Elements of Computability
Handout 1: Sets etc.

G.Bellin

January 16, 2004

Here you find a few notions you already know, some notations you have seen before and some reflections about them you need to be aware of.

1 Sets, functions and relations

The notion of a *set* is so general that we cannot define it without using a similar notion, such as that of a *collection*, a *multiplicity*. Following the German mathematician Georg Cantor, we agree that when we define a set (1) we collect in our thought a multiplicity of objects (its *members*) into a unity and (2) we regard this collection itself as an object that can be member of other sets.

Examples: (i) We can consider the set of the days of the week and write
$D = \{$Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday$\}$,
but also
$D = \{x | x \text{ is a day of the week } \}$

(ii) Within the set $\mathbf{N}$ of natural numbers, we can consider the set P of prime numbers. Since this set is infinite, we cannot list all its members. If we write informally $\{2, 3, 5, 7, \dots \}$, the dots suggest an infinite list, but we can only grasp the set P by giving a property that characterizes it:
$P = \{x | x \text{ is a prime number } \}$
where, as we know, the property "*x is a prime number*" is defined thus: *x is a natural number, which is different from* 1 *and divisible only by x and by* 1.

Remarks. If $\phi(x)$ is a property of x, then the notation $\{x|\phi(x)\}$ makes and assumption about a *universe of discourse*. Consider

$$S = \{x | x > 2\}$$

If x ranges over *real numbers* $\mathbf{R}$ then $x = 2.5$ and $x = \pi$ $(3.14\ldots)$ are in S; if x ranges over the integers $\mathbf{Z}$, then 2.5 and π *are not* in S. So when we define a set from a property ϕ as

$$S = \{x|\phi(x)\}$$

we must ensure that we have specified the universe of discourse $\mathcal{U}$; explicitly,

$$S = \{x \in \mathcal{U}|\phi(x)\}.$$

When we write such a definition, we are assuming that *if $\mathcal{U}$ is a set*, then also S is a set. This assumption can be made explicit in logical symbols as follows

$$\exists y.\forall x.(x \in y \leftrightarrow x \in \mathcal{U} \wedge \phi(x)).$$

Every such formula is called a *comprehension axiom.* There is a very serious issue lurking here, see below the paragraph on *Russell's paradox.*

1.1 Properties of sets

Equality of sets. When we define a set, the order in which its elements are considered does not matter: thus

$$\{p, q, r, s\} = \{r, p, s, q\}.$$

Also it doesn't matter how many times we may have stared at its elements:

$$\{p, p, q, q, r, s\} = \{p, q, r, s\}.$$

Indeed, *A and B are the same set* $(A = B)$ *if and only if A and B have the same elements*, exactly. This principle is called *extensionality axiom.*

The following definitions are certainly familiar to you:

Empty set. We can define a set with no elements, e.g.,

$$\{x \in \mathcal{U}|x \neq x\}.$$

By extensionality, there is only one empty set, *the* empty set $\emptyset = \{\quad\}$.

Subsets. We write $A \subseteq B$ if and only if for all x, $x \in A$ implies $x \in B$. We write $A \subset B$ if $A \subseteq B$ and $A \neq B$.
Thus $\emptyset \subseteq A \subseteq \mathcal{U}$, for all sets A (exercise).

Powerset. We write $\wp(A)$ (the powerset of A) for the set of all subsets of A. E.g., if $A = \{1, 2, 3\}$, then

$$\wp(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

If a set A has n elements, then $\wp(A)$ has 2^n elements.

Ordered pairs. We write (a, b) for the pair having a and b as first and second element, respectively. How can we write this using only set-theoretic notions?

$$(a, b) = \{\{a, b\}\{a\}\}.$$

This may be regarded as an *encoding* of the notion of an ordered pair. It works: indeed, an ordered pair is uniquely identified as soon as we know its elements $\{a, b\}$ and moreover a distinguished element, e.g., the first one $\{a\}$.

Operations on sets. Given two sets A and B, we define

$\overline{A}$ (the *complement* of A) $= \{x \in \mathcal{U} | x \notin A\}$;

$A \cup B$ (the *union* of A and B) $= \{x \in \mathcal{U} | x \in A \text{ or } x \in B\}$;

$A \cup B$ (the *intersection* of A and B) $= \{x \in \mathcal{U} | x \in A \text{ and } x \in B\} = \{x \in A | x \in B\}$;

$A \setminus B$ (A *less* B) $= \{x \in A | x \notin B\}$;

$A \times B$ (the *product* of A and B) $= \{(a, b) | a \in A \text{ and } b \in B\}$.

Exercise: From these definitions you should be able to prove the fundamental algebraic properties of the operations of union and intersection, their associativity and commutativity, the distributivity of union over intersection and of intersection over union, De Morgan's laws, etc. Namely, for all sets A, B, C we have

$$\begin{array}{cc}
(A \cup B) \cup C = A \cup (B \cup C) & (A \cap B) \cap C = A \cap (B \cap C) \\
A \cup B = B \cup A & A \cap B = B \cap A \\
A \cup (B \cap C) = (A \cup B) \cap (A \cup C) & A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\
A \cup \overline{A} = \mathcal{U} & A \cap \overline{A} = \emptyset \\
A \cup A = A = A \cap A & A \cup (A \cap B) = A = A \cap (A \cup B) \\
A \cup \emptyset = A & A \cap \mathcal{U} = A \\
A \cup \mathcal{U} = \mathcal{U} & A \cap \emptyset = \emptyset \\
\overline{A \cup B} = \overline{A} \cap \overline{B} & \overline{A \cap B} = \overline{A} \cup \overline{B} \\
\multicolumn{2}{c}{(A \setminus B) \times C = (A \times C) \setminus (B \times C)}
\end{array}$$

More generally, if A_i is a set for all $i \in I$, then we can write

$$\cup_{i \in I} A_i = \{x \in \mathcal{U} | x \in A_i \text{ for some } i \in I\}$$

and

$$\cap_{i \in I} A_i = \{x \in \mathcal{U} | x \in A_i \text{ for all } i \in I\}.$$

Also for all sets A, B, C we have

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \quad (B \cup C) \times A = (B \times A) \cup (C \times A)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C) \quad (B \cap C) \times A = (B \times A) \cap (C \times A)$$

Is it true (under our set-theoretic definition of ordered pairs) that

$$A \times B = B \times A \quad \text{and} \quad (A \times B) \times C = A \times (B \times C)?$$

1.2 Relations

Let A and B be sets. A *relation* R (between A and B) is any subset of $A \times B$, i.e., $R \subseteq A \times B$. (Notice the *extensional* approach to relationships!) We write aRb for $(a, b) \in R$. If $R \subseteq A \times A$, then R is called a *relation on* (or *over*) A.

Let R be a relation on A. (We write "iff" for "if and only if".)

- R is *reflexive* iff aRa for all $a \in A$.
- R is *symmetric* iff aRb implies bRa, for all $a, b \in A$.
- R is *transitive* iff aRb and bRc imply aRc, for all $a, b, c \in A$.
- R is *antisymmetric* iff aRb and bRa imply $a = b$, for all $a, b \in A$.

A R relation on A is called an *equivalence relation* if it is reflexive, symmetric and transitive.

A *partition* of A is a collection of sets $\{A_1, \ldots, A_n\}$ such that

- each A_i is nonempty;
- for $i \neq j$, $A_i \cap A_j = \emptyset$;
- $\bigcup_{i=1}^{n} A_i = A$.

Lemma. *Every equivalence relation R on A determines a partition of A as follows: given $a \in A$, define the* equivalence class $[a]$ *of a by*

$$[a] = \{x \in A | aRx\}$$

Then the set $\{[a] | a \in A\}$ is a partition of A.

Proof. Each $[a]$ is nonempty, since $a \in [a]$; it is also clear that $\bigcup_{a \in A} [a] = A$. It remains to show that if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$. Suppose $c \in [a]$ and $c \in [b]$ thus aRc and bRc, thus by symmetry cRb. From aRc and cRb by transitivity we obtain (1) aRb. Now for every $x \in [b]$, using (1) we have aRb and bRx, so by transitivity aRx; therefore $[b] \subseteq [a]$.

Next, from (1) by symmetry we obtain (2) bRa. Now for every $y \in [a]$ using (2) we have bRa and aRy, so by transitivity bRy; therefore $[a] \subseteq [b]$. Since $[b] \subseteq [a]$ and $[a] \subseteq [b]$, we conclude $[a] = [b]$, as required.

Lemma. *Every partition $\{A_1, \ldots, A_n\}$ of A determines an equivalence relation, given by*

$$aRb \text{ if and only if for some } i,\ a \in A_i \text{ and } b \in A_i.$$

It is easy to prove that R is reflexive, symmetric and transitive.

Closure. If R is a relation on A, then the *reflexive* [*symmetric, transitive*] *closure* of R is the smallest reflexive [symmetric, transitive] relation that has R as a subset.

Example: Let $R = \{(0, 1), (1, 1), (1, 2)\}$.
The reflexive closure of R is $\{(0, 0), (1, 1), (2, 2), (0, 1), (1, 2)\}$.
The transitive closure of R is $\{(0, 1), (0, 2), (1, 1), (1, 2)\}$.

Exercise: Write the symmetric closure of R.

1.3 Orderings

Pre-orderings. A relation R on A which is *reflexive* and *transitive* is called a *pre-ordering*.

Orderings. A pre-ordering R on A is called an *ordering* if R is also *anti-symmetric.*

Lemma. *Every pre-ordering R on A determines a partial ordering, defined as follows. For each $a \in A$ let*

$$[a] = \{b \in A \mid aRb \text{ and } bRa\}$$

and define $[a]R'[b]$ iff aRb. *Then R' is a partial ordering on the set*

$$A_{/R} = \{[a] \mid a \in A\}.$$

Proof. Since R is reflexive, R' is also reflexive. Since R is transitive, so is R'. Now suppose $[a]R'[b]$ and $[b]R'[a]$, so that we have aRb and bRa. For every $x \in [a]$, xRa and aRb imply xRb and also bRa and aRx imply bRx, therefore $x \in [b]$ and $[a] \subseteq [b]$. Similarly we show that $[b] \subseteq [a]$ and therefore $[a] = [b]$ as required.

Partial, total orderings. If an ordering R exists on A, then we say that A is *partially ordered* by R. An ordering on A is *total* if A has no incomparable elements with respect to R, i.e., for all $a, b \in A$ either aRb or $a = b$ or bRa. A total order is also called a *linear* order and if A is totally ordered, then it is also called a *chain*.

Examples: The relation $<$ on the integers $\mathbf{Z}$ is not a partial order, but its reflexive closure $\leq$ is a partial order, which is also *total*.

Strict orderings. The relation $<$ on $\mathbf{Z}$ is called a *strict* order, and it is *total*. The symmetric closure of $<$ is the relation of inequality $\neq$.

Well-orderings. A relation R on A is called *well-founded* if every non-empty subset X of A has a minimal element with respect to R, i.e., for every $X \subseteq A$ there exists x_0 such that $(x, x_0) \notin X$ for all $x \in X$. A *well-order* is a well-founded total order.
Example: The relation $<$ is a well-order on the natural numbers $\mathbf{N}$ but not on the integers $\mathbf{Z}$.

1.4 Functions

Partial functions. A *partial* function ϕ from A to B is a relation $\phi \subset A \times B$ such that for every $a \in A$ there is *at most one* $b \in B$ such that $(a, b) \in \phi$. We follow the unfortunate but almost universal convention of writing $\phi(a) = b$ whenever $(a, b) \in \phi$. The *domain* of a partial function ϕ is the subset A' of A such that for every $a \in A'$ there exists one $b \in B$ such that $(a, b) \in \phi$.

Total functions. A function f from A to B is *total* if the domain of f is precisely A. We write $f : A \to B$ when f is total from A to B. The set B is called the *codomain* (or the *range*).

Surjections. A (partial or total) function ϕ from A to B is called *surjective* (or *onto* B) if for every $b \in B$ there exists $a \in A$ such that $(a, b) \in \phi$.

Injections. A (partial or total) function ϕ from A to B is called *injective* (or *one-to-one*) if $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

Bijections. A function is called *bijective* if it is both injective and surjective.

Composition. Given two (partial) functions ϕ from A to B and ψ from B to C, the *composition* $\psi \circ \phi$ is a function from A to C defined by

$$(a, c) \in (\psi \circ \phi) \text{ iff there exists } b \in B \text{ such that } (a, b) \in \phi \text{ and } (b, c) \in \psi.$$

Verify that composition of functions has the property that

$$(\chi \circ \psi) \circ \phi = \chi \circ (\psi \circ \phi).$$

Identity and inverses. The *identity on A* is the total function $1_A = \{(a,a)|a \in A\}$. Thus 1_A has the propery that $1_A(a) = a$ for all $a \in A$. The function $g : B \to A$ is an *inverse* of $f : A \to B$ if we have

$$g \circ f = 1_A \qquad \text{and} \qquad f \circ g = 1_B.$$

Lemma. *An inverse $g : B \to A$ of $f : A \to B$ is unique.*

Proof. Let g and g' be inverses of $f : A \to B$. Then

$$g = 1_A \circ g = (g' \circ f) \circ g = g' \circ (f \circ g) = g' \circ 1_B = g'$$

A function $f : A \to A$ is *self-inverse* if $f \circ f = 1_A$.

1.5 Infinite sets

Consider four examples:

1. **N**, the natural numbers 0, 1, 2, ...
2. **Z**, the integers ..., -2, -1, 0, 1, 2, ...
3. **Q**, the rationals;
4. **R**, the reals.

Can we represent these infinite sets in set theory?

(1) We can represent **N** as follows. Define

- let 0 be the empty set $\emptyset$;
- define the function $S(x)$ (*successor of* x) as $x \cup \{x\}$.

So $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, ...
We say that a set Y is *inductive* if it contains 0 and for all x, whenever $x \in Y$ then $S(x) \in Y$. We need the following *axiom*:

Axiom of infinity: there exists an inductive set.

Then by using comprehension we can define **N** as the *smallest* inductive set.

(2) Once we have **N**, we easily get **Z**.

(3) The rationals **Q** can be represented as pairs of integers.

(4) The reals **R** can be represented by their decimal expansion, as infinite sequences of integers (in other words, as functions $f : \mathbf{N} \to \mathbf{N}$).

2 Russell's paradox and axiomatic set-theory

The naif definition of a sets from an arbitrary properties

$$S = \{x|\phi(x)\}$$

leads to contradiction, as Bertrand Russell remarked in a famous letter to the great German philosopher Gottlob Frege.

Suppose we can define $S = \{x|x \notin x\}$ as a set. This definition immediately yields a contradiction: $S \in S$ iff $S \notin S$. The problem lies in the fact that we consider an *unrestricted universe of discourse* $\mathcal{U}$ as a set, i.e., we use an *unrestricted comprehension axiom*:

$$S = \{x \in \mathcal{U}|x \notin x\} \tag{1}$$

By unrestricted comprehension, S is a set, so

$$S \in \mathcal{U} \tag{2}$$

By definition (1)

$$S \in S \text{ iff } S \in \mathcal{U} \text{ and } S \notin S \tag{3}$$

By (2) and (3)

$$S \in S \text{ iff } S \notin S.$$

In some sense, Russell's paradox is a *limiting result*: it puts limits to our capacity of defining abstract entities in a meaningful way.

A way out of Russell's paradox is to distinguish between "small" collections (sets) and "large" collections (classes). Then we allow ourselves to write $x \in S$ only if x and S are sets. Therefore the collection of all sets $\mathcal{U}$ is a *class*, not a *set*; the collection $\{x \in \mathcal{U}|x \notin x\}$ is a class, not a set. We build up sets using *restricted comprehension axioms*

$$S = \{x \in z|x \notin x\}$$

where z is a set; in logical symbols

$$\forall z.\exists y.\forall x.(x \in y \leftrightarrow x \in z \wedge \phi(x)).$$

Next we need axioms to tell us how to enlarge our universe of sets by constructing new sets from given ones. *Zermelo*'s set theory has (1) *restricted comprehension* axioms; (2) the axiom of *extensionality*; (3) the axiom of *foundation* stating that $\in$ is a well-founded relation; (4) the *pairing* axiom which given two sets x and y, allows us to build the set $\{x, y\}$; (5) the *union* axiom, by which the generalized union of a set of sets is iteself a set; (6) the axiom of *infinity* and (7) the *powerset* axiom.