Section 5.3: Disproofs, Algebraic Proofs and Boolean Algebras

In this section we shall consider how to prove and disprove certain statements about sets using algebraic style proofs and direct proofs. In addition we shall introduce the idea of a Boolean algebra. Specifically, the operations we have defined on sets are in many respects very similar to the logical connective operations. It turns out that there is a common underlying structure to both of these ideas (which is also an underlying structure to many other concepts we already know), and we call this structure a Boolean algebra.

1. Disproving Set Properties

Note that a set property is a statement which is claimed to be true of all sets. As we discussed earlier, to show that such a claim is not true, we need to exhibit a single counterexample. Therefore, to show that a given set property is not true, we need to build a set(s) which do not satisfy the stated property. We illustrate with an example.

Example 1.1. Show that $(A \cap B) \cup C = A \cap (B \cup C)$ is not a set identity.

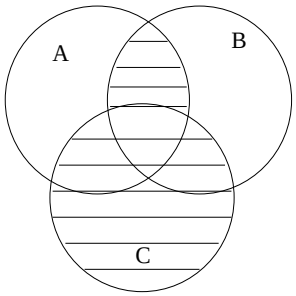
To show that this is not a set identity, we need to provide a counterexample i.e. construct sets A, B and C which do not satisfy this identity. Note that $A \cap (B \cup C)$ will be a subset of A whereas $(A \cap B) \cup C$ will have C as a subset. Therefore, if we choose C to contain any elements which A does not contain, then these will be different sets. Specifically, Let $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ and $C = \{4, 5\}$. Then

$$(A \cap B) \cup C = \{2, 3, 4, 5\}$$

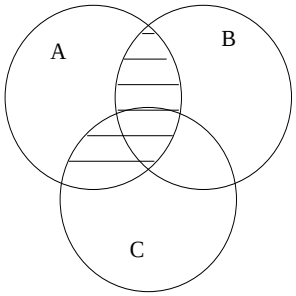
and

$$A \cap (B \cup C) = \{2, 3\}.$$

An alternative way to prove this is through the use of Venn diagrams. Specifically, we shade in the regions corresponding to both sides of the identity and check whether we have the same Venn diagram in each case:



$(A \cap B) \cup C$



$A \cap (B \cup C)$

2. Set Problem Solving

In general, as with any problem in mathematics, there are a couple of general steps one would take to solve it. These are:

(*i*) Ask yourself if the problem statement given seems true - test with a couple of examples to get a gut feeling or attempt a Venn Diagram if the number of sets is small. If there is any doubt, then start looking for a counterexample.

(*ii*) If you are sure the statement is true, then start to construct a set proof - either directly, indirectly or with one of the other methods of proof we discussed.

We have already seen an example of how to disprove a set identity, so we shall instead consider some examples of how to prove set identities. First, as we did in the previous section, we can use standard set identities to derive new set identities.

Example 2.1. Show that for all sets A, B and C, $A \cup (B - A) = A \cup B$.

We have

$$A \cup (B - A) = A \cup (B \cap A^c) = (A \cup B) \cap (A \cup A^c)$$

by the set difference and De Morgans law. Next, using the complement laws and the identity laws, we have

$$(A \cup B) \cap (A \cup A^c) = (A \cup B) \cap (U) = A \cup B$$

proving the identity.

Example 2.2. Show that for all sets A, B and C, $(A - B) \cap (C - B) = A - (B \cup C^c)$.

We have

$$(A - B) \cap (C - B) = (A \cap B^c) \cap (C \cap B^c)$$

by the set difference law. Next, using the distributive and idempotent laws, we have

$$(A \cap B^c) \cap (C \cap B^c) = (A \cap C) \cap (B^c \cap B^c) = (A \cap C) \cap B^c = A \cap (C \cap B^c).$$

Finally, using the set difference law, De Morgans law and the double complement law, we have

$$A \cap (C \cap B^c) = A - (C \cap B^c)^c = A - (C^c \cup B) = A - (B \cup C^c).$$

In addition to these algebraic style proofs, we can use other methods of proof to prove facts about sets. We illustrate with a classical result from set theory.

Theorem 2.3. *For all integers $n \geqslant 0$, if a set X has n elements, then $\mathcal{P}(X)$ has 2^n elements.*

Proof. We shall prove this by induction.
$n = 0$ (base case): if X has 0 elements, then it is the empty set. Since $\mathcal{P}(X)$ is the power set of X, it consists of all the subsets of X. The empty set is always a subset of any set. There are no other subsets (since there are no elements to form subsets with). Hence $\mathcal{P}(X)$ has 1 element and $1 = 2^0$, so the base case holds.

(Induction step) We assume the result holds for an n element set and prove it for a set with n elements. Suppose that X has $n+1$ elements and $z \in X$. Observe that we can break up $\mathcal{P}(X)$ into two distinct subsets - all subsets including z and all subsets which do not include z. Notice also that this divides the set $\mathcal{P}(X)$ exactly into 2. To see this, we observe that we can set up a one-to-one correspondence between such sets - specifically, we can associate any given subset which does not contain z to the subset with the same elements together with z i.e.

$$\{x_1, x_2, \ldots, x_r\} \leftrightarrow \{x_1, x_2, \ldots, x_r, z\}$$

Therefore, the size of $\mathcal{P}(X)$ will be equal to twice that of the number of subsets of X i.e. the size of the set $\mathcal{P}(X - \{z\})$. However, the set $X - \{z\}$ has size n, so by the induction hypothesis, $\mathcal{P}(X - \{z\})$ has 2^n elements. It follows that $\mathcal{P}(X)$ has $2 \cdot 2^n = 2^{n+1}$ elements.

□

3. Boolean Algebras

As observed previously, operations on sets are very similar to logical operators. This is because the abstract underlying structure of these mathematical objects are the same. In this section, we shall explore this abstract underlying structure and show that the results we have proved will generalize to all mathematical objects with this underlying structure. We start with a formal definition.

Definition 3.1. A Boolean algebra is a set B together with two operations, usually denoted $+$ and $\cdot$ such that for all $a, b \in B$, $a + b$ and $a \cdot b$ are in B, and the following properties hold:

- (*i*) (Commutative Laws) For all $a, b \in B$ we have
  - (a) $a + b = b + a$
  - (b) $a \cdot b = b \cdot a$
- (*ii*) (Associative Laws) For all $a, b, c \in B$ we have
  - (a) $(a + b) + c = a + (b + c)$
  - (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (*iii*) (Distributive Laws) For all $a, b, c \in B$ we have
  - (a) $a + (b \cdot c) = (a + b) \cdot (a + c)$
  - (b) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- (*iv*) (Identity Laws) There exists elements 0 and 1 in B such that for all $a \in B$:

(a) $a + 0 = a$
(b) $a \cdot 1 = a$

(v) (Complement Laws) For each $a \in B$, there exists an element $\bar{a} \in B$ called the complement, or negation of a such that:
(a) $a + \bar{a} = 0$
(b) $a \cdot \bar{a} = 1$

Just as we say with both logical operators and set operations, there are many further laws which can be derived such as De Morgans laws, and complement laws (see the text, Theorem 5.3.2 on page 288). We finish by illustrating how to prove such laws for an abstract Boolean algebra.

Theorem 3.2. *(Additive Idempotent Law) For all a in a Boolean algebra B, $a + a = a$*

Proof. We have

$$a = a + 0 = a + a \cdot \bar{a} = (a + a) \cdot (a + \bar{a}) = (a + a) \cdot 1 = a + a$$

□

Theorem 3.3. *(Additive Absorption Law) For all a and b in a Boolean algebra B, $(a + b) \cdot a = a$*

Proof. We have

$$(a + b) \cdot a = (a + b) \cdot (a + 0) = (a + b) \cdot (a + b\bar{b})$$
$$= a + b \cdot (b \cdot \bar{b}) = a + (b \cdot b) \cdot \bar{b} = a + b \cdot \bar{b} = a + 0 = a$$

□

Homework

(i) From the book, pages 290-293: Questions: 2, 6, 7, 13, 17, 19, 20, 23, 28, 31, 36, 39, 43, 49, 51, 52