{$all positive and negative fractions, $\frac{p}{q}\}$

<u>rational numbers</u>, ($\mathbb{Q}$uotient)

$\mathbb{R}$. real numbers 3.1415
2.11

When you count, you <u>pair off</u>.

Penny	Penny	Penny
$\updownarrow$	$\updownarrow$	$\updownarrow$
1	2	3

$1 \longleftrightarrow a$
$2 \longleftrightarrow b$
$3 \longleftrightarrow c$

Mathematize counting:

Let A and B be two sets.

We say that there is a bijective correspondence between A and B if you can do the following:

- Each element of A can be paired off with exactly one element from B in such a way that different elements of A are paired off with different elements of B, and every element in B is paired off with something in A (one thing)

$$\begin{aligned} 1 &\longleftrightarrow a \\ 2 &\longleftrightarrow b \\ 3 &\longleftrightarrow c \end{aligned}$$

✓

We say that A and B are equinumerous (same number of elements) if there is a bijective correspondence.

We write: $A \cong B$

We also write $|A| = |B|$

To say that set A has n elements, means the same thing as A has cardinality n, means the same thing as $A \cong \{1, \ldots, n\}$

Examples - cardinality

1) $|\emptyset| = 0$

2) $|\{\emptyset\}| = 1$

3) $|\{\emptyset, \{\emptyset\}\}| = 2$

$\mathbb{N} = \{0, 1, 2, \ldots\}$ $\quad |\{I, II, III\}| = 3$

$\mathbb{N} = \aleph_0$ aleph nought
or aleph null

Sets which are equinumerous with $\mathbb{N}$ are often called countably infinite.

Examples

1) $\mathbb{E} = \{0, 2, 4, 6, 8, \ldots\}$

1) <u>Claim</u>

$$|\mathbb{E}| = \aleph_0$$

<u>Proof</u>

$$\begin{array}{ccccccccc} \mathbb{N} & \rightarrow & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{E} & \rightarrow & 0 & 2 & 4 & 6 & 8 & 10 & \dots \end{array}$$

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

$$|\mathbb{Z}| = \aleph_0$$

2) <u>Proof</u>

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 \end{array}$$

3) $\mathbb{Q}^{\geqslant}$ = those rational numbers $\geqslant 0$

$= \{ p/q,\ q \neq 0,\ p, q \in \mathbb{N} \}$

$$|\mathbb{Q}^{\geqslant 0}| = \aleph_0$$

"upstairs"

"downstairs"	0	1	2	3	4
1	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$
2	$\frac{0}{2}$	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$
3	$\frac{0}{3}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$
4	$\frac{0}{4}$	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$

array

Every element in the set is in the table

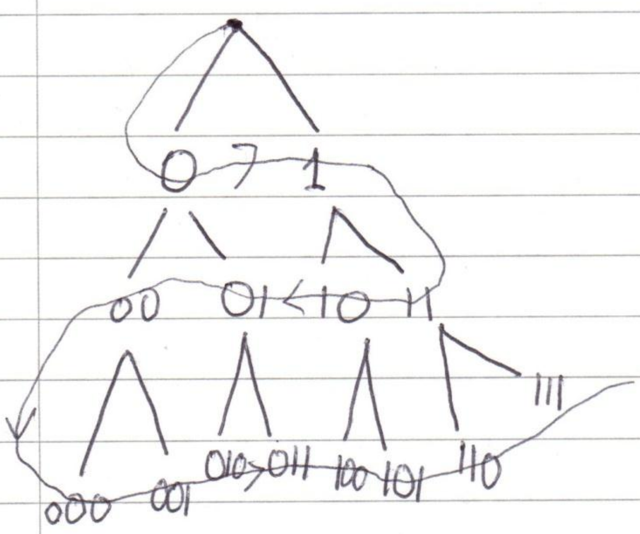
Count in a zig-zag pattern

This means there $\aleph_0$ elements

4) $|\mathbb{Q}| = \aleph_0$

5) Count Java programs

~~Proof~~ Cardinality of Java programs is at most the number of finite binary sequences.



Count all the binary sequences in the "Austrialian" tree

$|\text{Java programs}| = \aleph_0$

Logic and Proof
Section 2

The apparent problem with set notation is that order doesn't matter and repetitions are ignored.

Example

1) $\{a, b\} = \{b, a\}$

2) $\{a, a\} = \{a\}$

We shall begin by introducing some notation to overcome these two defects. (then later show that we can use clever sets to change the same thing).

An ordered pair (a, b) look at the type of brackets

is defined as follows:

$(a, b) = (c, d)$

$a = c$ and $b = d$

(a, b)

first component, second component

In general, we shall want n-tuples which are ordered lists with n components:

(ordered)

$$(a_1, a_2, a_3, \dots a_n)$$

Let A and B be sets.

Define

such that

$$A \times B = \{(a, b) : a \in A, b \in B$$

to be the product of A and B.

more generally,

$A_1, \dots, A_n$ sets

$A_1, \dots, A_n$

$$A_1 \times \dots A_n = \{(a_1, \dots, a_n) : a_1 \in A_1, a_2 \in A_2, \dots a_n \in A_n$$

We abbreviate

$$\underbrace{A \times \dots \times A = A^n}_{n \text{ times}}$$

$n \geq 1$

Examples

$A = \{1,2,3\} \quad B = \{a,b\}$

$A \times B \quad \left\{ \begin{matrix} (1,a), (1,b), (2,a), (2,b), \\ (3,a), (3,b) \end{matrix} \right\}$

In this case, the cardinality of $|A \times B| = |A|\,|B|$

(always true)

2) UK dates

date = (day, month, year)

day $\in \{1, \ldots, 31\} = D$

month = $\{\text{Jan}, \ldots, \text{Dec}\} = M$

year $\in \mathbb{N}$

date $\in D \times M \times \mathbb{N}$

N.B. Not all elements in $D \times M \times \mathbb{N}$ are allowed.

3) British car registration plates

7 tuple

(letter, letter, digit, digit, letter, letter, letter)

$\mathcal{L} = \{A, \dots, Z\}$

$\mathcal{D} = \{0, \dots, 9\}$

$\therefore$ registration plate $\in \mathcal{L}^2 \times \mathcal{D}^2 \times \mathcal{L}^3$

<u>Strings</u>

Strings are applications of tuples.

<u>Example</u>

1) $A = \{0, 1\}$ – "alphabet" – important in CS

2) $B = \{\text{True}, \text{False}\}$ – "alphabet" – true in logic

3) $E = \{$ all words in <u>English</u> in a given dictionary $\}$

4) $F = \{A, G, T, C\}$ – "alphabet" important in Biology

5) $J = \{$ tokens in Java $\}$

Let A be any alphabet (finite, non-empty set)

Then a string over A is just an element of A^n
(of length n)

Note When writing strings we usually omit brackets and commas.

Example

Alphabet $A = \{0, 1\}$

$(0, 1, 1, 0)$ is a string of length 4.

We usually write this as 0110.

This proves that there are $\aleph_0$ Java programs.

Question

$|\mathbb{N} \times \mathbb{N}| = ?$

$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}^2|$

Draw a table

	0	1	2	3	4	5	6	...
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)	
1	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	
2	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	
3								
4								
5								
6								
.								
.								
.								

and so on

$$|\mathbb{N}^2| = \aleph_0$$

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\boxed{\aleph_0^2 = \aleph_0}$$

$$c + \aleph_0 = c$$

$$2^{\aleph_0} = \aleph_1 = c$$

Functions

Machines, programs all follow the IPO cycle.

I = coins from some well defined set
P =
O = drawn from some set

The allowable inputs are called <u>domain</u>
The allowable ouputs are called <u>codomain</u>

The process is known to be <u>deterministic</u>.

Some inputs deliver the same ouputs.

But one output could be the result of different inputs.

This is called a function.

A function consists of three parts of information.

Input is known as the <u>domain</u> of allowable inputs

Output is known as the <u>codomain</u> of allowable outputs

A rule that tells you how to transform inputs into outputs, is called the process.

[The same inputs <u>must</u> always produce the same outputs]

<u>Example</u>

I define function f as follows:

domain of $f = \mathbb{N}$
codomain of $f = \mathbb{E}$

rule of f = $n \mapsto 2n$

input output

<u>Category theory</u>

take functions as the foundations of maths, not sets

So you are just doubling

We could also write that

$$2n = f(n)$$

$f: A \to B$, $A \xrightarrow{f} B$

Ways of defining functions

1) By means of tables   D = domain C = codomain

$D = \{1, 2, 3\}$ $C = \{a, b, c\}$

Function f

f:

x	$f(x)$
1	a
2	b
3	c

2) By means of formulae

$D = \mathbb{N}$ $C = \mathbb{N}$

Function g

$g: \mathbb{N} \to \mathbb{N}$, $g(n) = n^2$

3) <u>Arrow diagrams</u>

$$\begin{array}{ccc} 1 & \longrightarrow & a \\ 2 & \nearrow & b \\ 3 & \longrightarrow & c \end{array}$$

4) Recurssion

The function !

$$\mathbb{N} \xrightarrow{!} \mathbb{N}$$

Notations of writing a function

$$(a, b) \mapsto \underline{a} \times \underline{b}$$

ordered sets

infix notation

$$(a,b) \mapsto m(a,b) \overset{def}{=} a \times b \qquad (a,b)m$$

prefix notation

suffix notation

suffix notation

$$n \mapsto n!$$

i) $0! = 1$

ii) $n! = n\boxed{(n-1)!}$

this is recursion

Calculate

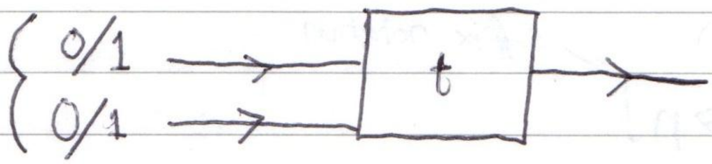
$$
\begin{aligned}
5! &= 5\cdot(4!) \\
&= 5\cdot 4\cdot(3!) \\
&= 5\cdot 4\cdot 3\,(2!) \\
&= 5\cdot 4\cdot 3\cdot 2\,(1!) \\
&= 5\cdot 4\cdot 3\cdot 2\cdot 1\,(0!) \\
&= 5\cdot 4\cdot 3\cdot 2\cdot 1\,(1)
\end{aligned}
$$

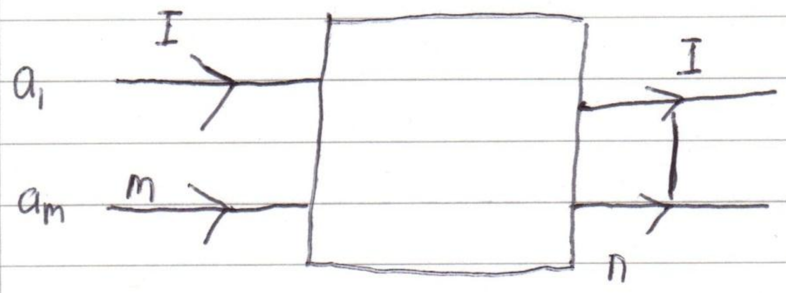
Input	Control	Output
0	0	0
1	0	1
0	1	0
1	1	0

The domain = $(0,0)$
$(0,1)$
$(1,0)$
$(1,1)$

$\boxed{\text{Transistor} : B^2 \to B}$

B for Boolean





input is an element of $\underbrace{A \times \ldots \times A = A^m}_{m \text{ times}}$ $\qquad f: A^m \to A^n$

$(a_1, \ldots a_m)$

Properties of functions

$f: A \to B, \qquad a \mapsto f(a)$

f is called injective if

$a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$

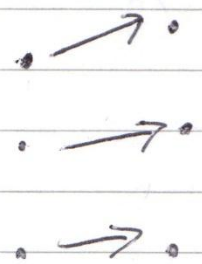
- different inputs yield different outputs

f is called surjective if given $B \in b$ there exists at least one $a \in A$ $f(a) = b$

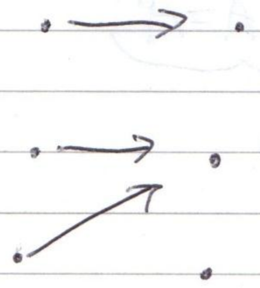
- Everything in the codomain is the image of something in domain

Pictures

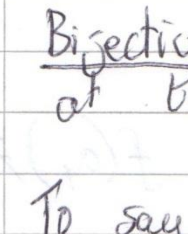
Injective



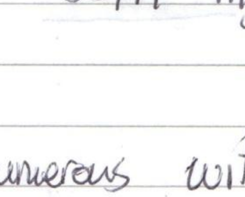
Not injective



Surjective



Not surjective



Bijective means to be both Injective and surjective at the same time.

To say that A is Equinumerous with B is to say exactly that there is a bijection between A and B.

Example question

$$R = \{ x : x \text{ is a set and } x \notin x \}$$

The set in here could be the empty set

Is $R \in R$?

claim 1 $R \notin R \Rightarrow R \in R$

claim 2 $R \in R \Rightarrow R \notin R$

R is not a set