MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.02 – Subsets and power sets

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Subsets

Note: The phrase "if and only if" is used in mathematical definitions to indicate equivalence of statements.

Definition. A set S is a subset of a set T if and only if every element of S is also an element of T.

Notation. We write $S \subseteq T$ to mean "S is a subset of T". Similarly, we write $S \not\subseteq T$ to indicate S is not a subset of T.

For example, we have $\{1, 3\} \subseteq \{1, 2, 3\}$ and $\{1, 2, 3\} \subseteq \{1, 2, 3\}$, but $\{1, 2, 3, 4\} \not\subseteq \{1, 2, 3\}$. We can also see that $\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Definition. Two sets S and T are equal (written $S = T$) if and only if they contain exactly the same elements. This means that every element of S is an element of T, and every element of T is an element of S. So we have that $S = T$ if and only if $S \subseteq T$ and $T \subseteq S$.

Definition. A set S is a proper subset of a set T if and only if $S \subseteq T$ and $S \neq T$. (Equivalently, $S \subseteq T$ and $T \not\subseteq S$.)

Notation. We write $S \subset T$ or $S \subsetneq T$ to mean "S is a proper subset of T".

For example, we have $\{1, 3\} \subset \{1, 2, 3\}$, but $\{1, 2, 3\} \not\subset \{1, 2, 3\}$.

Example – Identifying elements and subsets

Example. Decide whether each of the statements below is true or false.

- $1 \in \{1, \{1\}\}$ is a true statement since 1 is an element of $\{1, \{1\}\}$.
- $1 \subseteq \{1, \{1\}\}$ is a false statement since 1 is not a set, so it cannot be a subset.
- $\{1\} \in \{1, \{1\}\}$ is a true statement since $\{1\}$ is an element of $\{1, \{1\}\}$.
- $\{1\} \subseteq \{1, \{1\}\}$ is a true statement since every element of $\{1\}$ is an element of $\{1, \{1\}\}$.
- $\{\{1\}\} \in \{1, \{1\}\}$ is a false statement since $\{\{1\}\}$ is not an element of $\{1, \{1\}\}$.
- $\{\{1\}\} \subseteq \{1, \{1\}\}$ is a true statement since every element of $\{\{1\}\}$ is an element of $\{1, \{1\}\}$.

Theorem. For any set S, we have $S \subseteq S$ and $\{\} \subseteq S$.

Proof. Clearly $S \subseteq S$, since every element of S is again an element of S. The statement $\{\} \subseteq S$ is vacuously true since every element of $\{\}$ (of which there are none) is an element of S.

Proving statements about set containment

Suppose that S and T are sets. To prove that S is a subset of T, we must show that every element of S is also an element of T. If S is very large, it might be impractical to check each element of S individually. So we typically prove that any arbitrary element of S also belongs to T by working with a general element $x \in S$.

That is, to prove that $S \subseteq T$, we write a proof with the following structure:

Let $x \in S$ be an arbitrary element of S.
$\vdots$
Then $x \in T$.
Thus $S \subseteq T$.

To prove that $S \not\subseteq T$, we only have to show that there is some particular element in S that is not in T. Such a proof would have the structure:

Choose $x \in S$ to be the particular element...
$\vdots$
Then $x \notin T$.
Thus $S \not\subseteq T$.

Example – Proving set containment

Example. Let $S = \{2k + 1 \ : \ k \in \mathbb{Z}\}$ and $T = \{4n - 1 \ : \ n \in \mathbb{Z}\}$. Prove that $S \not\subseteq T$.

Solution. Consider the number 1. Clearly $1 \in S$, since $1 = 2 \times 0 + 1$ and $0 \in \mathbb{Z}$. However $1 \notin T$, since the only solution to $1 = 4n - 1$ is $n = \frac{1}{2}$, which is not an integer. Thus 1 is an element of S that is not an element of T, meaning that $S \not\subseteq T$.

Example. Let $S = \{6k + 1 \ : \ k \in \mathbb{Z}\}$ and $T = \{3n - 2 \ : \ n \in \mathbb{Z}\}$. Prove that $S \subseteq T$.

Solution. Let $x \in S$ be an arbitrary element of S. Then $x = 6k + 1$ for some integer k. We can rewrite this as

$$x = 6k + 1 = 3(2k + 1) - 2,$$

so $x = 3n - 2$ where $n = 2k + 1$ is some integer. This means that $x \in T$, so any element of S is also an element of T, and thus $S \subseteq T$.

Proving further statements about set containment

To prove that $S = T$, we must prove that $S \subseteq T$ and that $T \subseteq S$. Note that this means we must provide two separate proofs (using the structure shown on the previous slide).

To prove that $S \neq T$, we must prove that $S \nsubseteq T$ or that $T \nsubseteq S$. Note that this just means we have to show there is some particular element that belongs to one of the sets but not the other.

To prove that $S \subset T$, we must prove that $S \subseteq T$ and that $S \neq T$. Note that this means after proving that $S \subseteq T$, we just have to find some particular element of T that is not in S.

(To prove that $S \not\subset T$, we must prove that $S \nsubseteq T$ or that $S = T$.)

Example. Let $S = \{6k + 1 \ : \ k \in \mathbb{Z}\}$ and $T = \{3n - 2 \ : \ n \in \mathbb{Z}\}$.
We have already shown that $S \subseteq T$. Prove that S is a proper subset of T.

Solution. To prove that $S \subset T$, it remains to show that $S \neq T$.

Consider the number 4. Clearly $4 \in T$, since $4 = 3 \times 2 - 2$ and $2 \in \mathbb{Z}$. However $4 \notin S$, since the only solution to $4 = 6k + 1$ is $k = \frac{1}{2}$, which is not an integer. Thus 4 is an element of T that is not an element of S, meaning that $S \neq T$. Since we already know $S \subseteq T$, we can conclude that $S \subset T$.

Example – Proving set equality

Example. Let $S = \{6k + 1 \ : \ k \in \mathbb{Z}\}$ and $T = \{6n - 5 \ : \ n \in \mathbb{Z}\}$. Prove that $S = T$.

Solution. We need to prove both that $S \subseteq T$ and that $T \subseteq S$.

<u>Proving $S \subseteq T$:</u> Let $x \in S$ be an arbitrary element of S. Then $x = 6k + 1$ for some integer k. We can rewrite this as

$$x = 6k + 1 = 6(k + 1) - 5,$$

so $x = 6n - 5$ where $n = k + 1$ is some integer. This means that $x \in T$, so any element of S is also an element of T, and thus $S \subseteq T$.

<u>Proving $T \subseteq S$:</u> Let $x \in T$ be an arbitrary element of T. Then $x = 6n - 5$ for some integer n. We can rewrite this as

$$x = 6n - 5 = 6(n - 1) + 1,$$

so $x = 6k + 1$ where $k = n - 1$ is some integer. This means that $x \in S$, so any element of T is also an element of S, and thus $T \subseteq S$.

Since we have now shown that both $S \subseteq T$ and $T \subseteq S$, we can conclude that $S = T$.

Power sets

Definition. The power set of a set S, written as $\mathcal{P}(S)$ or just $P(S)$, is the set of all possible subsets of S.

For example, the subsets of $\{1,2\}$ are $\{\}$, $\{1\}$, $\{2\}$, and $\{1,2\}$, so the power set of $\{1,2\}$ is $\mathcal{P}(\{1,2\}) = \{\,\{\},\{1\},\{2\},\{1,2\}\,\}$.

Example. Find $\mathcal{P}(\{a,b,c\})$.

Solution. We first list the subsets of $\{a,b,c\}$ in increasing size order:

- The only subset of size 0 is $\{\}$.
- The subsets of size 1 are $\{a\}$, $\{b\}$, and $\{c\}$.
- The subsets of size 2 are $\{a,b\}$, $\{a,c\}$, and $\{b,c\}$.
- The only subset of size 3 is $\{a,b,c\}$.

Thus $\mathcal{P}(\{a,b,c\}) = \{\,\{\},\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\,\}$.

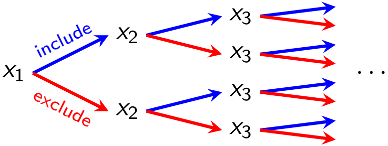
Notice that $|\mathcal{P}(\{1,2\})| = 4 = 2^2$, while $|\mathcal{P}(\{a,b,c\})| = 8 = 2^3$. We can also easily check that $|\mathcal{P}(\{1\})| = 2^1$ and $|\mathcal{P}(\{\})| = 2^0$. This seems to indicate a connection between cardinalities of power sets and powers of 2...

Cardinality of power sets

Theorem. For any finite set S, the cardinality of its power set is given by

$$|\mathcal{P}(S)| = 2^{|S|}.$$

Proof. Since S is finite, we may write $S = \{x_1, x_2, x_3, \ldots, x_n\}$ where $n = |S|$ and each x_i is a different element of S. We can think of creating a subset of S by choosing for each element whether it is included or excluded in the subset. These branching choices can be represented by the tree diagram:



Each path from left to right produces a different subset of S, and all possible subsets are accounted for. At each step, the number of branches doubles, and the last choice is for x_n at the nth step. So there are $2^n = 2^{|S|}$ total different paths available, and thus there are $2^{|S|}$ different subsets of S.

Example. Find the following cardinalities:

- $|\mathcal{P}(\{1, 2, 3, 4\})| = 2^4 = 16.$
- $|\mathcal{P}(\mathcal{P}(\{1\}))| = 2^{|\mathcal{P}(\{1\})|} = 2^{2^1} = 4.$

Proofs involving power sets

The following fact follows straight from our definition of a power set, and can be useful when proving properties of power sets.

Fact. For any sets S and T, we have $S \subseteq T$ if and only if $S \in \mathcal{P}(T)$.

In order to prove a statement involving power sets, we first introduce a lemma about sets. ("Lemma" in mathematics means a minor theorem.)

Lemma. Suppose A, B, and C are sets such that $A \subseteq B$ and $B \subseteq C$. Then $A \subseteq C$.

Proof. Try this yourself! (See tutorial Problem Set 1, Question 7.)

Example. Suppose that S and T are sets such that $S \subseteq T$. Prove that $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.

Solution. Let $X \in \mathcal{P}(S)$ be an arbitrary element of $\mathcal{P}(S)$. Then $X \subseteq S$ by the definition of a power set. Since $S \subseteq T$, by the above lemma we know that $X \subseteq T$. This means that $X \in \mathcal{P}(T)$, so any element of $\mathcal{P}(S)$ is also an element of $\mathcal{P}(T)$, and thus $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.