Basic notations and definitions

8/10/2007

Sets

Set:

- explicit notation e.g. $V = \{a, e, i, o, u\}$

  informally, we also use ... e.g. $\mathbb{N} = \{0, 1, 2, \ldots\}$

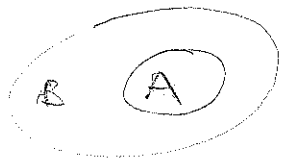
- using a <u>set former</u>, i.e. $\{x \mid E(x)\}$

  where $E(x)$ is a boolean expression depending on x

  e.g. $\{x \mid x \in \mathbb{N} \wedge x \geq 10 \wedge x \leq 50\}$

<u>Subset</u>: $A \subseteq B$ denotes that A is a <u>subset of</u> B (or A is contained in B)

i.e. $\forall x$: if $x \in A$ then $x \in B$



$A \subset B$ means $A \subseteq B$ and $A \neq B$

N.B. We may have sets whose elements are themselves sets

e.g. $A = \{\{0,1\}, \{0,2\}\}$

$B = \{\{0,1\}, \{0,2\}, \{1,2,3\}\}$

If $A \subseteq B$, this does not simply anything wrt the containment between $X \in A$ and $X \in B$, e.g. $x \subseteq y$

<u>Powerset</u>: of a set A: denoted 2^A

$2^A = \{X \mid X \subseteq A\}$

N.B. $x \in 2^A \iff x \subseteq A$

Set operations:

- intersection : $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- union : $A \cup B = \{x \mid x \in A \vee x \in B\}$
- difference $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

When we refer to an implicit universe U, we may denote with $\bar{A}$ the complement of A (wrt U)

i.e. $\bar{A} = U \setminus A$ (e.g. $U = \mathbb{N}$ or $U = \Sigma^*$)

Cartesian product of sets $A_1, A_2 \dots, A_n$

$A_1 \times A_2 \times \dots \times A_n = \{(x_1, \dots, x_n) \mid x_1 \in A_1 \wedge \dots \wedge x_n \in A_n\}$

... set of n-tuples of elements respectively of $A_1, \dots, A_n$

Relations

- binary relation between two sets A and B

$R \subseteq A \times B$

e.g. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ is defined as :

$\leq = \{(x,y) \mid x \in \mathbb{N}, y \in \mathbb{N}, \exists k \in \mathbb{N} \text{ s.t. } x + k = y\}$

- we may use infix notation: $(x,y) \in R \Leftrightarrow x R y$

- $R \subseteq S \times S$ is called a precedence relation
  - reflexive: $\forall a \in S : a R a$
  - symmetric: $\forall a, b \in S$: if $a R b$ then $b R a$
  - transitive: $\forall a, b, c \in S$: if $a R b$ and $b R c$ then $a R c$
  - antisymmetric: $\forall a, b$: if $a R b$ and $b R a$ then $a = b$

- Types of precedence relations:
  - equivalence: reflexive, symmetric, and transitive
  - preorder: reflexive and transitive
  - partial order: antisymmetric preorder
  - total order on S: for all $x, y \in S$ either $x \, R \, y$ or $y \, R \, x$

When $\prec \in S \times S$ is a partial order (on S), we say also that $(S, \prec)$ is a partially ordered set.

- minimal element $x \in S$: $\forall y \in S : y \not\prec x$
- maximal — " — — " — $x \not\prec y$

- Transitive closure of $R \subseteq S \times S$, denoted R^+

$$R^+ = \bigcup_{i \in \mathbb{N}; i \geq 1} R^i \text{, with}$$

$$\begin{cases} R^1 = R \\ R^{i+1} = \{(a, c) \mid \exists b. \, (a, b) \in R^i \wedge (b, c) \in R\} \end{cases}$$

FL 17/10/2008

Functions:

Consider an n-ary relation $R \subseteq A_1 \times \cdots \times A_n$ and $k < n$.
Then R is a k-argument function if
for each k-tuple $(x_1, \ldots, x_k) \in A_1 \times \cdots \times A_k$
there is a unique $n-k$-tuple $(x_{k+1}, \ldots, x_n) \in A_{k+1} \times \cdots \times A_n$
such that $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \in R$.

We denote this as $R : A_1 \times \cdots \times A_k \longrightarrow A_{k+1} \times \cdots \times A_n$

$A_1 \times \dots \times A_k$ ... domain of R

$A_{k+1} \times \dots \times A_n$ ... co-domain of R

We may use $\vec{x}$ to denote an n-tuple of elements, i.e.

$\vec{x} = (x_1, \dots, x_n)$ (where n depends on the context)

For simplicity we consider now just functions $f: A \to B$

(but the same holds for $f: A_1 \times \dots \times A_k \to A_{k+1} \times \dots \times A_n$)

Each $f: A \to B$ is also a relation $f \subseteq A \times B$.

The converse does in general not hold.

But we can associate to each $R \subseteq A \times B$ a function

$$f_R : A \to 2^B \quad \text{with} \quad f_R(x) = \{ y \mid x R y \}$$

$f: A \to B$ is
- injective if $f(x_1) = f(x_2)$ implies $x_1 = x_2$
- surjective if $\forall y \in B, \exists x \in A : f(x) = y$
- bijective if it both injective and surjective

For $D \subseteq A$, $f(D)$ denotes the image of D via f, i.e.

$$f(D) = \{ y \mid \exists x \in D . f(x) = y \}$$

f^{-1} denotes the <u>inverse</u> of f.

f^{-1} may not be a function.

But we can always define for $D \subseteq B$ the <u>inverse image</u> of D

$$f^{-1}(D) = \{ x \mid x \in A \wedge f(x) \in D \}$$

Partial functions:

$f: A \to B$ is <u>total</u> if it is <u>defined</u> for every $x \in A$.

i.e. if $\forall x \in A: \exists y \in B: f(x) = y$ (i.e., $x\, f\, y$)

If f is not defined for some $x \in A$ it is called <u>partial</u>
(we denote partial functions with greek letters)

We use $A \to B$ to denote the set of total functions from A to B.

We use $\varphi(x)\downarrow$ when φ is defined on x

" $\varphi(x)\uparrow$ " is not defined "

Domain of φ: $\mathrm{dom}(\varphi) = \{x \mid \varphi(x)\downarrow\}$

Range of φ: $\mathrm{range}(\varphi) = \{x \mid \exists y.\ \varphi(y) = x \neq \uparrow\}$

(where $\uparrow$ denotes the undefined value)

Cardinality of sets:

$|S|$ denotes the <u>cardinality</u> of a set S

- when S is finite, then $|S|$ is the number of its elements
- when S is infinite, defining $|S|$ is more complicated

<u>Definitions:</u>

- A and B are <u>equinumerous</u> if there is a bijection $f: A \to B$, written $A \approx B$.
- Then $|S|$ denotes the collection of sets Y such that $Y \approx S$.
- $|A| \leq |B|$ if there is an injection $f: A \to B$

Easy: if $A \subseteq B$ then $|A| \leq |B|$

$A < B$ if $A \leq B$ but $A \not\approx B$

A (infinite) set S is <u>countable</u> if it has the same cardinality as $\mathbb{N}$, i.e. $S \approx \mathbb{N}$

The cardinality of the infinite countable sets is denoted $\aleph_0$ (aleph 0)

A set S is finite if $|S| < \aleph_0$

Note: an infinite set can have the same cardinality as one of its proper subsets

e.g. $\mathbb{N}$ and the even numbers

This is not possible for finite sets

<u>Theorem</u>: $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ is countable

Proof: we have to define a bijection $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$i \backslash j$	0	1	2	3	
0	0	1	3	6	10
1	2	4	7		
2	5	8			
3	9				

$$\varphi(i,j) = i + \frac{(i+j)(i+j+1)}{2}$$

<u>Corollary</u>: the set $\mathbb{Q}$ of rationals is countable

Examples of countable sets:

- the set $\mathbb{Z}$ of integers $\begin{matrix} \mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ \downarrow & & & & & & & \\ \mathbb{Z} & 0 & 1 & -1 & 2 & -2 & 3 & \dots \end{matrix}$
- n-tuples of integers, for any n, since the union of countably many countable sets is countable [Exercise]

Not all sets are countable!

We use Cantor's diagonalization method to show that $\mathbb{R}$ is not countable

Def: a function $f: \mathbb{N} \to \{0,1\}$ is called a characteristic function

Each characteristic fun. defines a subset of $\mathbb{N}$

Theorem: The set of all characteristic functions is not countable

Proof: assume it is countable.

Then there is a bijection $g: \mathbb{N} \to \{f \mid f: \mathbb{N} \to \{0,1\}\}$.

Let $g(0) = f_0$, $g(1) = f_1, \ldots, g(k) = f_k, \ldots$

Then, the characteristic function $\hat{f}(n) = 1 - f_n(n)$ does not belong to the enumeration $\{f_i\}_{i \in \mathbb{N}}$.

To see this, consider writing down the f_i's, one per row

	0	1	2	3	...
f_0	(0)	1	1	0	...
f_1	0	(1)	0	0	...
f_2	1	1	(1)	0	
f_3	1	0	0	(0)	
	⋮				
$\hat{f}$	1	0	0	1	...

for each n:

$\hat{f}(n) \neq f_n(n)$

Hence, the assumption that the set was countable was wrong!

More generally, for every set S, we can consider the functions $f: S \to \{0,1\}$.

Such a set $S \to \{0,1\}$ of functions is equinumerous to 2^S.

We can define a bijection $c: (S \to \{0,1\}) \to 2^S$ with

$$c(f) = \{x \mid f(x) = 1\}$$

We can generalize the previous theorem to

Theorem of Cantor: Let S be a set. Then $|S| < |2^S|$

Proof: Let us assume towards a contradiction that there is a bijection $\uparrow: S \to 2^S$.

Let $A = \{x \in S \mid x \notin \uparrow(x)\}$

Since $A \subseteq S$, i.e. $A \in 2^S$ and $\uparrow$ is surjective, there exists an $a \in S$ s.t. $\uparrow(a) = A$.

Now we ask whether $a \in A$:

- if $a \in A$, then by definition of A, $a \notin \uparrow(a) = A$
- if $a \notin A = \uparrow(a)$, the by definition of A, $a \in A$.

We get a contradiction in both cases.

Hence, the initial assumption that $\uparrow$ exists is false.

By Cantor's theorem, we can define an infinite sequence of sets of growing cardinality:

$$|\mathbb{N}| < |2^{\mathbb{N}}| < |2^{2^{\mathbb{N}}}| < \dots$$

Other examples of non-countable sets:

- $2^{\mathbb{N}}$, since it is trivially equinumerous to the set of characteristic functions

$$f \leftrightarrow S_f = \{n \mid f(n) = 1\}$$

- the set of partial functions from $\mathbb{N}$ to $\mathbb{N}$

$$\overrightarrow{\mathbb{N}}_p = \{f \mid f : \mathbb{N} \to \mathbb{N}\}$$

each $f \subseteq \mathbb{N} \times \mathbb{N}$, hence $\overrightarrow{\mathbb{N}}_p \subseteq 2^{\mathbb{N} \times \mathbb{N}}$

Moreover $\mathbb{N} \times \mathbb{N}$ is equinumerous to $\mathbb{N}$.

- the set $\mathbb{R}$ of reels

proof sketch

1) the set of characteristic functions is equinumerous to the interval $[0,1)$

$$0.b_0 b_1 b_2 \ldots \leftrightarrow f \text{ s.t. } f(i) = b_i \;\; \forall i \in \mathbb{N}$$
$$\uparrow b_i \in \{0,1\}$$

2) the interval $[0,1)$ is equinumerous to $\mathbb{R}$

$$g : \mathbb{R} \to (0,1) \quad \text{with} \quad g(x) = \frac{1}{2^x + 1}$$

- the set $\mathbb{R} \times \mathbb{R}$ and, more generally $\mathbb{R}^n$

We have seen that $\aleph_0 = |\mathbb{N}| < |2^{\mathbb{N}}| = |\mathbb{R}|$

Question: is $|2^{\mathbb{N}}|$ the smallest non-countable cardinality?

<u>Continuum Hypothesis</u>: each subset of $\mathbb{R}$ is either countable or has cardinality $|2^{\mathbb{N}}|$

The impact on computer science:

For every programming language, there will exist functions that cannot be computed by a program in that language

Proof: each program is a sequence of symbols.

We can enumerate the programs, e.g. by sorting them according to length, and among programs with the same length, lexicographically.

Hence, the set of programs has cardinality $\aleph_0$.

Instead, the set of characteristic functions has cardinality $|2^{\mathbb{N}}|$ and $\aleph_0 < |2^{\mathbb{N}}|$.

The same holds for the set $\mathbb{N} \to \mathbb{N}$ of functions.

Hence there are (uncountable infinitely many) functions that cannot be computed by any prog

Review of basic definitions:

- **Alphabet**: finite, nonempty set of symbols: Σ

  e.g. $\Sigma = \{0, 1\}$

  $\Sigma = \{a, b, \ldots, z\}$

  Σ = set of Unicode characters

- **String**: finite sequence of symbols from Σ

  $w = a_1 a_2 \cdots a_n$, with $a_i \in \Sigma$ for $i \in \{1, \ldots, n\}$

  e.g. · 01101

  · ciaociao

  · empty string: denoted ε : string with no symbols

  · length of a string = number of (positions for) symbols in the string

  denoted $|w|$ If $w = a_1 \cdots a_n$, then $|w| = n$

  e.g. $|\varepsilon| = 0$ ε is the only string of length 0

  $|b| = 1$

  $|ciaociao| = 8$

  Notice: strictly speaking, the number of symbols in ciaociao is 4

- **Powers of an alphabet**:

  $\Sigma^k = \underbrace{\Sigma \times \Sigma \times \cdots \times \Sigma}_{k \text{ times}}$ ... set of all strings over Σ of length k

  e.g. $\Sigma^0 = \{\varepsilon\}$

  $\{0,1\}^1 = \{0,1\}$ ← what is the difference between lhs and rhs?

  $\{0,1\}^2 = \{00, 01, 10, 11\}$

Closure of an alphabet Σ : Σ^* is the set of all finite strings over Σ

i.e. $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \dots$

also $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \dots$ hence $\Sigma^* = \Sigma^0 \cup \Sigma^+$

Note: all strings in Σ^* are finite

Σ^* is an infinite set

e.g. $\Sigma = \{0, 1\}$

$\Sigma^* = \{0, 1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots\}$

Concatenation of two strings:

$x = a_1 a_2 \cdots a_m \in \Sigma^*$

$y = b_1 b_2 \cdots b_n \in \Sigma^*$

$\Rightarrow x \cdot y = a_1 \cdots a_m b_1 \cdots b_n$ (we may omit the $\cdot$)

Note: $\varepsilon \cdot x = x \cdot \varepsilon = x$, i.e. ε is the identity for conc.

$|x \cdot y| = |x| + |y|$

Language L over Σ : is any subset of Σ^* (i.e. $L \subseteq \Sigma^*$)

Note: L contains only finite strings, but it may be infinite

Examples:

$\begin{cases} \Sigma = \{a, b, \dots, z\} \\ L = \text{set of all English words} \end{cases}$

$\begin{cases} \Sigma = \text{Unicode characters} \\ L = \text{compilable Java programs} \end{cases}$

$\begin{cases} \Sigma = \{0, 1\} \\ L = \{\varepsilon, 01, 0011, 000111, \dots\} \end{cases}$ all strings with equal # of 0 and 1, with all 0's preceding the 1's

$\emptyset$ the empty language ($\neq \{\varepsilon\}$)

Languages versus problems:

So far we talked about languages, and we will continue. However, in Computer Science we are interested in problems, and devising algorithms that solve them.

Let's first consider decision problems, i.e. problems with a yes/no answer.

e.g. - Is 5 a root of $f(x) = 0$?
- Is this first-order logic formula valid?
- Is there a route through all cities shorter than k?
⋮

When trying to solve a problem Π using a computing device, we have to decide how to encode instances of the problem:
- fix an alphabet Σ
- associate to each instance I of Π a string $w_I \in \Sigma^*$

⇒ We can associate to Π a language $\mathcal{L}_\Pi$ over Σ:

$$\Pi = \{ I \mid \Pi(I) = \text{yes} \} \quad \text{... i.e. } \Pi \text{ is the set of yes-instances}$$

$$\mathcal{L}_\Pi = \{ w_I \mid I \in \Pi \} = \{ w_I \mid \Pi(I) = \text{yes} \}$$

⇒ Checking whether $I \in \Pi$ amounts to checking $w_I \in \mathcal{L}_\Pi$.

When we have an arbitrary problem, where we have to "compute" a solution, we can reduce it to a decision problem by making the solution become part of the input, and trying out all solutions.
This idea can be formalized (see later).